Obligaciones de control de proveedores externos

Seguridad de la información y ciberseguridad

Para proveedores clasificados como de alto riesgo de ciberdelito o delitos contra la información

Versión 9.0 con fecha de abril de 2019

Título / Área de control	Descripción del control	Por qué es importante
1. Gobernanza, política y normas en materia de seguridad de la información o ciberseguridad	El proveedor dispondrá de procesos de gobernanza para los riesgos de seguridad de información/ciberseguridad que garanticen el conocimiento de su entorno tecnológico y del estado de los controles de seguridad de la información/ciberseguridad, así como de un programa de seguridad que proteja al proveedor en caso de ataques contra la seguridad de la información o la ciberseguridad, con arreglo a los códigos de prácticas recomendadas del sector (por ejemplo, NIST, SANS, ISO27001) y los requisitos industriales aplicables. El proveedor realizará evaluaciones de riesgo en relación con la seguridad de la de la información o la ciberseguridad periódicamente (como mínimo una vez al año) e implantará los controles y adoptará las medidas que hagan falta para mitigar los riesgos identificados. Si se identifica un riesgo material que pueda afectar negativamente a la reputación o al servicio suministrado a Barclays, el proveedor debe notificárselo a Barclays. El proveedor mantendrá políticas aprobadas por la dirección ejecutiva, así como unas normas de gestión de los ciberriesgos o los riesgos para la información y las revisará, como mínimo, una vez al año.	De no aplicarse este control, o Barclays o sus proveedores podrían no disponer de (y no ser capaces de demostrar) una supervisión adecuada de la seguridad de la información o la ciberseguridad. Las normas y las políticas documentadas son elementos cruciales de la gobernanza y la gestión de riesgos, ya que definen la perspectiva de la dirección sobre los controles necesarios para gestionar el riesgo para la información o el ciberriesgo.

2. Uso autorizado	El proveedor elaborará y publicará un documento con los requisitos de uso aceptable, en el que informará a todo su personal de sus responsabilidades. Deberán considerarse los siguientes temas: (a) el uso de internet; (b) el uso de las redes sociales; (c) el uso del correo electrónico corporativo; (d) el uso de la mensajería instantánea; (e) el uso de equipo informático facilitado por el proveedor; (f) el uso de equipo informático no facilitado por el proveedor (por ejemplo, el uso de dispositivos propios para trabajar); (g) el uso de dispositivos de almacenamiento portátiles o extraíbles; (h) las responsabilidades relativas al tratamiento de activos de información de Barclays; y (i) la salida de canales de filtración de datos. El proveedor emprenderá las acciones necesarias para garantizar el cumplimiento de estos requisitos.	Los requisitos en cuanto a uso aceptable contribuyen a respaldar el entorno de control que protege los activos de información.
3. Funciones y responsabilidades	El proveedor definirá y comunicará las funciones y responsabilidades en relación con la seguridad de la información o la ciberseguridad, las cuales se revisarán periódicamente (y, en cualquier caso, al menos una vez cada 12 meses) y después de que se introduzca algún cambio importante en la actividad o el modelo operativo del proveedor. Las funciones principales incluirán a un ejecutivo sénior que será responsable de la seguridad de la información o la ciberseguridad.	Una definición clara de las funciones y las responsabilidades contribuye a la implantación del Anexo sobre las obligaciones de control de proveedores externos.

4. Respeto por la legislación y las normativas locales	El proveedor se asegurará del cumplimiento de los requisitos legislativos y normativos en materia de seguridad de la información de la jurisdicción en la que opera y de que dicho cumplimiento esté debidamente documentado. Nota: los equipos locales podrían especificar otros requisitos vinculados a la legislación local sobre banca y a regulación relativa a proveedores que presten servicios a Barclays Suiza y Barclays Mónaco.	El incumplimiento de las obligaciones legislativas y normativas podría tener repercusiones graves tanto para el proveedor como para Barclays (por ejemplo sanciones y, en casos extremos, la pérdida de la licencia de banca por parte de Barclays).
5. Educación y conocimiento	El proveedor brindará a todos los empleados pertinentes educación y conocimiento. La educación y el conocimiento resultarán apropiados para sus funciones y responsabilidades y bastarán para que los usuarios conozcan e identifiquen posibles ataques e informen de los problemas. En la formación se abordará, como mínimo, cómo mantener la seguridad en internet (en el trabajo, en casa o cuando viajen), los riesgos de la ingeniería social y las medidas de protección prácticas pertinentes. El proveedor se asegurará de que todos sus empleados (tanto las nuevas incorporaciones como los traslados) realicen un curso de formación, en un plazo razonable, que garantice que entienden sus funciones y responsabilidades en materia de seguridad de la información. Se impartirán cursos para concienciar sobre seguridad de la información o ciberseguridad a los administradores de sistemas, como mínimo con carácter anual, para educarles sobre situaciones/amenazas específicas de su función, sobre cómo protegerse contra los ciberataques o los ataques a la seguridad de la información, y cómo notificar cualquier problema.	En la educación y el conocimiento se basan todos los demás controles de este anexo. De no aplicarse este control, los empleados pertinentes no conocerán los ciberriesgos ni los vectores de ataque y serán incapaces de detectar o evitar ataques.

