Obligaciones de control de proveedores externos

Planificación de la recuperación

Versión 13.0 Septiembre de 2023

1. Definiciones:

«Evento de interrupción»	Registro de los impactos de los incidentes, independientemente de la causa, que los proveedores han decidido mitigar mediante la implementación de la planificación y las capacidades de recuperación y resiliencia.
«**Incidente**»	Se refiere a un acontecimiento que supone un trastorno y que se pueda gestionar como parte de las operaciones rutinarias, mediante la aplicación de planes de recuperación.
«Plan de recuperación»	Los planes de recuperación son documentos que detallan los pasos y las acciones que han de realizarse para restaurar la operatividad de un servicio. Estos planes de recuperación se pueden denominar plan de continuidad empresarial o recibir una nomenclatura similar.
«**Planificación de la recuperación**»	Proceso o planificación para la recuperación de los servicios empresariales, el proceso empresarial y las dependencias subyacentes.
«**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.
«Categoría de resiliencia»	La categoría de resiliencia es una calificación que utiliza Barclays para aplicar requisitos de resiliencia a un servicio. La categoría de resiliencia determina el objetivo del tiempo de recuperación (RTO), el objetivo del punto de recuperación (RPO) y el requisito de la frecuencia de validación.

2. Matriz de criticidad de la resiliencia:

Barclays asigna los servicios del proveedor a una categoría de resiliencia específica (0-4), que refleja el impacto que puede causar una interrupción del servicio en Barclays. Una categoría de resistencia superior (es decir, un número inferior) exigirá un nivel superior de resistencia o recuperación, en proporción a la importancia del servicio. El proveedor se asegurará de que sus servicios alcancen el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) que se especifican a continuación con respecto a la categoría de resiliencia aplicable indicada por Barclays para los servicios contratados: La siguiente tabla especifica qué controles del proveedor son aplicables en función de la categoría de resiliencia definida, y los detalles de dichos controles se establecen en la sección 3 (*Controles*) a continuación.

Evaluación del impacto de los riesgos	Impacto excepcional	Impacto alto	Impacto moderado	Impacto bajo	Impacto insignificante
Categoría de resiliencia	0	1	2	3	4
Objetivo de RTO	Hasta un máximo de 1 hora	Hasta un máximo de 4 horas	Hasta un máximo de 12 horas	Hasta un máximo de 24 horas	No hay recuperación planificada
Objetivo de 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	No hay recuperación planificada
Frecuencia de pruebas de tecnología	Categoría de resiliencia 0	Categoría de resiliencia 1	Categoría de resiliencia 2	Categoría de resiliencia 3	Categoría de resiliencia 4
Validación del plan de recuperación de sistemas	Mínimo dos veces al año	Mínimo dos veces al año	Mín. cada 12 meses	Mín. cada 24 meses	No hay recuperación planificada
Validación del plan de recuperación de datos	Validación anual del plan en un entorno similar al de producción	Validación anual a través de un tutorial de escritorio	Opcional	Opcional	No hay recuperación planificada
Validación de plan de reconstrucción de plataformas y aplicaciones	Validación anual a través de un tutorial de escritorio	Validación anual a través de un tutorial de escritorio	Opcional	Opcional	No hay recuperación planificada

Aplicabilidad de controles del proveedor	Categoría de resiliencia 0	Categoría de resiliencia 1	Categoría de resiliencia 2	Categoría de resiliencia 3	Categoría de resiliencia 4
1. Requisitos de mapeo de dependencias para su inclusión en la planificación de la recuperación	✔	✔	✔	✔	O
2. Eventos que suponen un trastorno para los requisitos de planificación de la recuperación	✔	✔	✔	✔	O
3. Requisito de validación y planificación de la recuperación	✔	✔	✔	✔	O
4. Requisito de pruebas integradas	✔	✔	O	O	O
5. Requisito de validación y planes de recuperación de sistemas	✔	✔	✔	✔	O
6. Requisito de validación y planes de recuperación de datos	✔	✔	O	O	O
7. Requisito del proveedor de servicios en la nube y diversidad en el centro de datos	✔	✔	✔	✔	O
8. Requisito de los planes de reconstrucción de plataformas y aplicaciones	✔	✔	O	O	O

✔ = obligatorio	O = opcional

Si se identifica algún problema durante la revisión o el incumplimiento de los requisitos durante la prueba de los controles, el proveedor debe informar a Barclays de inmediato (normalmente en un plazo de 10 días) y solucionar los problemas en un plazo acordado.

3. Controles:

El proveedor debe adoptar un enfoque estructurado de la resiliencia (continuidad del negocio y recuperación ante desastres) respaldado por un documento de políticas y estándares que rija los requisitos de resiliencia operativa y técnica de acuerdo con las prácticas recomendadas del sector y los requisitos normativos, según corresponda. El enfoque estructurado de la resiliencia debe ser supervisado por la dirección ejecutiva y revisado y probado anualmente para determinar su eficacia.

