Obligaciones de control de proveedores externos

Planificación de la recuperación

Versión 12.0 Octubre de 2022

1. Definiciones:

«Crisis»	Se refiere a un acontecimiento que supone un trastorno o perjudique la reputación y precisa una respuesta que trasciende la estructura y/o los recursos de las operaciones habituales, por lo que es necesario que intervenga la dirección ejecutiva para tomar decisiones y coordinar la respuesta.
«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.
«Transversalidad de producción»	Este término se utiliza cuando un sistema tecnológico se conmuta automáticamente a un entorno alternativo (DR) y se emplea para ejecutar funciones de producción durante un periodo de tiempo prolongado.
«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 se utiliza para aplicar requisitos de resiliencia a un servicio. Estas incluyen RTO, RPO, requisitos de validación y frecuencia.

2. Matriz de criticidad de la resiliencia:

A los servicios del proveedor se les asigna una categoría de resiliencia específica (0-4) de 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:

	Evaluación del impacto de los riesgos	Impacto excepcional	Impacto alto	Impacto moderado	Impacto bajo	Impacto insignificante
	Categoría de resiliencia	0	1	2	3	4
	Tipo de resiliencia	Continua	Muy resiliente	Resiliente	Recuperar	Suspender / Solo copia de seguridad
Evento de interrupción – Aplicación	Objetivo de RTO (no datos/eventos cibernéticos)	Hasta un máximo de 1 hora	Hasta un máximo de 4 horas	Hasta un máximo de 12 horas	Hasta un máximo de 24 horas	Sin recuperación planificada
Evento de interrupción – Aplicación	Objetivo de RPO (no datos/eventos cibernéticos)	Hasta un máximo de 5 minutos	Hasta un máximo de 15 minutos	Hasta un máximo de 30 minutos	Hasta un máximo de 24 horas	Sin recuperación planificada

3. Controles:

Título del control	Descripción del control	Por qué es importante
1. Requisitos de los eventos que suponen un trastorno para la planificación de la recuperación	Barclays establecerá la categoría de resiliencia para los servicios contratados. 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. La planificación de eventos de interrupción debe tener en cuenta como mínimo: ▪ 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. ▪ 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 del proveedor de servicios en la nube que afecta a todos los servicios de tecnología). ▪ 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 esto evoluciona con el tiempo.	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
	El proveedor debe ser capaz de demostrar que se han tenido en cuenta, probado y validado diversos factores de gravedad.	
2. 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. Dichas dependencias deberán ser objeto de mantenimiento y revisión cada 12 meses. Las dependencias a tener en cuenta son: ▪ Tecnología y datos (proporcionados por el subcontratista e internos). ▪ Subcontratistas esenciales (aquellos que son fundamentales para prestar el 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 indisponibilidad del servicio para Barclays.
3. Validación de los requisitos de la planificación de la recuperación	El proveedor debe mantener los planes de recuperación de negocio para los eventos de interrupción acordados. Los planes de recuperación del negocio 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 para demostrar que los niveles de servicio acordados pueden ser prestados y que los	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
	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 y aportará planes de reparación detallados (que incluyan las medidas que se adoptarán y las fechas de finalización correspondientes).	
4. Prueba integrada	El proveedor con una categoría de resiliencia 0-1, a instancias de Barclays en una fecha mutuamente acordada, deberá participar en una prueba integrada para validar la resiliencia/continuidad colectiva de ambos, del proveedor y 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. Planes de recuperación de sistemas	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 Barclays y los correspondientes objetivos de tiempo de recuperación (RTO) y de punto de recuperación (RPO). Es preciso revisar la precisión de los planes cada 12 meses.	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. Planes de recuperación de datos	El proveedor con una categoría de resiliencia 0-1 debe contar con planes de recuperación de datos para cada sistema/servicio 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 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 nos enfrentamos, 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
7. Diversidad del centro de datos	El proveedor debe garantizar que cada sistema/servicio 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 para reducir el riesgo de que dichos centros se vean afectados simultáneamente por un evento individual. Si el sistema tecnológico se aloja en un proveedor de servicios en la nube, el servicio debe estar disponible en una zona de disponibilidad diferente para mitigar una interrupción total. Los servicios con una categoría de resiliencia 0-1 deberían ser resilientes en todas las regiones de la nube.	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.
8. Validación del plan de recuperación de sistemas	El proveedor debe probar y validar los planes de recuperación de sistemas para demostrar que los sistemas/servicios tecnológicos se pueden recuperar y cumplir el objetivo de tiempo de recuperación y el objetivo de punto de recuperación, tal como se define en la matriz de criticidad de resiliencia. 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 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). En el caso de los servicios diseñados como activo/activo, la validación debe demostrar la continuidad del funcionamiento en caso de pérdida de un entorno activo (escenario de recurso de procesamiento reducido). 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 PRS debe realizarse como mínimo cuatro veces al año a través del PCO. - Categoría de resiliencia 1: La validación de los PRS y del PCO debe realizarse como mínimo dos veces al año a través del PCO. - Categoría de resiliencia 2: La validación de los SRP debe realizarse como mínimo cada 12 meses. - Categoría de resiliencia 3: La validación de los SRP debe realizarse como mínimo cada 24 meses. Si alguna prueba no cumple los requisitos de recuperación mínimos para la categoría	Los sistemas tecnológicos suministrados por terceros pueden afectar a la experiencia de los clientes de Barclays. Asegurar que los terceros 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-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.

Título del control	Descripción del control	Por qué es importante
	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).	
9. Validación del plan de recuperación de datos	El proveedor con una categoría de resiliencia 0-1 debe probar y validar los planes de recuperación de datos para cada sistema/servicio tecnológico necesario para ofrecer soporte a la prestación de servicios de Barclays y demostrar que el proceso de recuperación puede restaurar la operatividad de los datos. La validación debe llevarse a cabo como mínimo cada 12 meses. Si algún plan 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).	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.
10. Planes de reconstrucción de plataformas y aplicaciones	El proveedor con una categoría de resiliencia 0-1 debe contar con un plan de reconstrucción de plataformas y aplicaciones para cada servicio/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. 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 Si algún plan no cumple los requisitos de recuperación mínimos para la categoría de resiliencia correspondiente, el proveedor deberá notificarlo inmediatamente a Barclays	Es fundamental que los servicios tecnológicos y los acuerdos de asistencia cuenten con planes de recuperación adecuados para un evento de ciberintegridad de datos.

Título del control	Descripción del control	Por qué es importante
	y aportar planes de reparación detallados (que incluyan las medidas que se adoptarán y las fechas de finalización correspondientes).	