6. Proceso de gestión de incidentes	Es necesario establecer y gestionar un proceso de respuesta a incidentes para tratar y notificar de forma oportuna y periódica los incidentes que afecten a la información de Barclays y/o a los servicios utilizados por el banco. Como parte del procedimiento de respuesta a incidentes, se definirán los siguientes aspectos: • Las infracciones relacionadas con datos y los incidentes de seguridad que hayan afectado o se hayan dirigido a los activos y/o servicios prestados a Barclays deberán comunicarse a Barclays en cuanto sea posible. Además, se facilitará información actualizada sobre los progresos realizados con las medidas correctivas. • Es necesario establecer un proceso de respuesta a incidentes para tratar y notificar de forma oportuna y periódica las intrusiones que afecten a la información de Barclays y/o a los servicios utilizados por el banco. • Se comunicarán a Barclays, a título informativo, aquellas violaciones de las que no se tenga constancia que hayan afectado al sistema de Barclays, así como las actualizaciones/medidas correctivas adoptadas para resolverlas. • El proveedor se asegurará de que se efectúen pruebas, como mínimo de carácter anual, de los procesos y equipos de respuesta a incidentes para asegurarse de que el proveedor pueda responder a los incidentes de ciberseguridad identificados. Las pruebas incluirán una validación de la capacidad para notificar a Barclays, demostrando la capacidad de ponerse en contacto con las personas apropiadas. • Se definirá y utilizará un proceso para identificar y gestionar la mitigación de vulnerabilidades tras un incidente de seguridad sin poner en peligro investigaciones ni actividades de respuesta. • El proveedor dispondrá de procesos y procedimientos para analizar la raíz de los incidentes externos e internos (del proveedor). • 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.	Un proceso de respuesta y gestión en caso de incidentes contribuye a garantizar que estos se contengan rápidamente y a evitar tener que remitirlos a instancias superiores.

7. Mejora continua	El proveedor aprenderá continuamente de los incidentes y aplicará lo aprendido a mejorar las defensas contra los ciberriesgos.	De no aplicarse este control, los proveedores no podrán utilizar lo aprendido con acontecimientos anteriores para mejorar y reforzar su entorno de control.
8. Responsables de los activos de información	El proveedor designará a una persona de contacto para la comunicación con el responsable del activo de información de Barclays.	Es fundamental conocer los responsables de los activos de información para poder protegerlos de manera adecuada.
9. Plan de etiquetado de la información	***Cuando proceda****, el proveedor deberá aplicar el Plan del etiquetado de la información de Barclays y los requisitos de tratamiento (Apéndice B, Tabla B1 y B2A2), o un plan alternativo acordado con Barclays, a todos los activos de información custodiados o procesados en nombre de Barclays. * «***cuando proceda***» *se refiere a las ventajas del etiquetado frente a los costes asociados. Por ejemplo, sería inapropiado etiquetar un documento si ello infringe los requisitos normativos para evitar su manipulación.*	Resulta esencial disponer de un inventario completo y exacto de activos de información para garantizar la implantación de los controles pertinentes.
10. Gestión de activos	El proveedor mantendrá un inventario exacto de todos los activos informáticos pertinentes utilizados para prestar servicio a Barclays y se debe realizar, como mínimo cada año, una revisión de validación para determinar que el inventario está actualizado, que está completo y que es correcto.	Si no se aplica este control, los activos de Barclays o los activos utilizados por proveedores para prestar servicio a Barclays podrían estar en peligro, lo que podría generar pérdidas económicas, pérdida de datos, daños a la reputación y sanciones reglamentarias.
11. Seguridad en tránsito	Los activos de información de Barclays (salvo los que se consideren «No restringidos» o de categoría equivalente) se protegerán cuando se encuentren en tránsito de forma adecuada al riesgo asociado.	Los controles en tránsito protegen la información de Barclays contra su intercepción y divulgación.

12. Destrucción/Eliminación/Desmantelamiento de información lógica y física	Cuando se destruyan o eliminen activos de información de Barclays que se guarden en formato físico o electrónico, dicha destrucción o eliminación se efectuará utilizando medidas de seguridad adecuadas al riesgo asociado y garantizando que no puedan recuperarse.	La destrucción segura de los activos de información ayuda a garantizar que los activos de información de Barclays no puedan recuperarse mediante una vulneración de la seguridad de los datos o de actividades malintencionadas.
13. Seguridad de la red	El proveedor se asegurará de que todos los sistemas informáticos que utilice él o sus subcontratistas y que se empleen para los servicios prestados a Barclays se encuentren protegidos contra el desplazamiento lateral de las amenazas dentro de la red del proveedor (y de cualquier subcontratista pertinente). El proveedor tendrá en cuenta los siguientes mecanismos de protección: • por medio de una separación lógica de los puertos/las interfaces de gestión de dispositivos del tráfico de usuarios; • controles de autenticación pertinentes; y • la habilitación de todos los controles de mitigación disponibles en el sistema operativo y en las aplicaciones y los agentes instalados. El proveedor definirá y utilizará las capacidades para detectar dispositivos no autorizados, software malintencionado y software no autorizado de alto riesgo en su red. El proveedor colocará sensores de red para detectar ataques en todos los puntos perimetrales de entrada y salida de la red. *Nota: el término «red» se utiliza en este control en referencia a cualquier red no perteneciente a Barclays de la que sea responsable el proveedor, incluida la red de subcontratistas de este.*	De no aplicarse este control, las redes externas e internas pueden verse amenazadas.

