Obligaciones de control para Proveedores externos

EUDA – Aplicaciones desarrolladas para el usuario final

Versión 9 con fecha de abril de 2019

Debe tenerse en cuenta que el término "EUDA" tal como se menciona en este SCO, solo se aplica a las EUDA tal como están identificadas a través del árbol de decisión EUDA de Barclays y a las utilizadas para respaldar los servicios que el Proveedor presta a Barclays.

Área de control	Título del control	Descripción del control	Por qué es importante
Gobernanza y Garantías	1. Funciones y Responsabilidades	El Proveedor definirá y comunicará las funciones y responsabilidades relativas a las EUDA. Se revisarán después de cualquier cambio esencial en el modelo operativo o negocio del Proveedor. Las funciones principales incluirán a un ejecutivo senior, responsable de las EUDA.	Se requiere un alto nivel de patrocinio para garantizar que los controles de las EUDA sean diseñados, implementados y operados de forma efectiva. Es necesaria la supervisión continua para que la dirección senior tenga garantías sobre el diseño y operación de los controles de riesgo de la información.
Gobernanza y Garantías	2. Notificación de los riesgos de la información	Se pondrán en práctica controles y procesos documentados que garanticen la notificación y gestión de los incidentes de riesgo de las EUDA. El Proveedor responderá a los incidentes de las EUDA, así como a las vulneraciones de la seguridad de la información, y lo comunicará a Barclays inmediatamente. Se establecerá un proceso de respuesta a incidentes para gestionar y notificar de forma oportuna los errores que afecten a la información de Barclays y/o a los servicios utilizados por el banco. El Proveedor se asegurará de contar con un plan de reparación (acción, persona responsable y fecha efectiva) donde se incluyan las medidas correctivas a emprender en caso de que se produzca un incidente. Este plan se pondrá en conocimiento de Barclays para su aprobación.	
Gobernanza y Garantías	3. Supervisión continua	El Proveedor evaluará, revisará y documentará el cumplimiento de este Anexo periódicamente y, en cualquier caso, al menos una vez al año.	
Gobernanza y Garantías	4. Cumplimiento de los requisitos legislativos y normativos locales	El Proveedor se asegurará de que se cumplan los requisitos legislativos y normativos relativos a las EUDA de la jurisdicción en la que opere y de que estén debidamente documentados.	*(igual que el anterior)*

Gobernanza y Garantías	5. Educación y sensibilización sobre las EUDA	El Proveedor identificará a los empleados con responsabilidades sobre las EUDA. Los empleados a los que se les haya asignado funciones relativas a las EUDA recibirán la debida formación y poseerán los conocimientos necesarios para desempeñar su función. Se realizará este control al menos una vez al año y se conservarán las pruebas que lo demuestren.	
Objetivos del control de las EUDA	6. Identificación de las EUDA	Se documentará e implementará un proceso para identificar a todos los Proveedores que posean o gestionen EUDA que soporten servicios de Barclays.	La identificación de las EUDA es de vital importancia para determinar el nivel correcto de control necesario para todas las EUDA.
Objetivos del control de las EUDA	7. Evaluación de la criticidad de las EUDA	Se evaluará la criticidad de cada EUDA antes del primer uso en producción y antes de que se aplique cualquier cambio a cada una de las EUDA. La evaluación de la criticidad del Proveedor tendrá en cuenta elementos, como pueden ser el impacto financiero, normativo y en la reputación para el servicio que presta el Proveedor a Barclays. La evaluación de la criticidad también tendrá en cuenta la importancia y la probabilidad de error. Consulte el Apéndice C. Respecto a la importancia, los criterios relevantes incluyen los siguientes: • ¿Admiten las EUDA actividades críticas relacionadas con el producto o servicio ofrecido a Barclays? • ¿Pueden los resultados de las EUDA afectar económicamente a Barclays? • ¿Pueden los clientes de Barclays verse afectados negativamente si la información, los cálculos o los resultados de la EUDA son inexactos, obsoletos o corruptos? Desde el punto de vista de la probabilidad de errores, los criterios destacados incluyen los siguientes: • Complejidad percibida de las EUDA (sin cálculos importantes hasta un alto grado de fórmulas complejas y avanzadas);	El conocimiento de la criticidad de las EUDA puede ayudar a nuestro Proveedor a determinar y aplicar el nivel adecuado de controles para las EUDA.

