Obligaciones de control de proveedores externos

Riesgo tecnológico

Versión 11.0 con fecha de octubre de 2021

Área de control	Título del control	Descripción del control	Por qué es importante
1. Gestión de la obsolescencia	Garantizar medidas de apoyo permanentes	El proveedor informará de inmediato a Barclays de los cambios conocidos en su capacidad para prestar servicios de asistencia técnica, ya sean directos o indirectos, para los activos informáticos utilizados para prestar los servicios a Barclays, incluso cuando los productos presenten aspectos de seguridad vulnerables. Asimismo, se asegurará de actualizar o retirar dichos activos cuando proceda.	Los registros y/o procedimientos inadecuados sobre activos de hardware y software que van a dejar de contar con un servicio de asistencia técnica o los servicios tecnológicos que pasarán a depender de hardware o software desfasado podrían generar un funcionamiento, inestabilidad, seguridad o vulnerabilidad inaceptables, así como una pérdida de negocio y costes de migración excesivos.
2. Gestión de incidentes	Grabación, clasificación y resolución de incidentes	El proveedor implantará un régimen de gestión de incidentes en relación con el funcionamiento de sus sistemas y servicios informáticos, garantice que se identifiquen, registren, prioricen, clasifiquen y resuelvan de inmediato al primer contacto o remitiéndolos oportunamente a quien corresponda. Esto incluirá un proceso solvente para tratar de manera inmediata y eficaz los incidentes más importantes.	Los incidentes tecnológicos no comunicados a tiempo o de manera no suficientemente pormenorizada, o si no se toma la medida correctiva necesaria, podrían generar una interrupción del servicio o los sistemas evitable o una pérdida o corrupción de los datos. Los incidentes más importantes exigen una respuesta más amplia y urgente, ya que constituyen un riesgo importante para la empresa y pueden tener graves consecuencias, como cortes importantes en el servicio, daños a la reputación, una repercusión económica y un impacto en los procesos empresariales centrales.
3. Gestión de problemas	Identificación, evaluación/análisis y resolución de problemas tecnológicos	El proveedor contará con un régimen de investigación puntual de los problemas subyacentes a incidentes tecnológicos importantes, que garantice la identificación y el registro de dichos problemas mediante un análisis de su raíz, así como su resolución eficaz para reducir al mínimo la probabilidad de que el incidente se repita y la repercusión que eso tendría. El proveedor también debería garantizar que se realice un análisis proactivo de los incidentes rutinarios para identificar y resolver la causa de incidentes habituales y reiterados de alto volumen.	Si no se identifican y resuelven puntualmente los problemas que generan incidentes que influyen en la prestación de servicios tecnológicos, se puede producir una interrupción del servicio/los sistemas evitable o una pérdida o corrupción de los datos.

4. Gestión de cambios	Aplicación de rigurosos controles de cambios	El proveedor se asegurará de que todos los componentes informáticos que se utilicen para prestar servicios a Barclays se gestionen de acuerdo a un riguroso régimen de control de los cambios, que tenga plenamente en cuenta los siguientes objetivos: 1. No se efectuará ningún cambio sin la pertinente autorización o aprobación previa a su introducción 2. La separación de las obligaciones de iniciar, aprobar y ejecutar el cambio entre diferentes personas 3. La planificación y gestión de los cambios conforme al nivel de riesgo asociado 4. Los cambios tienen debidamente en cuenta la posible repercusión sobre el rendimiento y/o la capacidad de los componentes tecnológicos afectados 5. Los cambios se someten a pruebas técnicas y empresariales pertinentes para el cambio antes de su introducción y se conservan pruebas de ello cuando es necesario 6. Los cambios se probarán después de su aplicación, para garantizar que hayan funcionado correctamente y que no hayan tenido una repercusión imprevista	Los procesos de cambio inadecuados para evitar cambios inapropiados, mal gestionados o no autorizados en los servicios tecnológicos pueden generar interrupciones del servicio, corrupción y pérdida de los datos, errores de procesamiento o fraudes.
5a. Resiliencia tecnológica	Plan de recuperación de sistemas (SRP)	El proveedor debe contar con planes de recuperación de sistemas (SRP) para cada sistema/servicio tecnológico necesario con el fin de ofrecer soporte a la prestación de servicios de categoría de resiliencia 0-3 de Barclays y los objetivos de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) correspondientes. Es preciso revisar la precisión de los planes cada 12 meses. **Nota:** En el caso de los sistemas/servicios tecnológicos con categoría de resiliencia 0-1 diseñados con una configuración	Si los planes de recuperación de sistemas fueran inadecuados o totalmente nulos, podrían registrarse pérdidas inaceptables del servicio tecnológico prestado a la empresa o los clientes tras un incidente. Mantener al día la documentación sobre resistencia y someterla a prácticas garantiza que los planes de recuperación sigan en consonancia con las necesidades empresariales.