14. Perímetro de defensa	El proveedor mantendrá un inventario de las conexiones de red externas, los anfitriones accesibles en Internet y las transferencias de datos utilizadas para transmitir datos de Barclays a Barclays o a cualquier tercero (lo que incluye cualquier subcontratista del proveedor, sin limitación). Se aplicará un diseño de red con varias zonas, separadas en el perímetro, en función de la exposición al riesgo y de las necesidades del negocio. Solo se situarán en el perímetro los dispositivos que exijan o faciliten acceso a/desde redes externas.	Una adecuada protección del perímetro contribuye a garantizar que la red y los activos de información de Barclays se protejan debidamente.
15. Acceso remoto y acceso a la red	El proveedor se asegurará de que se lleve un control del acceso a la red interna y de que solo se permitan dispositivos autorizados, por medio de controles de acceso a la red pertinentes. Si se permite acceso remoto a activos de información de Barclays guardados en el entorno gestionado por el proveedor, se llevarán a cabo una autorización y autenticación de dos factores del extremo, teniendo en cuenta la identidad del usuario, el tipo de dispositivo y la postura de seguridad del dispositivo (por ejemplo, el nivel del parche, el estado de las herramientas para evitar software malintencionado, si es un dispositivo móvil anclado o no anclado, etc.). De manera predeterminada no se proporciona acceso remoto a los entornos de Barclays para conectarse desde la ubicación de un proveedor ni fuera del horario laboral o fuera del horario de soporte de la empresa. Todo acceso remoto debe ser aprobado por los equipos pertinentes de Barclays (incluida la Dirección General de Seguridad).	Los controles de acceso a la red ayudan a garantizar que no se conecten a la red del proveedor dispositivos que no sean seguros ni se introduzcan así nuevas vulnerabilidades
16. Detección de denegación de servicio	El proveedor implantará y mantendrá capacidades para detectar ataques de denegación de servicio. El proveedor se asegurará de que los canales externos o conectados a internet que se empleen para prestar servicios a Barclays cuenten con una adecuada protección contra ataques de denegación de servicio, a fin de garantizar los criterios de disponibilidad acordados con Barclays.	De no aplicarse este control, Barclays y sus proveedores podrían no ser capaces de evitar que un ataque por denegación de servicio alcance su objetivo.

17. Supervisión / Registro	El proveedor se asegurará de que se implante una capacidad de seguimiento de la infraestructura informática en régimen 24/7 para detectar posibles problemas de ciberseguridad. El proveedor recabará los datos de cada incidente de los sensores y las fuentes de los sistemas aplicables, estableciéndose la correlación entre ellos y analizándolos para identificar y entender los diferentes ataques / incidentes. Una vez identificados los incidentes importantes y/o la vulneración de controles de seguridad, el proveedor ha de asegurarse de seguir el proceso de gestión de incidentes (incluido en el anterior apartado 6). El proveedor configurará todos los sistemas principales, incluidas las aplicaciones básicas, de tal modo que registren los incidentes clave y sincronizará la hora de los diferentes sistemas usando el protocolo NTP. El proveedor centralizará los registros, los protegerá debidamente y los conservará durante 12 meses como mínimo. Los incidentes clave registrados incluirán aquellos que puedan afectar a la confidencialidad, la integridad y la disponibilidad de los servicios prestados a Barclays y que pueden ayudar a identificar o investigar incidentes importantes y/o vulneraciones de los derechos de acceso que se hayan producido en relación con los sistemas del proveedor.	De no aplicarse este control, los proveedores no podrán detectar ni responder a los ciberataques ni recuperarse y aprender de los incidentes que se hayan producido en su red analizando los registros pertinentes.
18. Separación de activos de información	El proveedor almacenará los activos de información de Barclays en una red separada (tanto lógica como físicamente) de otros clientes.	Una red separada ayuda a garantizar que los activos de información de Barclays se protejan de manera adecuada contra una divulgación no autorizada.

