Obrigações de controlo de fornecedores externos

EUDA – Aplicações desenvolvidas pelo utilizador final

Versão 10.0 Datada de outubro de 2020

Tenha em conta que o termo "EUDA", conforme mencionado ao longo deste SCO, é aplicável apenas às EUDA identificadas através da árvore de decisões sobre EUDA do Barclays e àquelas utilizadas para apoiar o(s) serviço(s) prestado(s) pelo fornecedor ao Barclays.

Área de controlo	Designação do controlo	Descrição do controlo	Por que é importante
Governação e garantia	1. Funções e responsabilidades	O fornecedor tem de definir e comunicar funções e responsabilidades para as EUDA. Estas têm de ser revistas após qualquer mudança substancial no modelo de operação ou negócios do fornecedor. As principais funções têm de incluir um executivo sénior, responsável pelas EUDA.	As EUDA exigem apoio de alto nível por forma a garantir que são desenvolvidos, implementados e operados controlos eficazmente. É necessária uma monitorização contínua para dar garantias à direção relativamente à conceção e à operação dos controlos do risco de informação.
Governação e garantia	2. Relato de riscos de informação	Têm de existir controlos e processos documentados por forma a garantir que os incidentes em matéria de segurança de EUDA são relatados e geridos. Os incidentes e as violações em matéria de segurança de EUDA têm de ser objeto de resposta pelo fornecedor e relatados imediatamente ao Barclays. Deve ser estabelecido um processo de resposta a incidentes para tratar e relatar erros que tenham impacto sobre as informações e/ou serviços utilizados pelo Barclays. O fornecedor tem de garantir que as ações corretivas identificadas após um incidente são corrigidas com um plano de correção (ação, responsabilidade, data de conclusão) e partilhadas e acordadas com o Barclays.	
Governação e garantia	3. Monitorização contínua	O fornecedor tem de medir, rever e documentar a sua conformidade com este plano regularmente, pelo menos uma vez por ano.	

Governação e garantia	4. Cumprimento de requisitos legislativos e estatutários locais	O fornecedor tem de garantir que os requisitos legislativos e estatutários relacionados com EUDA aplicáveis à jurisdição onde o fornecedor opera são adequadamente documentados e cumpridos.	*(igual ao acima indicado)*
Governação e garantia	5. Formação e sensibilização sobre EUDA	O fornecedor tem de identificar os funcionários com responsabilidades no âmbito das EUDA. Os funcionários que assumam uma função no âmbito das EUDA terão de concluir a formação e sensibilização adequadas às suas funções. Este controlo deve ser realizado, pelo menos, uma vez por ano, devendo reter-se as evidências que demonstrem esse mesmo facto.	
Objetivos de controlo EUDA	6. Identificação das EUDA	Deve ser documentado e implementado um processo para identificar todas as EUDA detidas ou geridas pelo fornecedor que suportem serviços do Barclays.	A identificação das EUDA é fundamental para determinar o nível de controlo adequado necessário para todas as EUDA.
Objetivos de controlo EUDA	7. Avaliação de sensibilidade das EUDA	A sensibilidade de cada EUDA deve ser avaliada antes da sua primeira utilização na produção e antes da implementação de quaisquer alterações às EUDA. A avaliação de sensibilidade por parte do fornecedor deve ter em conta elementos como os impactos regulamentares, financeiros e ao nível da reputação no serviço prestado pelo fornecedor ao Barclays. A avaliação da sensibilidade também deve ter em conta a importância e a probabilidade de erro. Consultar o Anexo C Em termos de importância, os critérios relevantes incluem o seguinte: • As EUDA apoiam atividades críticas relacionadas com o produto/serviço oferecido ao Barclays? • Os resultados das EUDA têm um impacto financeiro no Barclays? • Os clientes Barclays podem ser afetados negativamente se a informação, cálculos ou resultados das EUDA forem imprecisos ou estiverem desatualizados ou corrompidos? Em termos de probabilidade de erro, os critérios relevantes incluem o seguinte:	Compreender a sensibilidade das EUDA pode permitir ao nosso fornecedor determinar e implementar o nível de controlos adequado para as EUDA em questão.