		• Frecuencia de uso; • Frecuencia de los cambios en la fórmula o la lógica de las EUDA; y • Número de usuarios. La criticidad de las EUDA se acordará con Barclays.	
Objetivos del control de las EUDA	8. Requisitos mínimos de control basados en la criticidad de las EUDA	El Proveedor implementará controles que satisfagan los requisitos de los objetivos de control basados en el nivel de criticidad acordado con Barclays. Los objetivos de control marcados con una "I" en este Anexo son imperativos. Todos los demás objetivos de control son solo opcionales ("O"). Ver Apéndice B para la tabla de controles. Se conservarán las pruebas, sonde proceda, a fin de demostrar que se han alcanzado los objetivos con respecto a los controles aplicables.	Se aplicará el nivel de control correcto en consonancia con el riesgo que represente la EUDA para evitar el control excesivo de una EUDA de menor riesgo.
Objetivos del control de las EUDA	9. Justificación de las EUDA	Cada una de las EUDA se someterá a un procedimiento de justificación antes del primer uso, para evaluar si es necesario o si otros medios de soporte de los procesos empresariales correspondientes (p. ej., transición a un servicio gestionado) pudieran ser mucho más eficientes y/o plantearían un menor riesgo que mantener una EUDA. El procedimiento de justificación de una EUDA se llevará a cabo en la primera fase de creación de una EUDA (es decir, antes del primer uso) y se repetirá periódicamente en lo sucesivo. Los resultados y las pruebas del procedimiento de justificación se conservarán y notificarán a Barclays antes del primer uso de la EUDA y siempre que se vuelva a realizar el procedimiento a partir de ese momento.	Al someter una EUDA a un procedimiento de justificación, el Proveedor tiene la oportunidad de evaluar si la EUDA es realmente necesaria.
Objetivos del control de las EUDA	10. Registro de las EUDA	Se realizará un inventario de las EUDA a fin de aportar transparencia sobre el número completo de EUDA existentes para el Proveedor, así como para recopilar los principales atributos que respalden las disposiciones de este Anexo. Se documentará e implantará un proceso para garantizar la existencia de un inventario completo, fiable y actualizado de las EUDA. El inventario de las EUDA	La integridad del inventario de las EUDA es fundamental para asegurar la debida seguridad y operatividad de las EUDA.

		se revisará, como mínimo, cada año a fin de mantener la exactitud y comprobar su integridad.	
Objetivos del control de las EUDA	11. Acceso	Se restringirá el acceso a los datos y a la lógica empresarial de todas las EUDA, limitándolo a los usuarios pertinentes que dispongan de los derechos de acceso adecuados. Se revisará el acceso utilizando un enfoque basado en el riesgo.	Se aplicarán controles de acceso adecuados para proteger a las EUDA contra el acceso no autorizado, inadecuado o imposible de atribuir a alguien en concreto.
Objetivos del control de las EUDA	12. Disponibilidad	Se implementarán controles para asegurar que las EUDA estén disponibles en línea con los requisitos acordados con Barclays.	La disponibilidad de las EUDA garantiza la continua operatividad de los procesos comerciales.
Objetivos del control de las EUDA	13. Gestión de cambios	Tras introducir un cambio, la observancia de los principios de gestión de cambios garantiza que las EUDA sigan funcionando según lo previsto tras los cambios en la lógica empresarial. Los cambios en la lógica empresarial de las EUDA o los datos estáticos clave no provocarán errores en la notificación o producción. Los usuarios de las EUDA solo podrán tener acceso a las versiones relevantes de las EUDA para uso operativo. La integridad y precisión de los datos de entrada, cálculos y datos de salida se validarán a través de pruebas (automáticas o manuales) para garantizar que cualquier cambio aplicado genere el resultado esperado. Se identificarán y acordarán con Barclays los pasos de las pruebas para cada EUDA con una calificación de media o alta en la evaluación de criticidad de las EUDA, para garantizar que los cambios no provocan errores de información. Las versiones de archivos no se guardarán en el mismo lugar que las versiones de producción. El Proveedor deberá designar a una segunda persona para que respalde el uso y mantenimiento continuo de las EUDA en ausencia del usuario(s) principales.	Es fundamental que se lleve a cabo una gestión del cambio adecuada para que las EUDA continúen funcionando según lo previsto después de cualquier cambio.