19. Protección contra software / código malintencionado	Cuando se ofrezca soporte para el sistema operativo, los sistemas informáticos, los servicios informáticos y los dispositivos tecnológicos dispondrán en todo momento de una solución contra software malintencionado, a fin de evitar ataques contra la seguridad o alteraciones en el servicio. El proveedor: • establecerá y mantendrá sistemas de protección actualizados contra código / software malintencionado, de conformidad con las prácticas recomendadas del sector (por ejemplo, NIST, ISO27001); y • establecerá medidas de protección contra la transmisión de código malintencionado a los sistemas de Barclays, los clientes de Barclays y otros terceros, de conformidad con los métodos habituales del sector (por ejemplo NIST, ISO27001).	Las soluciones contra el software malintencionado resultan esenciales para proteger los activos de información de Barclays contra el código malintencionado.
20. Conciliación de cambios de seguridad y normas sobre revisiones de versiones seguras	El proveedor debe definir e implantar normas relacionadas con las revisiones de versiones de todo el software nuevo configurable que se utilice de manera generalizada (por ejemplo, los sistemas operativos, las bases de datos) y el firmware de la infraestructura de uso habitual (por ejemplo, los dispositivos de red o SAN). Se corregirán los incumplimientos de las normas en esta materia. Los cambios de seguridad (por ejemplo, los cambios en la configuración de seguridad, la modificación de privilegios de las cuentas) se incluirán siempre en un registro guardado en un entorno inviolable. Se efectuará una conciliación de los cambios aplicados y los cambios autorizados. Los dispositivos de red y los sistemas de alojamiento que formen parte de los sistemas del proveedor se configurarán de tal manera que funcionen conforme a las prácticas recomendadas del sector (por ejemplo, NIST, SANS, ISO27001).	Los controles sobre revisiones de versiones estándar ayudan a proteger los activos de información contra accesos no autorizados. El cumplimiento respecto de los controles y las normas sobre revisiones de versiones que garanticen que los cambios se autoricen contribuye a garantizar la protección de los activos de información de Barclays.
21. Tecnologías de protección de la seguridad	Se emplearán las tecnologías pertinentes para hacer frente a ciberamenazas actuales y emergentes manteniendo una línea básica coherente de controles para evitar que se envíen, perpetren, aprovechen y filtren ataques al exterior.	De no aplicarse este control, los activos de información de Barclays podrían no contar con una protección suficiente contra los ciberataques.

22. Seguridad en los extremos	El proveedor reforzará los dispositivos utilizados para acceder a la red de Barclays o procesar datos de Barclays, a fin de protegerlos contra los ataques. Esto incluye, por ejemplo, restringir la superficie de ataque por medio de la deshabilitación del software/los servicios/ los puertos innecesarios, asegurarse de que estén en vigor los servicios de asistencia técnica de todas las versiones instaladas, que se disponga de capacidades de protección contra software malintencionado y de programas de firewall debidamente configurados, así como de controles para frenar cualquier intento de aprovechamiento.	De no aplicarse este control, la red de Barclays y la red del proveedor, así como sus extremos podrían ser vulnerables a los ciberataques.
23. Detección de software y dispositivos no autorizados	El proveedor se asegurará de contar con la capacidad y los procesos necesarios para detectar dispositivos y software no autorizados que se identifiquen como malintencionados, así como software no autorizado de alto riesgo.	De no aplicarse este control, los proveedores podrían no ser capaces de detectar, eliminar o deshabilitar software o dispositivos no autorizados o malintencionados, dejando así los activos de Barclays expuestos a ciberataques.
24. Prevención de las filtraciones de datos	Se evaluará y mitigará el riesgo de filtración de datos al que se encuentra expuesta la información en relación con la salida a través de la red o de un medio físico de los servicios que preste el proveedor a Barclays. Deberán tenerse en cuenta los siguientes canales de filtración de datos: • transferencia no autorizada de información fuera de la red interna o la red del proveedor; • pérdida o robo de activos de información de Barclays en medios electrónicos portátiles (como puede ser la información electrónica de ordenadores portátiles, dispositivos móviles y soportes portátiles); • transferencia no autorizada de información a soportes portátiles; • intercambio no seguro de información con terceros (subcontratistas); • impresión o copia inadecuadas de información; • errores y omisiones en la clasificación y el etiquetado de activos; y • filtración no autorizada de información a través del sistema DNS.	Los controles de prevención de filtraciones de datos pertinentes son un elemento esencial de la seguridad de la información, que contribuyen a garantizar que no se pierda información de Barclays.

25. Proceso y almacenamiento seguro	Se implantarán controles para proteger los activos de información (relacionados con los servicios prestados a Barclays por el proveedor) allí donde se guarden y procesen (esto se aplica a la información almacenada como parte de métodos estructurados y no estructurados).	Los activos de información suelen almacenarse juntos y, por lo tanto, su riesgo se encuentra concentrado, de modo que se implantarán medidas de seguridad al respecto.
26. Copias de seguridad y recuperación	Se llevarán a cabo las disposiciones necesarias para garantizar que se haga una copia de seguridad de la información y que esta pueda recuperarse de forma adecuada, cumpliendo los requisitos acordados con el responsable de activos de información de Barclays. Asimismo, se mantendrá la seguridad del activo de información a lo largo de todo el proceso. La frecuencia y el método de copia de seguridad se acordarán con el responsable del activo de información. Los activos de información incluidos en la copia de seguridad tendrán controles definidos para garantizar que solo se otorgue acceso a los mismos cuando sea necesario.	En las copias de seguridad se almacenan activos de información y, por lo tanto, deben someterse a los mismos controles que estos.