		• Complexidade percebida das EUDA (sem cálculos relevantes até às fórmulas com elevado grau de complexidade e avançadas); • Frequência da utilização; • Frequência das alterações à fórmula/lógica das EUDA; e • Número de utilizadores. A sensibilidade das EUDA tem de ser acordada com o Barclays.	
Objetivos de controlo EUDA	8. Requisitos de controlo mínimos baseados na sensibilidade das EUDA	O fornecedor tem de implementar controlos que satisfaçam os requisitos dos objetivos de controlo com base no nível de sensibilidade acordado com o Barclays. Os objetivos de controlos assinalados com um "M" são obrigatórios ao abrigo deste plano. Todos os outros objetivos de controlo são apenas opcionais ("O"). Consultar o Anexo B para conhecer a tabela de controlos. Quando adequado, têm de manter-se evidências para demonstrar que os objetivos de controlos aplicáveis estão a ser atingidos.	O nível correto de controlo tem de ser aplicado de acordo com o risco representado pelas EUDA para se evitar um controlo excessivo numa EUDA de risco inferior.
Objetivos de controlo EUDA	9. Justificação das EUDA	Cada EUDA deve ser sujeita a um procedimento de justificação antes da sua primeira utilização, a fim de avaliar se é necessária ou se outros meios alternativos de apoio ao respetivo processo empresarial (por ex., transição para um serviço gerido) seriam mais eficientes e/ou representariam menos riscos do que a manutenção de uma EUDA. O procedimento de justificação das EUDA tem de ser realizado quando uma EUDA é inicialmente criada (ou seja, antes da sua utilização pela primeira vez) e repetido periodicamente daí em diante. Os resultados e as evidências do procedimento de justificação têm de ser guardados e comunicados ao Barclays antes de este utilizar a EUDA pela primeira vez e, posteriormente, sempre que o procedimento seja realizado.	Ao submeter-se a um procedimento de justificação de EUDA, o fornecedor tem a oportunidade de aferir se a EUDA é mesmo necessária.
Objetivos de controlo EUDA	10. Registo das EUDA	Deve existir um inventário EUDA para proporcionar transparência de todos os elementos relevantes em matéria de EUDA para o fornecedor, bem como para captar atributos-chave para suportar as disposições deste plano.	A exaustividade do inventário de EUDA é fundamental para garantir a segurança e operação adequadas das EUDA.

		Deve ser documentado e implementado um processo para garantir um inventário completo, rigoroso e atualizado de EUDA. O inventário de EUDA tem de ser revisto pelo menos anualmente para manter o rigor e verificar a cobertura.	
Objetivos de controlo EUDA	11. Acesso	O acesso a dados e a lógica comercial para todas as EUDA tem de ser limitado a utilizadores apropriados com os direitos de acesso adequados. O acesso tem de ser revisto utilizando uma abordagem baseada nos riscos.	Controlos de acesso adequados protegem as EUDA de um acesso não autorizado, impróprio ou não atribuível.
Objetivos de controlo EUDA	12. Disponibilidade	Têm de existir controlos para garantir que estão disponíveis EUDA de acordo com os requisitos, conforme acordado com o Barclays.	A disponibilidade das EUDA garante uma operação contínua dos processos comerciais.
Objetivos de controlo EUDA	13. Gestão da mudança	Seguir os princípios de gestão da mudança garante que as EUDA funcionam conforme esperado no acompanhamento de mudanças na lógica comercial. As mudanças na lógica comercial das EUDA ou em dados de estatística essenciais não podem resultar em erros de resultados ou relato. Os utilizadores da EUDA devem aceder apenas à(s) versão/versões relevante(s) da mesma para utilização operacional. A completude e exatidão dos dados inseridos, cálculos e dados produzidos são validadas através de testes (automatizados e/ou manuais) a fim de garantir que quaisquer alterações aplicadas produziram o resultado esperado. Os passos de teste deverão ser identificados e acordados com o Barclays relativamente a cada EUDA com uma classificação de "Média" ou "Elevada" na avaliação da sensibilidade da EUDA, a fim de garantir que as alterações não resultam na comunicação de erros. As versões de arquivo não podem ser armazenadas no mesmo local que a(s) versão/versões de produção. O fornecedor tem de designar uma segunda pessoa para auxiliar na utilização e manutenção contínuas das EUDA na ausência do(s) utilizador(es) principal/principais.	Uma gestão de mudança apropriada é fundamental para as EUDA continuarem a funcionar conforme esperado após qualquer mudança

