Obligaciones de control de proveedores externos

EUDA: aplicaciones desarrolladas por usuarios finales

Versión 10.0 con fecha de octubre de 2020

Debe tenerse en cuenta que el término «EUDA», tal y como se menciona a lo largo de este SCO, se aplica solamente a las EUDA identificadas en el árbol de decisiones de EUDA de Barclays y las utilizadas para sustentar 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 las responsabilidades en relación con las EUDA. las cuales se revisarán cuando se introduzca algún cambio importante en la actividad o el modelo operativo del proveedor. Las funciones principales incluirán a un alto ejecutivo que será responsable de las EUDA	Para garantizar el diseño, aplicación y funcionamiento eficaces de controles para las EUDA, es necesario un alto nivel de promoción. Será necesaria una supervisión continua para que la dirección ejecutiva tenga garantías sobre el diseño y funcionamiento de los controles de riesgo de las EUDA.
Gobernanza y garantías	2. Informes sobre el riesgo de las EUDA	Existirán controles y procesos documentados que garanticen la notificación y gestión de los incidentes de riesgo de las EUDA. El proveedor deberá responder a los incidentes de las EUDA, así como a las violaciones de la seguridad de la información, y notificarlo a Barclays inmediatamente. Es necesario establecer un proceso de respuesta a incidentes para tratar y notificar de forma oportuna los errores que afecten a la información de Barclays o a los servicios utilizados por el banco. El proveedor se asegurará de contar con un plan de reparación (acción, persona responsable y fecha de entrega) 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 medirá, revisará y documentará el cumplimiento de este Anexo periódicamente (al menos una vez al año).	

Gobernanza y garantías	4. Respeto por la legislación y las normativas locales	El proveedor se asegurará del cumplimiento de los requisitos legislativos y normativos en materia de EUDA de la jurisdicción en la que opera y de que están debidamente documentados.	*(igual que arriba)*
Gobernanza y garantías	5. Educación y conocimiento de las EUDA	El proveedor deberá identificar a los empleados con responsabilidades relativas a las EUDA. Los empleados a los que se haya asignado una función relativa a las EUDA deben completar la formación en educación y conocimiento correspondiente a su puesto. Este control debe llevarse a cabo una vez al año como mínimo y se deben conservar pruebas que lo demuestren.	
Objetivos de control de EUDA	6. Identificación de las EUDA	Se documentará e implantará un proceso para identificar todas las EUDA propiedad o gestionadas por los proveedores en las que se basen los servicios de Barclays.	La identificación de las EUDA resulta crucial para establecer el nivel de control adecuado que se necesita con respecto a todas esas aplicaciones.
Objetivos de control de EUDA	7. Evaluación de la criticidad de las EUDA	La criticidad de cada EUDA debe evaluarse antes de utilizarse por primera vez en la producción así como después de implementarse cambios en cada EUDA. La evaluación de la criticidad del proveedor debe incluir la consideración de elementos como el impacto normativo, financiero y para la reputación en el servicio que el proveedor presta a Barclays. La evaluación de la criticidad debe tener en cuenta también la relevancia y probabilidad de error. Consulte el Apéndice C En términos de relevancia, los criterios relevantes incluyen los siguientes: • ¿Se basan en EUDA actividades críticas vinculadas al producto/servicio que se ofrece a Barclays? • ¿Pueden los resultados de las EUDA tener un impacto económico en Barclays? • ¿Pueden verse negativamente afectados los clientes de Barclays si la información o los resultados de las EUDA fueran imprecisos, obsoletos o corruptos?	La comprensión de la criticidad de las EUDA puede permitir a nuestro proveedor determinar e implementar el nivel apropiado de controles para las EUDA.