27. Gestión de accesos lógicos (LAM)	Se restringirá el acceso a la información, teniendo debidamente en cuenta los principios relativos a su divulgación solo cuando sea necesario conocerla, al privilegio mínimo y a la separación de funciones. El responsable de activos de información se encarga de decidir el acceso que necesita cada persona. • El principio de divulgación de información solo cuando sea necesario conocerla se basa en que solo se debería tener acceso a ella cuando se necesite conocerla para desempeñar las obligaciones para las que nos hayan autorizado. Por ejemplo, si un empleado trata en exclusiva con clientes que tengan su sede en Reino Unido, no «necesitará conocer» información que pertenezca a clientes con sede en Reino Unido. • El principio de privilegio mínimo se basa en que solo deberíamos disfrutar del nivel mínimo de privilegios necesarios para desempeñar las obligaciones para las que nos hayan autorizado. Por ejemplo, si un empleado precisa ver la dirección de un cliente pero no va a tener que cambiarla, el principio de «Privilegio mínimo» exige por lo tanto que tenga acceso de «solo lectura», que es el que debería asignársele en lugar del acceso de lectura/escritura. • El principio de separación de funciones es que serán, al menos, dos personas las responsables de las diferentes partes de cualquier tarea para evitar errores y fraudes. Por ejemplo, un empleado que solicite la creación de una cuenta no debería ser el que apruebe dicha solicitud. Estos principios deberían aplicarse de acuerdo con los riesgos, teniendo en cuenta la clasificación de la información en cuanto a confidencialidad . Cada cuenta debería estar asociada a una sola persona, que responderá de toda actividad que se lleve a cabo usando la cuenta. Esto no impedirá el uso de cuentas conjuntas, aunque solo una persona deberá responder de cada cuenta conjunta. Se definirán procesos de gestión del acceso de acuerdo con las buenas prácticas del sector que incluirán, como mínimo, lo siguiente: • implantación de un solvente proceso de autorización para crear/modificar/eliminar cuentas;	Los controles de LAM pertinentes ayudan a garantizar la protección de los activos de información contra un uso inadecuado.

	• un proceso de revisión del acceso de los usuarios periódicamente y, como mínimo una vez al año, para validar dicho acceso de los usuarios; • controles del personal que se desplaza: modificación o eliminación del acceso en el plazo de cinco días hábiles desde la fecha de traslado; • controles del personal que abandona la empresa: todo acceso lógico utilizado para prestar servicios a Barclays se eliminará en un plazo de 24 horas desde la fecha de cese, todos los demás accesos secundarios se eliminarán en el plazo de siete días; y • se suspenderán las cuentas inactivas que no se usen durante sesenta (60) días consecutivos o más.	
28. Métodos de acceso	La actividad llevada a cabo usando una cuenta debe poder rastrearse hasta llegar a una única persona. Se aplicarán medidas técnicas y de proceso para respetar el nivel de acceso pertinente para el activo de información. Los controles de seguridad relativos a las cuentas (por ejemplo, solventes procesos de autenticación o de emergencia) deben ser proporcionales al riesgo de uso indebido o puesta en peligro de la cuenta. Se definirá un método de acceso de acuerdo con las buenas prácticas del sector que incluirán, como mínimo, lo siguiente: • Las contraseñas para las cuentas interactivas deben cambiarse al menos cada 90 días y la nueva contraseña debe ser distinta a las doce (12) anteriores. • Las cuentas privilegiadas deben modificarse después de cada uso y, cada 90 días, como mínimo. • Las cuentas interactivas se desactivarán tras un máximo de cinco (5) intentos consecutivos de acceso fallidos. Se permitirá el acceso remoto a los servicios de Barclays a través de mecanismos acordados por los equipos pertinentes de Barclays. El acceso remoto debe usar autenticación multifactor.	Los controles de gestión de acceso contribuyen a garantizar que solo puedan acceder a los activos de información los usuarios autorizados.

29. Protección de aplicaciones	Las aplicaciones se desarrollarán usando prácticas de codificación seguras y en entornos seguros. Si el proveedor desarrolla aplicaciones para que Barclays las utilice, o que se utilicen para respaldar el servicio prestado a Barclays, durante el proceso de desarrollo se implantarán procesos y controles para identificar y corregir aspectos vulnerables del código. El código binario de las aplicaciones debe protegerse contra cambios no autorizados, tanto durante su despliegue como en las bibliotecas de código fuente. El proveedor debe asegurarse de separar las funciones para el desarrollo de sistemas. Esto incluye asegurarse de que los desarrolladores de sistemas no tengan acceso al entorno activo, salvo si hay una emergencia, en cuyo caso el acceso debe protegerse con medidas de control adecuadas, como procedimientos de emergencia. En estas circunstancias, estas actividades deben registrarse y someterse a una revisión independiente.	Los controles que protegen el desarrollo de aplicaciones contribuyen a garantizar que se mantiene la seguridad de estas durante su despliegue.