		activa/pasiva, la validación del SRP exige que el sistema se mantenga en el entorno recuperado durante un período prolongado y que funcione como BAU para confirmar que todos los elementos operan de forma efectiva. Esto, en efecto, es un evento transversal de producción (PCO)	
5b. Resiliencia tecnológica	Plan de recuperación e integridad de los datos (DIRP)	El proveedor debe contar con planes de recuperación e integridad de los datos (DIRP) para cada sistema/servicio tecnológico necesario con el fin de ofrecer soporte a la prestación de servicios de categoría de resiliencia 0-1 de Barclays. Es preciso revisar la precisión de los planes cada 12 meses.	La pérdida de datos es una de las amenazas más graves a las que nos enfrentamos ya que puede ser fruto de actos maliciosos o fallos del sistema. Es crítico contar con un plan para este escenario y ayuda a identificar y comprender el origen de los datos y las dependencias.
5c. Resiliencia tecnológica	Diversidad del centro de datos	El proveedor debe garantizar que cada sistema/servicio tecnológico necesario para ofrecer soporte a la prestación de servicios de categoría de resiliencia 0-3 de Barclays sea resiliente en todos los centros de datos y esté lo suficientemente separado para reducir el riesgo de que dichos centros se vean afectados simultáneamente por un evento individual.	Los centros de datos deben contar con sistemas de alimentación, enlaces de red, etc. alternativos y estar lo suficientemente separados como para reducir el riesgo de que dichos centros se vean afectados simultáneamente por un evento individual.
5d. Resiliencia tecnológica	Validación de los SRP	El proveedor probará y validará los planes de recuperación de sistemas (SRP) para demostrar que los servicios/sistemas tecnológicos cumplen los requisitos de la categoría de resiliencia 0-3 establecidos Barclays. Para cada sistema/servicio tecnológico necesario para ofrecer soporte a la prestación de servicios de categoría de resiliencia 0-1 de Barclays diseñado con configuración	Los sistemas tecnológicos suministrados por los proveedores pueden afectar a la experiencia de los clientes de Barclays. Asegurar que los proveedores que apoyan las operaciones empresariales de Barclays cuentan con planes de resiliencia adecuados probados es crucial, además de un mandato normativo, para que en Barclays se aplique la adecuada gobernanza en la gestión de nuestros proveedores. La transversalidad de producción (PCO) es un método para validar que la instancia pasiva de los sistemas activos-

		activa/pasiva en medidas de resiliencia, el entorno pasivo debe activarse siguiendo el SRP documentado y utilizarse como entorno de producción BAU durante un tiempo suficiente para demostrar la capacidad y la funcionalidad de integración total (transversalidad de producción). Los requisitos de frecuencia de validación deben contar con el soporte de la categoría de resiliencia asociada, por ejemplo: - Categoría de resiliencia 0: La validación de los SRP debe realizarse cada 12 meses y en el caso de la PCO cada 3 meses - Categoría de resiliencia 1: La validación de los SRP y los PCO debe realizarse cada 12 meses - Categoría de resiliencia 2-3: La validación de los SRP debe realizarse cada 24 meses Si alguna prueba no cumple los requisitos de recuperación mínimos para la categoría de resiliencia correspondiente, el proveedor deberá notificarlo inmediatamente a Barclays y aportar planes de reparación detallados (que incluyan las medidas que se adoptarán y las fechas de finalización correspondientes). El proveedor notificará previamente a Barclays la ejecución de los PCO.	pasivos configurados funciona según lo previsto y con la capacidad necesaria para el funcionamiento BAU. Además, los PCO también validan que cualquier dependencia o sistema ascendente o descendente sigue funcionando según lo previsto.
5e. Resiliencia tecnológica	Validación de los DIRP	El proveedor debe probar y validar los planes de recuperación e integridad de los datos (DIRP) para cada sistema/servicio tecnológico necesario para ofrecer soporte a la prestación de servicios de categoría de resiliencia 0-1 de Barclays con el fin de demostrar la integridad de los datos durante la recuperación. La validación debe llevarse a cabo cada 12 meses. Si algún plan no cumple los requisitos de recuperación mínimos para la categoría de resiliencia correspondiente, el proveedor	Los datos constituyen un elemento crítico que puede verse negativamente afectado de muchas formas. Es preciso ejecutar el plan documentado para restaurar, recuperar o recrear los datos para confirmar que es preciso y viable.