Objetivos de controlo EUDA	14. Requisito de documentação	O conhecimento de inserções, os cálculos, os resultados e a capacidade para os modificar não podem estar limitados a uma única pessoa. Além disso, tem de existir uma documentação adequada que possa ser utilizada por um indivíduo proficiente em EUDA para alterar e manter as EUDA.	Tendo em conta que as EUDA são geridas pelos utilizadores finais, é importante uma documentação adequada para garantir que as informações críticas sobre a EUDA são guardadas por forma a permitir a transferência de conhecimentos e minimizar a possibilidade de perdas de conhecimento.

Anexo A: Definições utilizadas pelo Barclays

Definições	
EUDA	EUDA são aplicações e ferramentas criadas, utilizadas e geridas pelos utilizadores finais. Geralmente, são desenvolvidas utilizando software padrão (principalmente o Microsoft Excel ou Access) e outros tipos de bases de dados, consultas, macros, scripts, ferramentas de relato, executáveis e pacotes de códigos. As EUDA atuam ou fazem parte de um processo empresarial numa base de continuidade (não numa utilização única), sendo que se os respetivos cálculos ou resultados não forem precisos, não estiverem disponíveis ou estiverem desatualizados ou corrompidos, podem ter impacto financeiro, regulamentar ou na reputação do Banco ou podem ser prejudiciais para o cliente.

Anexo B: Requisitos de controlo mínimos

A aplicabilidade de cada controlo é determinada de acordo com a seguinte tabela (O = "Opcional" e M = "Obrigatório"):

Designação do controlo	Classificação de sensibilidade das EUDA			
	Muito baixa	Baixa	Média	Alta
1. Funções e responsabilidades	M	M	M	M
2. Relato de riscos de informação	M	M	M	M
3. Monitorização contínua	M	M	M	M
4. Cumprimento de requisitos legislativos e estatutários locais	M	M	M	M
5. Formação e sensibilização sobre EUDA	M	M	M	M
6. Identificação das EUDA	M	M	M	M
7. Avaliação de sensibilidade das EUDA	M	M	M	M
8. Requisitos de controlo mínimos baseados na sensibilidade das EUDA	M	M	M	M
9. Justificação das EUDA	M	M	M	M
10. Registo das EUDA	O	M	M	M
11. Acesso	O	M	M	M
12. Disponibilidade	O	O	M	M
13. Gestão da mudança	O	O	M	M
14. Requisito de documentação	O	O	O	M

Anexo C: Avaliação de sensibilidade das EUDA

A Avaliação de sensibilidade das EUDA contém duas subavaliações; os Utilizadores principais das EUDA têm de realizar ambas as subavaliações para determinar a Sensibilidade das EUDA.

- Uma avaliação da importância da EUDA para o Barclays.
- Uma avaliação da Probabilidade de erro da EUDA.

A Importância de cada EUDA individual é definida como sendo a classificação mais elevada alcançada a partir dos critérios abaixo enumerados

Critérios de importância das EUDA1	**Classificação da importância das EUDA**			
	Baixa	**Moderada**	**Alta**	**Excecional**
1) A EUDA apoia atividades críticas com impacto regulamentar (equivalente a Ativos ponderados pelo risco ("RWA") ou Exposição diretamente afetada pela EUDA)?	< 50 milhões de libras	≥ 50 milhões ≤ 500 milhões de libras	> 500 milhões ≤ mil milhões de libras	> mil milhões de libras
2) Os resultados das EUDA têm um impacto na comunicação financeira?	Impacto nos Lucros e perdas < 1 milhão de libras Impacto no Balanço < mil milhões de libras	Impacto nos Lucros e perdas ≥ 1 milhão < 10 milhões de libras Impacto no Balanço ≥ mil milhões < 2 mil milhões de libras	Impacto nos Lucros e perdas ≥ 10 milhões < 50 milhões de libras Impacto no Balanço ≥ 2 mil milhões ≤ 3 mil milhões de libras	Impacto nos Lucros e perdas ≥ 50 milhões de libras Impacto no Balanço > 3 mil milhões de libras
3) Se as informações, cálculos e resultados da EUDA forem incorretos ou estiverem desatualizados ou corrompidos, qual seria o impacto **provável** nos clientes do banco2?	Clientes afetados < 100 Perda agregada dos clientes <1 milhão de libras	Clientes afetados ≥ 100 < 1000 Perda agregada dos clientes ≥ 1 milhão < 10 milhões de libras	Clientes afetados ≥ 1000 < 10 000 Perda agregada dos clientes ≥ 10 milhões < 50 milhões de libras	Clientes afetados ≥ 10 000 < 50 000 Perda agregada dos clientes ≥ 50 milhões de libras
4) Se as informações, cálculos e resultados da EUDA forem incorretos ou estiverem desatualizados ou corrompidos, qual seria o impacto **provável** no banco?	Impacto interpretado como "não material" ao nível de uma unidade empresarial local. Sem impacto na marca ou reputação do Grupo.	Impacto interpretado como "controlável" ao nível de uma unidade empresarial local. Sem impacto na marca ou reputação do Grupo.	Impacto adverso em mais de uma empresa/região. É improvável qualquer impacto na marca do Grupo.	Impacto provável na marca do Grupo.