30. Gestión de las vulnerabilidades	El proveedor utilizará un mecanismo coherente para registrar, clasificar y responder a vulnerabilidades identificadas. El proveedor establecerá capacidades para identificar y clasificar vulnerabilidades de seguridad en los sistemas informáticos basándose en el riesgo en todas las plataformas utilizadas por la organización. El proveedor se asegurará de que se aborde la gestión de las vulnerabilidades en el transcurso habitual de sus operaciones, lo que incluye procesos para detectar y evaluar los riesgos de vulnerabilidades, para eliminar o corregir aspectos vulnerables en todos los sistemas y evitar que se introduzcan nuevas vulnerabilidades durante procesos de cambio y durante la instalación de nuevos sistemas. Todos los problemas y aspectos vulnerables que pudieran afectar de forma importante a los sistemas de Barclays o a los servicios que el proveedor preste a Barclays y cuyo riesgo el proveedor haya decidido aceptar se comunicarán de inmediato a Barclays y se acordarán por escrito con esta entidad. El proveedor instalará parches de seguridad informática y actualizaciones para resolver vulnerabilidades en la seguridad por medio de un proceso aprobado interno (del proveedor) y de forma puntual, a fin de evitar cualquier vulneración de la seguridad. Se dotará a los sistemas del proveedor que no se puedan actualizar por cualquier motivo de medidas para proteger estos sistemas vulnerables.	De no aplicarse este control, los atacantes podrían aprovechar las vulnerabilidades de los sistemas para atacar a Barclays y a sus proveedores.

31. Simulación de amenazas/ Pruebas de penetración/ Evaluación de la seguridad informática	El proveedor contratará a un proveedor de seguridad cualificado e independiente para realizar una simulación de amenazas o una evaluación de la seguridad informática de las aplicaciones y las infraestructuras informáticas en relación con los servicios que preste a Barclays. Se realizará una vez al año como mínimo para identificar vulnerabilidades que se podrían aprovechar para violar la confidencialidad de los datos de Barclays mediante ciberataques. Hay que asignar prioridades a las vulnerabilidades, y se debe hacer un seguimiento de su resolución. Todos los problemas cuyo riesgo se haya decidido aceptar se comunicarán a Barclays para acordarlos con el banco. El proveedor informará a Barclays del alcance de la evaluación de seguridad, y lo determinará de acuerdo con este, en especial en lo que se refiere a las horas/fechas de inicio y finalización, para no interferir en las actividades clave de Barclays.	De no aplicarse este control, los proveedores podrían no ser capaces de valorar las ciberamenazas a las que se enfrentan o si sus defensas son apropiadas y lo suficientemente sólidas.

32. Gestión de cambios y revisiones	Los datos de Barclays y los sistemas utilizados para almacenarlos o procesarlos deben protegerse contra cambios inapropiados que puedan afectar a su disponibilidad o integridad. El proveedor debe desarrollar e implementar una estrategia de gestión de revisiones respaldada por controles de gestión, procedimientos de gestión de revisiones y documentación operativa. En cuanto estén disponibles las revisiones de seguridad informática y las actualizaciones de vulnerabilidad de seguridad, deben instalarse de forma oportuna mediante un proceso aprobado para evitar infracciones de seguridad. Hay que instalar medidas de seguridad en los sistemas del proveedor que no se puedan actualizar por alguna razón, para proteger estos sistemas vulnerables. Todos los cambios deben realizarse en conformidad con el proceso de gestión de cambios del proveedor aprobado. Deben comprobarse las vulnerabilidades pendientes de solución de las aplicaciones de código abierto. El proveedor se asegurará de que se implementen las correcciones urgentes cuando estén disponibles y sean autorizadas, a menos que supongan riesgos más importantes para la empresa. Hay que instalar medidas de seguridad en los sistemas del Proveedor que no se puedan actualizar por alguna razón, para proteger estos sistemas vulnerables. Todos los cambios se realizarán de conformidad con el proceso de gestión de cambios del proveedor.	Si este control no se implementa, los servicios también pueden ser vulnerables a problemas de seguridad que podrían poner en riesgo los datos de los consumidores, provocar pérdidas de servicio o permitir otras actividades malintencionadas.
33. Criptografía	El proveedor revisará y evaluará la tecnología criptográfica y los algoritmos de encriptación que utiliza a fin de garantizar que sigan siendo adecuados para su finalidad. La intensidad del cifrado aplicado será acorde a la tolerancia al riesgo, ya que puede tener un impacto operativo o de rendimiento. Las implementaciones criptográficas deben respetar los requisitos y los algoritmos definidos.	Los algoritmos y la protección del cifrado pertinentes y actualizados garantizan una protección continua para los activos de información de Barclays.

34. Computación en la nube	Todo uso de servicios de computación en la nube (pública/privada/comunitaria/híbrida), por ejemplo SaaS/PaaS/IaaS, que se haga como parte de los servicios acordados prestados a Barclays debe ser revisado y aprobado por los equipos de Barclays pertinentes (incluida la Dirección General de Seguridad); y los controles de protección de la información y el servicio deben ser proporcionales al perfil de riesgo y a la criticidad del activo de información, para evitar filtraciones de datos e infracciones de ciberseguridad.	De no aplicarse este principio, la seguridad de los activos de la información de Barclays protegidos de manera incorrecta podría verse afectada. Esto tendría como consecuencia una sanción legal o reglamentaria, o daños en la reputación.
35. Derecho de inspección	El proveedor permitirá que Barclays, previa notificación por escrito con una antelación mínima de diez días hábiles, pueda llevar a cabo una revisión de seguridad de cualquier instalación o tecnología utilizada por el proveedor o sus subcontratistas para desarrollar, probar, mejorar, mantener u operar los sistemas del proveedor utilizados en los servicios, a fin de comprobar que el proveedor cumple con sus obligaciones. El proveedor también permitirá a Barclays realizar una inspección inmediatamente después de un incidente de seguridad. Todo incumplimiento de controles identificado por Barclays durante una inspección se someterá a una evaluación de riesgos por parte de Barclays y este especificará un plazo para que se corrija. El proveedor se encargará entonces de implantar cualquier medida correctiva que sea necesaria en el plazo establecido. El proveedor prestará a Barclays toda la asistencia necesaria durante una inspección.	Si no aceptan, los proveedores no podrán garantizar plenamente que se cumplen estas obligaciones de seguridad.
36. Espacio dedicado al banco	Para servicios suministrados que requieran Espacio dedicado al banco (EDB), deben establecerse requisitos físicos y técnicos de EDB. (Si el EDB fuera un requisito del servicio, se aplicarían los requisitos de control del Apéndice C).	Si este control no se implementa, puede que no se establezcan los controles físicos y técnicos apropiados. Esto tendría como consecuencia retrasos o interrupciones del servicio, o infracciones de ciberseguridad.

