Obrigações de controlo de fornecedores externos

Planeamento de recuperação

Versão 12.0 Outubro de 2022

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.
"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.
"Convergência de produção"	Convergência de produção (PCO) é um termo utilizado para a ativação pós-falha de um sistema tecnológico para um ambiente alternativo (DR) e utilizado para executar funções de produção por um longo período de tempo.
"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 para aplicar requisitos de resiliência a um serviço. Estes incluem RTO, RPO, requisitos de validação e frequência.

2. 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) e o objetivo de ponto de recuperação (RPO) abaixo especificados para a categoria de resiliência aplicável estipulada pelo Barclays para os serviços contratados:

		Avaliação de impacto de risco	Impacto excecional	Impacto elevado	Impacto moderado	Impacto reduzido	Impacto insignificante
		Categoria de resiliência	0	1	2	3	4
		Tipo de resiliência	Contínua	Altamente resiliente	Resiliente	Recuperar	Suspender/ Efetuar apenas cópia de segurança
Evento de perturbação	Aplicação	Meta RTO (objetivo de tempo de recuperação) (sem dados/eventos cibernéticos)	Até 1 hora	Até 4 horas	Até 12 horas	Até 24 horas	Sem recuperação planeada
		Meta RPO (objetivo de tempo de recuperação) (sem dados/eventos cibernéticos)	Até 5 minutos	Até 15 min	Até 30 min	Até 24 horas	Sem recuperação planeada

3. 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 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 planeamento de eventos de perturbação deve considerar como um mínimo: ▪ 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. ▪ 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 de fornecedor de serviços na nuvem com impacto em todos os serviços tecnológicos). ▪ Perda de um subcontratante importante (serviços ou materiais).	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
	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. Essas dependências devem ser mantidas e revistas a cada 12 meses. As dependências a considerar incluem: ▪ Tecnologia e dados (fornecidos por pessoal interno e subcontratante). ▪ Subcontratante(s) importantes (aqueles que são críticos para a prestação 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.
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 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	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
	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 fornecer planos de correção detalhados (que incluam as ações a realizar e as respetivas datas de finalização).	
4. Teste integrado	O fornecedor de categoria de resiliência 0-1, mediante solicitação do Barclays numa data mutuamente acordada, 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 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. 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 ao Barclays, 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 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. Planos de recuperação de dados	O fornecedor de categoria de resiliência 0-1 deve ter planos de recuperação de dados para cada sistema/serviço 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 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 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
7. Diversidade dos centros de dados	O fornecedor tem de garantir que cada sistema/serviço tecnológico necessário para apoiar a prestação de serviços ao Barclays é resiliente ao longo nos centros de dados e com uma distância 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 serviço deve estar disponível em diferentes zonas de disponibilidade para mitigar uma interrupção na zona de disponibilidade. Os serviços de categoria de resiliência 0-1 devem ser resilientes em todas as regiões da nuvem.	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.
8. Validação do plano de recuperação do sistema	O fornecedor tem de testar e validar os planos de recuperação do sistema para demonstrar que o sistema/serviços tecnológicos podem ser recuperados e cumprir o objetivo de tempo de recuperação e o objetivo de ponto de recuperação, conforme definido pela matriz de níveis críticos de resiliência. Para cada sistema/serviço tecnológico necessário para apoiar a prestação de serviços de 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 plano de recuperação do sistema 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). Para serviços concebidos como ativo/ativo, a validação deve comprovar a continuação do funcionamento sob a perda de um ambiente ativo (cenário de recurso de processamento reduzido). 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	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
	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).	
9. Validação do plano de recuperação de dados	O fornecedor de categoria de resiliência 0-1 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 provar que o processo de recuperação pode recuperar dados para o estado operacional. 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 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.
10. Planos de reconstrução de plataforma e aplicação	O fornecedor de categoria de resiliência 0-1 deve manter um plano de reconstituição de plataforma e aplicação para cada serviço/sistema tecnológico necessário para apoiar a prestação de serviços ao Barclays e estar sujeito a revisão, aprovação e teste pelo menos uma vez a cada 12 meses. 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 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 fornecer	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
	planos de correção detalhados (que incluam as ações a realizar e as respetivas datas de finalização).	