		En términos de probabilidad de error, los criterios relevantes incluyen los siguientes: • La complejidad percibida de la EUDA (sin cálculos significativos hasta un nivel alto de fórmulas complejas y avanzadas); • Frecuencia de uso; • La frecuencia de los cambios en la fórmula/lógica de la EUDA; y • Número de usuarios. La criticidad de las EUDA deberá acordarse con Barclays.	
Objetivos de control de EUDA	8. Requisitos mínimos de control basados en la criticidad de las EUDA	El proveedor implantará controles que satisfagan los objetivos en cuanto a requisitos de control basándose en el nivel de criticidad acordado con Barclays. Los objetivos de control que se han marcado con una "I" en este Anexo son imperativos. Todos los demás objetivos en cuanto a controles son solo opcionales ("O"). Para consultar la tabla de controles, véase el apéndice B. Cuando proceda, se conservarán pruebas que demuestren la consecución de los objetivos en cuanto a controles aplicables.	Se aplicará el nivel de control correcto en consonancia con el riesgo que representen las EUDA, para evitar un control excesivo de una EUDA de riesgo inferior.
Objetivos de control de EUDA	9. Justificación de las EUDA	Cada EUDA debe someterse a un procedimiento de justificación antes de utilizarse por primera vez para evaluar si es necesaria o si medios alternativos de soporte del proceso empresarial vinculado (por ejemplo, transición a un servicio gestionado) resultarían más eficientes y/o plantearían un riesgo menor que mantener una EUDA. El procedimiento de justificación de las EUDA debe aplicarse cuando se crea inicialmente una EUDA (es decir, antes de su primer uso) y volver a ejecutarse periódicamente con posterioridad. Los resultados y las evidencias del procedimiento de justificación deben conservarse y notificarse a Barclays antes de utilizar la EUDA por primera vez y siempre que se ejecute el proceso posteriormente.	Al ejecutar un procedimiento de justificación de una EUDA, el proveedor tiene la oportunidad de evaluar si esta es realmente necesaria.
Objetivos de control de EUDA	10. Registro de la EUDA	Existirá un inventario de EUDA a efectos de transparencia sobre el número total de EUDA del proveedor, además de reseñar los atributos fundamentales para cumplir las disposiciones del presente Anexo.	Resulta fundamental contar con un inventario de las EUDA completo para garantizar su correcta seguridad y funcionamiento.

		Se documentará e implantará un proceso para garantizar la existencia de un inventario completo, exacto y actualizado de las EUDA. Este inventario de EUDA se revisará, como mínimo, cada año para mantener la exactitud y comprobar que está completo.	
Objetivos de control de EUDA	11. Acceso	Se restringirá el acceso a los datos y a la lógica de negocio de todas las EUDA, limitándolo a los usuarios pertinentes que dispongan de los derechos de acceso adecuados. Se revisará el acceso usando un planteamiento basado en el riesgo.	Unos controles de acceso adecuados protegen las EUDA contra accesos no autorizados, inadecuados o imposibles de atribuir a alguien concreto.
Objetivos de control de EUDA	12. Disponibilidad	Se implantarán controles para garantizar que las EUDA estén disponibles de acuerdo a los requisitos acordados con Barclays.	La disponibilidad de las EUDA garantiza un funcionamiento continuo de los procesos comerciales.
Objetivos de control de EUDA	13. Gestión de cambios	Si se respetan los principios de gestión de cambios, se garantiza que las EUDA funcionen según lo previsto después de introducir cambios en la lógica de negocio. Los cambios en la lógica de negocio de las EUDA o en los datos estáticos básicos no provocarán errores en los informes ni en las salidas generadas por los sistemas. Los usuarios de las EUDA solo deben poder acceder a las versiones relevantes de estas para su uso operativo. La integridad y precisión de los datos de entrada, los cálculos y los datos de salida se validan a través de pruebas (automatizadas y/o manuales) para garantizar que los cambios aplicados han producido el resultado previsto. Los pasos de las pruebas deben identificarse y acordarse con Barclays para cualquier EUDA con una valoración de media a alta en la evaluación de criticidad de las EUDA con el fin de garantizar que los cambios no den lugar a errores de información. Las versiones de archivo no deben guardarse en el mismo lugar que las de producción. El proveedor designará a una persona secundaria para prestar apoyo al uso y mantenimiento continuados de la aplicación cuando no esté disponible el usuario principal.	Para que la EUDA siga funcionando según lo previsto tras introducir un cambio, resulta esencial gestionar correctamente los cambios