Título del control	Descripción del control	Por qué es importante
1. Requisitos de mapeo de dependencias para su inclusión en la planificación de la recuperación	El proveedor debe definir y documentar las dependencias que son fundamentales para prestar el servicio a Barclays. Estas dependencias deben mantenerse y revisarse cada 12 meses o cuando se produzca un cambio significativo. Las dependencias a tener en cuenta son: ▪ Tecnología y datos (proporcionados por el subcontratista e internos). ▪ Subcontratistas de materiales (que podrían tener un impacto material en el rendimiento y la prestación del servicio a Barclays). ▪ Personal (pérdida de personas; considere la posibilidad de no tener una estrategia de recuperación del área de trabajo o capacidad de trabajar desde el domicilio).	Los proveedores de servicios deben conocer las dependencias para prestar su servicio a Barclays. Todas las dependencias formarán parte de su plan de recuperación del negocio para garantizar que se tengan en cuenta con el fin de mitigar el impacto de los incidentes y evitar la falta de disponibilidad del servicio para Barclays.
2. Eventos que suponen un trastorno para los requisitos de planificación de la recuperación	El proveedor deberá definir los acontecimientos que suponen un trastorno en el ámbito de la planificación, así como el nivel de planificación necesario para garantizar que los servicios puedan prestarse dentro de los niveles de servicio acordados y los correspondientes objetivos de tiempo de recuperación. El proveedor debe asegurarse de que dichos eventos de interrupción reflejen el panorama actual de riesgos/amenazas, se haya evaluado su gravedad y admisibilidad, y estén respaldados por información del sector y de servicios de inteligencia. Como mínimo, el proveedor debe incluir los siguientes eventos de interrupción dentro del alcance de su planificación. ▪ Pérdida de edificios en varias ubicaciones que afectan a la prestación de servicios a Barclays. (Los edificios y la infraestructura asociada no están disponibles). ▪ Pérdida de escenario de datos, incluyendo eventos cibernéticos y el impacto potencial en la prestación de servicios para Barclays.	Barclays impone un requisito comercial (y basado en el riesgo) de evitar y/o ser capaz de recuperarse de manera puntual de importantes eventos de interrupción de los procesos, es decir, de contar con una resiliencia adecuada. Se le garantizará a Barclays, y esta será capaz de garantizar a sus accionistas, que de producirse alteraciones, el servicio está diseñado para reducir al mínimo su repercusión (en los clientes, en las finanzas y/o en la reputación).

Título del control	Descripción del control	Por qué es importante
	▪ Pérdida de recursos de mano de obra que afectarían a la prestación de los niveles de servicio acordados (como pandemias, eventos geopolíticos, fallos críticos de la infraestructura nacional, etc.). ▪ Pérdida de servicios de tecnología (como la pérdida de los centros de datos o del proveedor de servicios en la nube). ▪ Pérdida de subcontratista esencial (servicios o suministros). Los eventos de interrupción deben ser revisados anualmente, y de forma continua, para informar la planificación y las pruebas y demostrar cómo evolucionan con el tiempo.	
3. Requisito de validación y planificación de la recuperación	El proveedor debe mantener los planes de recuperación de negocio para los eventos de interrupción acordados. Los planes de recuperación deben documentar los pasos detallados de recuperación y la respuesta del proveedor que sea posible para mitigar el impacto y/o aplazar la indisponibilidad del servicio prestado a Barclays. Como mínimo, deberá tener en cuenta: ▪ Posibles soluciones alternativas ▪ Protocolos de decisión ▪ Comunicación y priorización del negocio para reanudar/mantener un servicio mínimo viable ▪ Dependencias Los planes de recuperación deben comprobarse y validarse cada 12 meses, o cuando se produzca un cambio significativo, para demostrar que se pueden prestar los niveles de servicio acordados y que los servicios cumplen con los requisitos de la categoría de resiliencia estipulados por Barclays. Si algún plan no cumple los niveles de servicio o los requisitos aplicables en cuanto a categoría de resiliencia, el proveedor lo notificará de inmediato a Barclays (normalmente en un plazo de 10 días) y aportará planes de reparación detallados (que incluyan las medidas que se adoptarán y las fechas de finalización correspondientes).	Las pruebas y la validación se realizan para garantizar a Barclays que el diseño del servicio y el plan funcionan según lo previsto e incluyen todas las dependencias, y demuestran que se alcanzan los niveles de servicio acordados, y que los servicios cumplen los requisitos de resiliencia que haya establecido Barclays.