O Utilizador principal da EUDA tem de seguir os critérios abaixo indicados para avaliar a probabilidade de erro da EUDA. O Utilizador principal da EUDA tem de agregar as pontuações atribuídas aos critérios a fim de calcular a classificação final da "Probabilidade de erro".

Critérios da Probabilidade de erro da EUDA	Pontuação da Probabilidade de erro			
	Um	**Dois**	**Três**	**Quatro**
1) Qual a complexidade percebida da EUDA? (ver definição abaixo*)	Rudimentar	Ligeira	Intermédia	Avançada
2) Qual a frequência de utilização da EUDA?	Utilização menos frequente do que trimestralmente	Uma ou mais vezes por trimestre, mas menos do que uma vez por mês	Uma ou mais vezes por mês, mas não diariamente	Uma ou mais vezes por dia
3) Qual a frequência das alterações à fórmula/lógica da EUDA?	Nunca ou muito raramente	São realizadas alterações mas a título excecional	Alterações regulares, mas não sempre que a EUDA é utilizada	Sempre que a EUDA é utilizada
4) Quantos utilizadores tem a EUDA?	Utilizador único	Múltiplos utilizadores na mesma equipa operacional	Múltiplos utilizadores em equipas diferentes dentro de uma Unidade empresarial ou cargo	Múltiplos utilizadores em diferentes Unidades empresariais e/ou cargos

*Refere-se à funcionalidade da EUDA, sendo categorizada da seguinte forma:

- **Rudimentar** – Sem cálculos significativos na EUDA. Essencialmente utilizada como relatórios de síntese.
- **Ligeira** – Um revisor com conhecimentos limitados sobre a aplicação consegue interpretar a finalidade e eficácia das fórmulas mediante observação e sem explicações externas.

- **Intermédia** – Assume uma funcionalidade mais complexa. Um revisor experiente na utilização da aplicação (por ex., Excel, Access) pode necessitar de informações adicionais para interpretar a finalidade e eficácia da EUDA.

- **Avançada** – Elevado grau de complexidade e fórmulas avançadas. Também pode ligar a outras folhas de cálculo, bases de dados, websites, tabelas, etc.

A classificação final da "Probabilidade de erro" tem de ser calculada aplicando a pontuação agregada na tabela abaixo:

Classificação da Probabilidade de erro	Improvável	Possível	Provável	Muito provável
Pontuação agregada	≥ 4 < 6	≥ 6 < 9	≥ 9 < 12	≥ 12 ≤ 16

Avaliação de sensibilidade das EUDA

O Utilizador principal da EUDA tem de combinar as avaliações da Importância e da Probabilidade de erro a fim de determinar a sensibilidade global da EUDA. Deve ser utilizada a seguinte tabela. A Avaliação da sensibilidade da EUDA tem de ser registada no inventário das EUDA por parte do Utilizador principal da mesma.

Importância	Excecional	**Média**	**Média**	**Alta**	**Alta**
	Alta	**Média**	**Média**	**Média**	**Alta**
	Moderada	**Baixa**	**Baixa**	**Média**	**Média**
	Baixa	**Muito baixa**	**Muito baixa**	**Muito baixa**	**Muito baixa**
Probabilidade de erro		Improvável	Possível	Provável	Muito provável