		deberá notificarlo inmediatamente a Barclays y aportar planes de reparación detallados (que incluyan las medidas que se adoptarán y las fechas de finalización correspondientes).	
6. Gestión de capacidad y rendimiento	Adaptación permanente a las necesidades tecnológicas de Barclays	El proveedor definirá niveles adecuados de rendimiento y capacidad respecto a todos los componentes informáticos básicos que se utilicen para prestar servicios a Barclays en consonancia con las necesidades del banco indicadas. También velarán por que se implanten avisos y umbrales apropiados en componentes esenciales, a fin de avisar de posibles superaciones de los umbrales, y por que se revisen periódicamente para garantizar que la prestación del servicio se ajuste a las necesidades de Barclays.	Medidas inadecuadas para supervisar el rendimiento y/o los niveles de capacidad de los recursos informáticos y el hecho de no mantenerlos en consonancia con los requisitos actuales y futuros puede provocar una interrupción y/o reducción inaceptable de los servicios tecnológicos y pérdida de negocio. La definición y/o la documentación inadecuadas de las necesidades de los clientes/comerciales puede provocar un rendimiento inaceptable de los servicios tecnológicos y pérdida de negocio.

Área de control	Título del control	Descripción del control	Por qué es importante
7. Desarrollo de aplicaciones tecnológicas	Aplicación de controles de calidad repetibles	El proveedor se asegurará de que se pueda demostrar que todos los servicios y sistemas informáticos que utilice para prestar los servicios a Barclays se han sometido a procesos de control de calidad rigurosos, completos y repetibles, incluidos entre otros pruebas funcionales y no funcionales, pruebas estáticas de seguridad de las aplicaciones y controles de calidad del código, ya sea a través de una revisión por homólogos o de herramientas automatizadas.	Los servicios y sistemas que no cuenten con un control de calidad suficiente y no se hayan probado debidamente pueden dar lugar a pérdidas críticas impredecibles de funcionalidad en procesos empresariales y servicios tecnológicos.
	Aceptación de los resultados empresariales	El proveedor acordará de forma puntual o permanente definiciones de resultados empresariales aceptables para ambas partes, según las cuales se suministrarán a Barclays nuevas versiones o versiones actualizadas de los servicios y sistemas informáticos, y Barclays las aceptará.	La aceptación insuficiente del comportamiento funcional y no funcional de un sistema puede provocar una desviación del comportamiento del sistema de Barclays esperado y generar un riesgo para los procesos operativos y empresariales.

		El formato de dichas definiciones incluirá aspectos funcionales y no funcionales suficientes de los sistemas y servicios, y podrá adoptar cualquier forma pertinente establecida de mutuo acuerdo, como los manuales de sistema existentes, la documentación pormenorizada sobre requisitos estipulados de mutuo acuerdo, casos de los usuarios, ejemplos de uso u otro formato apropiado. El proveedor colaborará con Barclays para garantizar que los resultados empresariales, pactados de mutuo acuerdo total o parcialmente, sean aceptados de manera puntual o permanente basándose en la aceptación empresarial por parte de Barclays de estas definiciones previamente acordadas.	
8. Métodos de respaldo y copia de seguridad de sistemas y datos	Uso de procesos pertinentes y eficaces de copia de seguridad y restauración	El proveedor se asegurará de que todos los servicios y sistemas informáticos utilizados en la prestación de servicios a Barclays cuenten con procesos de copia de seguridad y restauración adecuados que funcionen conforme a las necesidades de Barclays y cuya eficacia se demuestre periódicamente.	Si los métodos de copia de seguridad de los datos empresariales están mal controlados o si no se controlan en absoluto, podría tener lugar una alteración del servicio o de los sistemas, una pérdida de datos o una filtración de datos inadecuada.
	Garantía de soportes seguros y fiables para las copias de seguridad	El proveedor se asegurará de que todos los soportes para copias de seguridad vinculados a la prestación de servicios a Barclays, así como los sistemas de gestión y almacenamiento de dichos soportes, sigan siendo seguros y fiables en todo momento.	Si los métodos de copia de seguridad de los datos empresariales están mal controlados o si no se controlan en absoluto, podría tener lugar una alteración del servicio o de los sistemas, una pérdida de datos o una filtración de datos inadecuada.
9. Gestión de la configuración	Aislamiento del entorno de producción	El proveedor se asegurará de que los servicios de producción prestados a Barclays no dependan de ningún componente no productivo, a fin de evitar una falta de seguridad o fiabilidad en la prestación del servicio.	Un registro inadecuado de los componentes tecnológicos (hardware y software), incluida la responsabilidad definida y las dependencias de terceros, puede dar lugar a unos servicios y datos que no sean seguros o fiables. El uso de componentes no productivos para prestar servicios de producción genera un riesgo, puesto que podrían no haberse construido de acuerdo a las normas de producción o no gestionarse de conformidad con estas.