Título del control	Descripción del control	Por qué es importante
4. Requisito de pruebas integradas	Para garantizar que se entienden las interdependencias entre Barclays y los servicios del proveedor en relación con la recuperación del servicio, el proveedor, a petición de Barclays y en una fecha mutuamente acordada, debe participar en una prueba integrada para validar la resiliencia/continuidad colectiva tanto del proveedor como de Barclays. Barclays no realizará esta solicitud más de una vez cada 2 años, a menos que las pruebas integradas anteriores hayan puesto de manifiesto deficiencias materiales o se haya producido un incidente que haya provocado la interrupción de los servicios.	Los ejercicios conjuntos ayudan a garantizar que existen protocolos de planificación de la recuperación adecuados con la adopción de estrategias de comunicación efectivas, y que tanto el proveedor como Barclays están adoptando una respuesta coordinada para la gestión de la interrupción del negocio y minimizar el impacto en los clientes de Barclays y el sistema financiero en general.
5. Requisito de validación y planes de recuperación de sistemas	El proveedor debe tener un plan de recuperación de sistemas que detalle las acciones necesarias para recuperar los sistemas a su estado operativo tras una interrupción. Los planes deben probarse y validarse para demostrar (con pruebas) que los sistemas se pueden recuperar dentro del objetivo de tiempo de recuperación y el objetivo de punto de recuperación definidos, según lo requiera la categoría de resiliencia definida. Para los sistemas diseñados con una configuración activa/pasiva, el entorno pasivo debe activarse y utilizarse como entorno de producción habitual durante el tiempo suficiente para demostrar la capacidad y la funcionalidad de integración completa. En el caso de los servicios diseñados como activos/activos, la validación debe demostrar la continuidad del funcionamiento en caso de pérdida de un nodo, instancia o zona de disponibilidad (para el alojamiento en la nube) de los sistemas (mínimo 60 minutos). Los requisitos de frecuencia de validación se definen en la categoría de resiliencia del sistema. Consulte la Matriz de criticidad de la resiliencia anterior	Si los planes de recuperación de sistemas fueran inadecuados o totalmente nulos, podrían registrarse pérdidas inaceptables del servicio tecnológico para Barclays o sus clientes tras un incidente. Mantener al día la documentación sobre resiliencia y someterla a prácticas garantiza que los planes de recuperación sigan en consonancia con las necesidades empresariales.
6. Requisito de validación y planes de recuperación de datos	El proveedor debe contar con planes de recuperación de datos para cada sistema tecnológico necesario con el fin de ofrecer soporte a la prestación de servicios de Barclays. Los planes deben revisarse para comprobar su precisión al menos una vez cada 12 meses, o cuando se produzca un cambio significativo, y debe considerarse, como mínimo, lo siguiente: ▪ Fuentes y flujo de datos (ascendente y descendente) ▪ Orígenes de copia de seguridad y replicación ▪ Requisitos de sincronización de datos tras la restauración	La pérdida de datos es una de las amenazas más graves a las que se enfrenta Barclays, ya que puede ser fruto de actos malintencionados o fallos del sistema. Es crítico contar con un plan para este escenario, que ayuda a identificar y comprender el origen de los datos y las dependencias.

Título del control	Descripción del control	Por qué es importante
	El proveedor debe probar y validar los planes de recuperación de datos para cada sistema tecnológico necesario para ofrecer soporte a la prestación de servicios de Barclays y demostrar (con pruebas) que el proceso de recuperación puede restaurar la operatividad de los datos prevista y con arreglo al objetivo de punto de recuperación requerido.	
7. Requisito del proveedor de servicios en la nube y diversidad en el centro de datos	El proveedor debe garantizar que cada sistema tecnológico necesario para ofrecer soporte a la prestación de servicios de Barclays sea resiliente en todos los centros de datos y esté lo suficientemente separado geográficamente para reducir el riesgo de que dichos centros se vean afectados simultáneamente por un evento individual. Los sistemas tecnológicos deben instalarse en múltiples centros de datos para protegerlos frente a apagones en los centros de datos. Esto se extiende a aquellos sistemas alojados en un proveedor de servicios en la nube, que deben instalarse en proveedores de sistemas en la nube de distinas regiones.	Deben instalarse sistemas tecnológicos en distintos centros de datos para proteger contra una interrupción del servicio del centro de datos. Esto se aplica a los sistemas alojados en el proveedor de servicios en la nube - Fallo regional.
8. Requisito de los planes de reconstrucción de plataformas y aplicaciones	El proveedor debe contar con un plan de reconstrucción de plataformas y aplicaciones para cada sistema tecnológico necesario para ofrecer soporte a la prestación de servicios de Barclays y quedará sujeto a procesos de revisión, aprobación y pruebas, como mínimo, una vez cada 12 meses, o cuando se produzca un cambio significativo. Estos planes se aplican a situaciones en las que las opciones tradicionales de recuperación/restauración no pueden utilizarse y el sistema ha de reconstruirse a partir de la «máquina desnuda». Los planes deben considerar lo siguiente: ▪ Sistema operativo/software de infraestructura ▪ Implementación y configuración de aplicaciones ▪ Controles/configuración de seguridad ▪ Dependencias del ecosistema del sistema y reintegración ▪ Requisitos de datos (plan de recuperación de datos) ▪ Dependencias de herramientas para ejecutar planes de recuperación	Es fundamental que los servicios tecnológicos y los acuerdos de asistencia cuenten con planes de recuperación adecuados para un evento de ciberintegridad de datos.