Objetivos del control de las EUDA	14. Requisito de documentación	El conocimiento de los datos de entrada, cálculos, datos de salida y la capacidad de modificarlos, no se limitará a una sola persona. Además, existirá documentación suficiente que pueda ser usada por una persona debidamente cualificada específicamente en EUDA para modificarlas y mantenerlas.	Dado que las EUDA son gestionadas por usuarios finales, es importante garantizar un nivel suficiente de documentación de las EUDA para que se puedan transmitir los conocimientos y minimizar así la pérdida de conocimientos.

Apéndice A: Definiciones utilizadas por Barclays

Definiciones	
EUDA	Las EUDA son aplicaciones y herramientas creadas, utilizadas y gestionadas por los usuarios finales. Se desarrollan normalmente usando software de escritorio estándar (más habitualmente, Microsoft Excel o Access) y otros tipos de bases de datos, consultas, macros, scripts, herramientas de reporting, archivos ejecutables y paquetes de códigos. Las EUDA realizan o forman parte de un proceso empresarial continuo (no de uso único) en el que si los cálculos o los resultados fueran imprecisos, no estuvieran disponibles, estuvieran desfasados o sufrieran algún daño, podría tener una repercusión económica, normativa o para la reputación del Banco o podrían causar algún perjuicio a los clientes.

Apéndice B: Requisitos mínimos de control

La aplicabilidad de cada control viene determinada por la tabla siguiente (O = Opcional y I = Imperativo):

Título del control	Valoración de la criticidad de las EUDA			
	Muy baja	Baja	Media	Alta
1. Funciones y Responsabilidades	I	I	I	I
2. Notificación de los riesgos de la información	I	I	I	I
3. Supervisión continua	I	I	I	I
4. Cumplimiento de los requisitos legislativos y normativos locales	I	I	I	I
5. Educación y sensibilización sobre las EUDA	I	I	I	I
6. Identificación de las EUDA	I	I	I	I
7. Evaluación de la criticidad de las EUDA	I	I	I	I
8. Requisitos mínimos de control basados en la criticidad de las EUDA	I	I	I	I
9. Justificación de las EUDA	I	I	I	I
10. Registro de las EUDA	O	I	I	I
11. Acceso	O	I	I	I
12. Disponibilidad	O	O	I	I
13. Gestión del cambio	O	O	I	I
14. Requisito de documentación	O	O	O	I

Apéndice C. Evaluación de criticidad de las EUDA

La evaluación de criticidad de las EUDA consta de dos subevaluaciones; los usuarios principales de las EUDA completarán ambas subevaluaciones para determinar su criticidad.

- Una evaluación de la importancia de las EUDA para Barclays.
- Una evaluación de la probabilidad de errores de las EUDA.

La importancia de toda EUDA individual se define como la máxima calificación alcanzada en los criterios que se enumeran a continuación.