Objetivos de control de EUDA	14. Requisito de documentación	No será una única persona quien conozca los datos de entrada, los cálculos y los datos de salida o quien posea la capacidad para modificarlos. Asimismo, existirá documentación suficiente que pueda ser utilizada por una persona específica experta en el uso de la EUDA para modificar y mantener la aplicación.	Puesto que las EUDA son gestionadas por usuarios finales, es importante que exista una documentación adecuada para garantizar que se mantiene información crítica relativa a las EUDA con el fin de permitir la transmisión del conocimiento y minimizar las posibilidades de pérdida de conocimientos.

Apéndice A. Definiciones empleadas por Barclays

Definiciones	
EUDA	Las EUDA son aplicaciones y herramientas creadas, usadas y gestionadas por los usuarios finales. Suelen desarrollarse utilizando software estándar (con mayor frecuencia, Microsoft Excel o Access) y otros tipos de bases de datos, consultas, macros, scripts, herramientas de generación de informes, archivos ejecutables y paquetes de código. Las EUDA realizan o forman parte de un proceso de negocio continuo (no de uso único) en el que si los cálculos o los datos de salida fueran imprecisos, no estuvieran disponibles, estuvieran desfasados o sufriesen algún daño, podría tener una repercusión económica, reglamentaria o para la reputación del Banco o podrían causar algún perjuicio a un cliente del banco.

Apéndice B: Requisitos mínimos de control

La aplicabilidad de cada control se determina de acuerdo con la siguiente tabla (O = Opcional y M = Obligatorio):

Título del control	Valoración de la criticidad de las EUDA			
	Muy bajo	Bajo	Medio	Alto
1. Funciones y responsabilidades	I	I	I	I
2. Informes sobre el riesgo de las EUDA	I	I	I	I
3. Supervisión continua	I	I	I	I
4. Respeto por la legislación y las normativas locales	I	I	I	I
5. Educación y conocimiento de 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 la EUDA	O	I	I	I
11. Acceso	O	I	I	I
12. Disponibilidad	O	O	I	I
13. Gestión de cambios	O	O	I	I
14. Requisito de documentación	O	O	O	I

Apéndice C: Evaluación de la criticidad de las EUDA

La evaluación de la criticidad de las EUDA contiene dos subevaluaciones; los usuarios principales de las EUDA deben completar ambas para determinar la criticidad de las mismas.

- Una evaluación de la relevancia de la EUDA para Barclays.
- Una evaluación de la probabilidad de error de la EUDA.

La relevancia de las EUDA individuales se define como la máxima valoración alcanzada a partir de los criterios que siguen

Relevancia de la EUDA Criterios1	**Valoración de la relevancia de las EUDA**			
	Bajo	**Moderado**	**Alto**	**Excepcional**
1) ¿Sustenta la EUDA actividades críticas que tengan un impacto normativo (activos ponderados al riesgo (RWA) equivalentes o exposición directamente afectada por la EUDA)?	<50 M de £	≥ 50 m de £ ≤ 500 m de £	>500 m de £ ≤ 1000 m de £	>1000 m de £
¿Pueden los resultados de las EUDA tener un impacto en los informes financieros?	Impacto en pérdidas y ganancias < 1 m de £ Impacto comercial < 1000 m de £	Impacto en pérdidas y ganancias ≥ 1 m de £ < 10 m de £ Impacto comercial ≥ 1000 m de £ < 2000 m de £	Impacto en pérdidas y ganancias ≥ 10 m de £ < 50 m de £ Impacto comercial ≥ 2000 m de £ ≤ 3000 m de £	Impacto en pérdidas y ganancias ≥ 50 m de £ Impacto comercial > 3000 m de £
3) Si la información, los cálculos o los resultados de la EUDA fueran imprecisos, obsoletos o corruptos, ¿cuál sería el impacto **probable** en los clientes del banco?	Clientes afectados < 100 Pérdidas totales de los clientes < 1 M de £	Clientes afectados ≥ 100 < 1000 Pérdidas totales de los clientes ≥ 1 M de £< 10 M de £	Clientes afectados ≥ 1000< 10000 Pérdidas totales de los clientes ≥ 10 M de £ < 50 M de £	Clientes afectados ≥ 10000 < 50000 Pérdidas totales de los clientes ≥ 50 M de £
4) Si la información, los cálculos o los resultados de la EUDA fueran imprecisos, obsoletos o corruptos, ¿cuál sería el impacto **probable** en la reputación del banco?	Impacto considerado no sustancial a escala de unidad de negocio local. Sin impacto en la marca o la reputación del Grupo.	Impacto considerado gestionable a escala de unidad de negocio local. Sin impacto en la marca o la reputación del Grupo.	Impacto negativo en más de un negocio/región. Impacto poco probable en la reputación del Grupo.	Impacto probable en la marca del Grupo.