Apéndice A. Glosario

Definiciones	
Activo de información	Toda información que tenga valor, considerado en términos de confidencialidad, integridad y requisitos de disponibilidad. O cualquier parte individual o grupo de información que tenga un valor para la organización.
Autenticación multifactor	Autenticación que utiliza dos o más técnicas de autenticación diferentes. Un ejemplo es el uso de un token de seguridad. En este caso, la autenticación se basa en algo que posee la persona (es decir, el token de seguridad) y algo que el usuario sabe (es decir, el PIN del token de seguridad).
Cifrado	La transformación de un mensaje (datos, voz o vídeo) en un formato sin significado que no puedan entender lectores no autorizados. Esta transformación se realiza partiendo de texto sin formato a un formato de texto cifrado.
Código malintencionado	Software escrito con intención de burlar la política de seguridad de un sistema informático, dispositivo o aplicación. Algunos ejemplos serían los virus informáticos, los troyanos y los gusanos.
Copia de seguridad, copia de seguridad	Una copia de seguridad o el proceso de copia de seguridad se refiere a la realización de copias de datos para poder recuperar el original tras un incidente de pérdida de datos.
Criptografía	La aplicación de teoría matemática para desarrollar técnicas y algoritmos que pueden aplicarse a los datos para garantizar objetivos tales como la confidencialidad, la integridad de los datos y/o la autenticación.
Cuenta	Un conjunto de credenciales (por ejemplo, el ID de un usuario y la contraseña) mediante el cual se gestiona el acceso a un sistema informático usando controles de acceso lógico.
Cuenta compartida	Una cuenta otorgada a más de un empleado, consultor, contratista o trabajador de una agencia, que posee acceso autorizado pero que no puede optar a cuentas individuales debido a la naturaleza del sistema al que se accede.
Cuenta privilegiada	Una cuenta que ofrece un mayor nivel de control sobre un sistema informático concreto. Estas cuentas se suelen utilizar para mantenimiento del sistema, administración de la seguridad o cambios de configuración de un sistema informático. Ejemplos: 'Administrador', 'root', cuentas Unix con uid=0, cuentas de soporte técnico, cuentas de administración de la seguridad, cuentas de administración del sistema y cuentas de administrador local.
Denegación de servicio (ataque)	Intento de privar a los usuarios de un recurso informático del que deberían disponer.
Destrucción / Eliminación	El hecho de sobrescribir, borrar o destruir físicamente información que no pueda recuperarse.
Espacio dedicado al banco	Espacio dedicado al banco significa cualquier instalación propiedad de un miembro del grupo del proveedor o de cualquier subcontratista, o bajo su control, que se dedique exclusivamente a Barclays y desde la que se presten o realicen los servicios.
Privilegio mínimo	El nivel mínimo de acceso/permiso que permite al usuario o a una cuenta desempeñar su función empresarial.
Responsable de activos de información	La persona de la empresa responsable de clasificar un activo y asegurarse de que se maneja correctamente.

Sistema	Un sistema, en el contexto del presente documento, está formado por las personas, los procedimientos, el equipo informático y el software. Los elementos de esta entidad compuesta se usan conjuntamente en el entorno operativo o de soporte previsto para realizar una tarea determinada o lograr una finalidad específica, un servicio o un requisito de una misión.
Usuario	Una cuenta designada para un empleado, consultor, contratista o trabajador de una agencia del proveedor que posee acceso autorizado a un sistema sin tener más privilegios.