Importancia de las EUDA Criterio1	**Calificación de la importancia de las EUDA**			
	Baja	**Moderada**	**Alta**	**Excepcional**
1) ¿Admite la EUDA actividades críticas que tienen un impacto normativo (equivalente a activos ponderados por riesgo (RWA) o repercusión directa de las EUDA en la exposición?	<50M GBP	≥ 50M GBP ≤ 500M GBP	>500M GBP ≤ 1000M GBP	> 1000M GBP
2) ¿Tiene el producto de la EUDA un impacto en los informes financieros)?	Impacto PyG < 1M GBP Impacto BS < 1000M GBP	Impacto PyG ≥ 1M GBP < 10M GBP Impacto BS ≥ 1000M GBP < 2000M GBP	Impacto PyG ≥ 10M GBP < 50m GBP Impacto BS ≥ 2000M GBP ≤ 3000M GBP	Impacto PyG ≥ 50M GBP Impacto BS > 3000 M GBP
3) Si la información, los cálculos, los resultados de la EUDA son inexactos, obsoletos o corruptos, ¿cuál sería el impacto **probable** en los clientes del banco2?	Clientes afectados < 100 Pérdida total de clientes < 1M GBP	Clientes afectados ≥ 100 < 1000 Pérdida total de clientes ≥ 1M GBP < 10M GBP	Clientes afectados ≥ 1000 < 10000 Pérdida total de clientes ≥ 10M GBP < 50M GBP	Clientes afectados ≥ 10000 < 50000 Pérdida total de clientes ≥ 50M GBP
4) Si la información, los cálculos, los productos de la EUDA son inexactos, obsoletos o corruptos, ¿cuál sería el impacto **probable** en la reputación del banco?	Se considera que el impacto no sería importante a nivel de la unidad de negocio local. Sin repercusión alguna en la marca ni en la reputación del grupo.	Se considera que el impacto sería manejable a nivel de la unidad de negocio local. Sin impacto alguno en la marca o la reputación del grupo.	Impacto negativo para más de una unidad de negocio o región. Es improbable que afecte a la marca del grupo.	Posible impacto en la marca del grupo.

.

El usuario principal de la EUDA aplicará los siguientes criterios para evaluar su probabilidad de errores. El usuario principal de la EUDA sumará las puntuaciones de los diferentes criterios para calcular la calificación final de probabilidad de errores.

Criterios de probabilidad de errores de las EUDA	Puntuación de probabilidad de errores			
	Uno	**Dos**	**Tres**	**Cuatro**
1) ¿Cuál es la percepción de la EUDA en cuanto a complejidad? (Véase la definición más abajo*)	Rudimentaria	Ligera	Intermedia	Avanzada
2) ¿Cuál es la frecuencia de uso de la EUDA?	Uso inferior a trimestral	Una o más veces al trimestre pero menos de una vez al mes	Una o más veces al mes pero no diariamente	Una o más veces al día
3) ¿Cuál es la frecuencia de cambio de la fórmula o la lógica de la EUDA?	Nunca o con muy poca frecuencia	Se hacen cambios pero de forma excepcional	Cambios periódicos pero no cada vez que se usa la EUDA	Cada vez que se usa la EUDA
4) ¿Cuántos usuarios tiene la EUDA?	Un solo usuario	Varios usuarios del mismo equipo operativo	Varios usuarios de diferentes equipos de una misma unidad de negocio o función	Varios usuarios de diferentes unidades de negocio y/o funciones

*Se refiere a la funcionalidad de la EUDA y se divide en las siguientes categorías:

- **Rudimentaria**: cálculos no importantes en la EUDA, utilizados principalmente como informes de resumen.
- **Ligera:** un revisor con escasos conocimientos de la aplicación puede interpretar la finalidad y efectividad de las fórmulas mediante la observación y sin explicaciones externas.
- **Intermedia**: su funcionalidad es más compleja. Un revisor experto en el uso de la aplicación (por ejemplo, Excel, Access) podría necesitar información adicional para interpretar la finalidad y la efectividad de la EUDA.

- **Avanzada**: alto grado de complejidad y fórmulas avanzadas. Además, puede incluir vínculos a otras hojas de cálculo, bases de datos, sitios web, tablas etc.

La calificación final de probabilidad de errores se calculará aplicando la puntuación total a la siguiente tabla:

Calificación de probabilidad de errores	**Improbable**	**Posible**	**Probable**	**Muy probable**
Puntuación total	≥ 4 < 6	≥ 6 < 9	≥ 9 <12	≥ 12 ≤16

Evaluación de criticidad de las EUDA

El usuario principal de la EUDA combinará las evaluaciones de importancia y probabilidad de errores para determinar la criticidad total de la EUDA. Debe utilizarse la siguiente tabla. El usuario principal de la EUDA debe registrar la evaluación de criticidad de esta en el inventario de EUDA.

Importancia	Excepcional	**Media**	**Media**	**Alta**	**Alta**
	Alta	**Media**	**Media**	**Media**	**Alta**
	Moderada	**Baja**	**Baja**	**Media**	**Media**
	Baja	**Muy baja**	**Muy baja**	**Muy baja**	**Muy baja**
Probabilidad de error		Improbable	Posible	Probable	Muy probable