	Mantenimiento y registro de datos de configuración	El proveedor mantendrá un registro exacto y completo de todos los elementos de configuración dentro de este ámbito que se utilicen para prestar servicios a Barclays (lo que incluye las responsabilidades y las dependencias o asignaciones superiores o inferiores). El proveedor implantará controles para garantizar el mantenimiento continuado de la precisión e integridad de los datos.	Un registro (junto con dependencias o asignaciones relacionadas con otros elementos de la configuración) de carácter inadecuado o incompleto puede provocar inseguridad o inestabilidad en los servicios y los datos a consecuencia de una evaluación ineficaz del impacto de cambios e incidentes.
10. Gestión de activos de hardware	Registro y mantenimiento de datos de activos de hardware	El proveedor implantará controles para garantizar el registro y mantenimiento continuado de los datos de los activos de hardware durante todo su ciclo de vida. El proveedor mantendrá un registro exacto y completo de todos los activos de hardware informático que se utilicen para prestar servicios a Barclays.	Un registro inadecuado de los activos de hardware tecnológicos, incluida la responsabilidad definida y las dependencias de terceros, puede dar lugar a unos servicios y datos que no sean seguros o fiables. Si los activos de hardware no se limpian y retiran de manera segura, podrían producirse daños económicos, normativos y para la reputación.
	Retirada de activos	Se eliminarán todos los datos de Barclays de los activos que se retiren y se destruirán de forma segura mediante un proceso forma de eliminación acorde a las exigencias de las normas de seguridad pertinentes de Barclays.	Es crítico que el proveedor obtenga y registre la confirmación formal de que el activo se ha retirado de manera correcta (incluida la destrucción segura de los datos bancarios). Si los activos de hardware no se limpian y retiran de manera segura, podrían producirse daños económicos, normativos y para la reputación.
	Activos faltantes	Todos los activos 'perdidos o robados' deben investigarse correctamente y declararse a Barclays para que apruebe el riesgo si no se encuentran.	Es crítico que el proveedor haya aplicado controles para garantizar que los activos ausentes se han investigado en profundidad y, si no se han encontrado, que se han declarado a Barclays para que consigne el riesgo. Si los activos de hardware se han perdido y, por tanto, no se limpian y retiran de manera segura, podrían producirse daños económicos, normativos y para la reputación.

Área de control	Título del control	Descripción del control	Por qué es importante
11. Gestión de activos de software	Registro y mantenimiento de datos de instalación/activos de software. Licencias de activos de software	El proveedor mantendrá un registro exacto y completo de todos los activos de software dentro de este ámbito, y de sus instalaciones, que se utilicen para prestar servicios a Barclays (lo que incluye las responsabilidades). El proveedor mantendrá la exactitud e integridad de los datos desde su adquisición hasta su retirada (y desde su instalación o desinstalación). El proveedor se asegurará además de que el uso del software se ajuste a las condiciones de la licencia definida.	Un registro inadecuado de los activos de software tecnológicos, incluida la responsabilidad definida puede dar lugar a servicios y datos que no sean seguros o fiables. Si el uso del software no se gestiona conforme a los derechos otorgados sobre el mismo, podrían producirse daños económicos, normativos y para la reputación.

Definiciones de resiliencia tecnológica:

Objetivo de tiempo de recuperación	se refiere al periodo de tiempo entre un fallo o interrupción imprevisto de los servicios y la reanudación de las operaciones.

Objetivo de punto de recuperación (RPO)	se refiere al estado del objetivo de disponibilidad de los datos al inicio del proceso de recuperación. Constituye una medida de la pérdida máxima de datos que puede tolerarse en una situación de recuperación.
Transversalidad de producción	se refiere al acto de activar una instancia alternativa (DR) para los sistemas diseñados con configuración activa-pasiva y utilizarlos como instancia de producción durante un período prolongado para validar su plena funcionalidad y capacidad.
Plan de recuperación de sistemas	se trata de un documento que define los elementos técnicos y detalla cómo recuperar un sistema o un componente fallido para devolverlo a su estado operativo.
Plan de recuperación e integridad de los datos	se trata de un documento que detalla los pasos que deben darse para recuperar datos perdidos como consecuencia de un fallo de sistema o un acto malicioso. El plan debe incluir escenarios con opciones relevantes (por ejemplo, recuperación de datos desde otros sistemas, restauración de datos desde archivos en cintas o recreación de datos).

Requisitos de resiliencia de Barclays por matriz de categorías de resiliencia

Categoría de resistencia	0	1	2	3
Objetivo de tiempo de recuperación	Hasta un máximo de 5 minutos	Hasta un máximo de 4 horas	Hasta un máximo de 12 horas	Hasta un máximo de 24 horas
Objetivo de punto de recuperación (RPO)	Hasta un máximo de 5 minutos	Hasta un máximo de 15 minutos	Hasta un máximo de 30 minutos	Hasta un máximo de 24 horas