El usuario primario de la EUDA debe utilizar los siguientes criterios para evaluar la probabilidad de error de la EUDA. El usuario primario de la EUDA debe sumar las puntuaciones de todos los criterios para calcular la valoración definitiva de la probabilidad de error.

Criterios de probabilidad de error de la EUDA	Valoración de la probabilidad de error			
	Uno	**Dos**	**Tres**	**Cuatro**
1) ¿Cuál es la complejidad percibida de la EUDA? (véase la definición que sigue*)	Rudimentaria	Baja	Intermedia	Avanzada
2) ¿Cuál es la frecuencia de uso de la EUDA?	Uso inferior al trimestral	Una vez o más por trimestre pero menos de una vez al mes	Una vez o más por mes pero no diariamente	Una vez o más por día
3) ¿Cuál es la frecuencia de los cambios de fórmula/lógica en la EUDA?	Nunca o con muy poca frecuencia	Se realizan cambios pero de forma excepcional	Cambios regulares pero no cada vez que se emplea la EUDA	Cada vez que se emplea la EUDA
4) ¿Cuántos usuarios tiene la EUDA?	Usuario único	Múltiples usuarios en el mismo equipo operativo	Múltiples usuarios en diferentes equipos dentro de una BU o función	Múltiples usuarios en diferentes BU o funciones

*Se refiere a la funcionalidad de la EUDA y se categoriza como sigue:

- **Rudimentaria** – Sin cálculos significativos en la EUDA. Se emplea principalmente como informes resumidos.
- **Baja** – Un revisor con conocimientos limitados de la aplicación es capaz de interpretar el objetivo y efectividad de la fórmula a través de la observación y sin explicaciones externas.
- **Intermedia** – Tiene una funcionalidad más compleja Un revisor que domine el uso de la aplicación (como Excel, Access) podría necesitar información adicional para interpretar el objeto y efectividad de la EUDA.
- **Avanzada** – Nivel elevado de complejidad y fórmulas avanzadas. Puede vincular también otras hojas de cálculo, bases de datos, sitios web, tablas, etc.

La valoración definitiva de probabilidad de error debe calcularse empleando la puntuación total según esta tabla:

Puntuación de la probabilidad de error	**Poco probable**	**Posible**	**Probable**	**Muy probable**
Puntuación total	**≥** 4 < 6	**≥** 6 < 9	**≥** 9 <12	**≥** 12 **≤**16

Evaluación de la criticidad de las EUDA

El usuario primario de la EUDA debe combinar las evaluaciones de relevancia y la probabilidad de error para determinar la criticidad total de la EUDA. Deberá emplearse la tabla que sigue. El usuario primario de la EUDA debe consignar la evaluación de la criticidad debe consignarse en el inventario de EUDA.

Relevancia	Excepcional	**Medio**	**Medio**	**Alto**	**Alto**
	Alto	**Medio**	**Medio**	**Medio**	**Alto**
	Moderado	**Bajo**	**Bajo**	**Medio**	**Medio**
	Bajo	**Muy bajo**	**Muy bajo**	**Muy bajo**	**Muy bajo**
Probabilidad de error		Poco probable	Posible	Probable	Muy probable