Obligaciones de control de proveedores externos

Riesgo tecnológico: Controles técnicos

V14.0 Octubre de 2024

Área de control	Título del control	Descripción del control	Por qué es importante
1. Gestión de problemas	Identificación y registro de problemas	El proveedor debe asegurarse de que se lleva a cabo una investigación puntual de la causa raíz de todos los incidentes importantes e incidentes repetidos en los que el efecto combinado sea suficiente para causar un impacto operativo significativo.	Cuando la causa raíz de incidentes significativos no se identifica y resuelve de manera oportuna, el servicio sigue en riesgo de sufrir fallos repetidos y evitables, lo que provoca interrupciones en los sistemas/servicios, daños en la reputación o daños/pérdidas de datos.
	Gestión y resolución de problemas	El proveedor debe asegurarse de que la causa raíz de los incidentes arriba descritos se solucione de forma oportuna o, cuando esto no sea posible, de que Barclays acepte el riesgo y se apliquen los controles de mitigación adecuados para limitar la probabilidad de que se repita.	
2. 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 en cuenta los siguientes requisitos: 1. El proveedor deberá informar a Barclays de todos los cambios significativos antes de su implementación, de modo que se pueda realizar una evaluación del impacto y adoptar las medidas de mitigación adecuadas según sea necesario. 2. La separación de las obligaciones de iniciar, aprobar y ejecutar el cambio, así como del rol de propietario, entre diferentes personas. 3. Los cambios deben planificarse y gestionarse de acuerdo con el nivel de riesgo asociado al mantenimiento del nivel mínimo requerido de servicio a Barclays. 4. Los cambios tienen debidamente en cuenta la posible repercusión sobre el rendimiento 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.

Área de control	Título del control	Descripción del control	Por qué es importante
3. Gestión de capacidad y rendimiento	Adaptación permanente a las necesidades tecnológicas de Barclays	El proveedor deberá definir, mantener y documentar niveles adecuados de rendimiento y capacidad para todos los componentes informáticos clave utilizados en la prestación de servicios a Barclays, de acuerdo con todos los requisitos contractuales, teniendo en cuenta la demanda empresarial conocida y la utilización actual de la capacidad para garantizar que la capacidad disponible siga cumpliendo los requisitos. También se asegurará de que existen avisos y umbrales apropiados en componentes esenciales, a fin de avisar de posibles superaciones de los umbrales, y de que estos se revisan periódicamente para garantizar que la prestación del servicio se ajusta a todos los requisitos contractuales y 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 pueden provocar una interrupción y/o reducción inaceptable de los servicios tecnológicos y pérdida de negocio.
4. Desarrollo de aplicaciones tecnológicas	Estrategia de prueba y finalización antes de la puesta en marcha técnica y/o empresarial	El proveedor debe asegurarse de que el software/servicio funciona como el proveedor ha descrito antes de vender o suministrar dicho software o servicio basado en software a Barclays o proporcionar una visión de los defectos conocidos y el impacto en la entrega del software/servicio. Todo el código de software debe estar en los sistemas de control de versiones y debe estar firmado por el proveedor antes de que se entregue a Barclays. El proveedor debe someter todos los cambios de la aplicación a pruebas de software para garantizar que el software cumpla los requisitos captados. El proveedor debe conservar las evidencias de las pruebas.	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.
	Confirmación de los requisitos del sistema	Al entregar el software conforme a las especificaciones de Barclays, el proveedor debe asegurarse de que los requisitos empresariales tecnológicos estén claramente definidos y acordados con Barclays.	Una definición inadecuada de los requisitos empresariales puede dar lugar a un comportamiento incorrecto del sistema, lo que conlleva riesgos para los procesos operativos y empresariales.
	Aceptación empresarial antes de la implementación	Al entregar el software conforme a las especificaciones de Barclays, el proveedor deberá acordar un proceso de aceptación empresarial con Barclays y seguirlo adecuadamente.	Una aceptación empresarial inadecuada antes de la implementación puede dar lugar a un comportamiento incorrecto del sistema, lo que conlleva riesgos para los procesos operativos y empresariales.

Definiciones tecnológicas:

Artículo de configuración	Cualquier componente que se deba gestionar para ofrecer un servicio informático. Los artículos de configuración pueden ser físicos (p. ej., un ordenador o un router), virtuales (p. ej., un servidor virtual) o lógicos (p. ej., un servicio). Los cambios (adiciones, modificaciones o ceses) deben realizarse conforme al control de la gestión de cambios.
Incidente	Una interrupción no planificada de un servicio informático o una reducción en su calidad, lo que incluye, entre otros supuestos, el fallo de un artículo de configuración que aún no ha afectado a un servicio.
Incidente importante	Un incidente que supone un riesgo/impacto significativo para Barclays y puede tener consecuencias graves, como una pérdida significativa de productividad, daños a la reputación/infracción de la normativa e impacto en los procesos empresariales principales, controles o sistemas clave.
Cambios significativos	Cambios que afectarán (o que puedan afectar) al funcionamiento eficaz de los servicios prestados a Barclays, o cambios para los que Barclays pueda necesitar llevar a cabo las acciones adecuadas de mitigación de riesgos para apoyar su implementación.