Apéndice B. Plan del etiquetado de la información de Barclays

Tabla B1: Plan del etiquetado de la información de Barclays

Etiqueta	Definición	Ejemplos
Secreta	Se clasificará la información como «secreta» si su divulgación no autorizada causara un perjuicio a Barclays, valorado de acuerdo con el marco de gestión de riesgos empresariales (ERMF) como «crítico» (financiero o no financiero). Esta información está restringida a un público específico y no debe distribuirse sin el permiso de la persona de la que se haya obtenido. El público puede incluir destinatarios externos con autorización explícita del responsable de información.	• Información sobre posibles fusiones o adquisiciones. • Información de planificación estratégica: empresarial y organizativa. • Determinada configuración de la seguridad de la información. • Determinados resultados de auditorías e informes. • Actas del Comité Ejecutivo. • Datos de autenticación o identificación y verificación: cliente y compañero. • Volúmenes generales de información de los titulares de tarjetas. • Pronósticos de beneficios o resultados financieros anuales (antes de hacerse públicos). • Cualquier elemento cubierto por un Acuerdo de confidencialidad formal.
Restringida – Interna	La información deberá clasificarse como Restringida – Interna si los destinatarios previstos son solo empleados de Barclays autenticados y Proveedores de servicios gestionados de Barclays con un contrato en vigor y restringida a un público específico.	• Estrategias y presupuestos. • Evaluaciones del personal. • Remuneración de los empleados y datos del personal. • Evaluaciones de la vulnerabilidad. • Resultados de auditorías e informes.

	La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero). Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla.	
Restringida – Externa	La información deberá clasificarse como Restringida – Externa si los destinatarios previstos son empleados autenticados de Barclays y proveedores de servicios gestionados de Barclays con un contrato en vigor, restringida a un público específico o partes externas autorizadas por el responsable de la información. La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero). Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla.	• Planes de nuevos productos. • Contratos de clientes. • Contratos legales. • Información de clientes individuales o de escaso volumen que deba enviarse externamente. • Comunicaciones de clientes. • Materiales de oferta de nuevas emisiones (por ejemplo, folleto, nota sobre la oferta). • Documento de investigación definitivo. • Información no pública de carácter material no perteneciente a Barclays (MNPI). • Todos los informes de investigación. • Determinados materiales de marketing. • Comentario de marketing.
Sin restricción	Información destinada a su distribución general o que no causaría ninguna repercusión en la organización si se distribuyera.	• Material de marketing. • Publicaciones. • Anuncios públicos. • Anuncios de ofertas de trabajo. • Información sin impacto para Barclays.

Tabla B2: Plan del etiquetado de la información de Barclays – Requisitos de tratamiento

*** La información de la configuración de seguridad de un sistema, resultados de auditorías y registros personales pueden clasificarse como «restringida - interna» o «secreta» según el impacto que pudiera tener para el negocio su revelación no autorizada.

Fase del ciclo de vida	Restringida – Interna	Restringida – Externa	Secreta
Creación e introducción	• A los activos se les asignará un responsable de la información.	• A los activos se les asignará un responsable de la información.	• A los activos se les asignará un responsable de la información.
Almacenamiento	• Los activos (físicos o electrónicos) no se almacenarán en áreas públicas (incluidas las áreas públicas de las instalaciones a las que puedan acceder visitantes sin supervisión). • No se dejará información en áreas públicas en las instalaciones a las que puedan acceder visitantes sin supervisión.	• Los activos (físicos o electrónicos) no se almacenarán en lugares donde personas no autorizadas puedan verlos o acceder a ellos. • Los activos almacenados en formato electrónico se protegerán mediante cifrado, o con controles de compensación apropiados, si hubiera un riesgo importante de que personal no autorizado pudiera acceder a ellos.	• Los activos (físicos o electrónicos) no se almacenarán en lugares donde personas no autorizadas puedan verlos o acceder a ellos. • Los activos almacenados en formato electrónico se protegerán mediante cifrado, o con controles de compensación apropiados, si hubiera un riesgo importante de que personal no autorizado pudiera acceder a ellos. • Todas las claves de cifrado privadas utilizadas para proteger los datos de Barclays, su identidad y/o reputación se protegerán mediante módulos de seguridad de hardware (HSM) con certificación FIPS 140-2 de Nivel 3 o superior.
Acceso y uso	• Los activos (físicos o electrónicos) no se dejarán en zonas públicas fuera de las instalaciones. • Los activos (físicos o electrónicos) no se dejarán en zonas públicas de las instalaciones a las que puedan acceder visitantes sin supervisión.	• No se trabajará con activos (físicos o electrónicos) ni se dejarán desatendidos en lugares donde personas no autorizadas puedan verlos o acceder a ellos. Se puede trabajar con los activos si se han implantado los controles adecuados (por ejemplo: filtros de privacidad).	• No se trabajará con activos (físicos o electrónicos) ni se dejarán desatendidos en lugares donde personas no autorizadas puedan verlos o acceder a ellos. Se puede trabajar con los activos si se han implantado los controles adecuados (por ejemplo: filtros de privacidad).

	• Los activos en formato electrónico se protegerán mediante controles de gestión de acceso lógico apropiados si fuera necesario.	• Los activos que se envíen a imprimir se recogerán inmediatamente de la impresora. Si no fuera posible, se usarán herramientas para la impresión segura. • Los activos en formato electrónico se protegerán mediante controles de gestión de acceso lógico apropiados.	• Para la impresión de activos se usarán herramientas de impresión segura. • Los activos en formato electrónico se protegerán mediante controles de gestión de acceso lógico apropiados.
Uso compartido	• Los activos en papel llevarán una etiqueta de información visible. La etiqueta irá como mínimo en la página que lleve el título. • Los activos electrónicos llevarán una etiqueta informativa clara. • Los activos solo se distribuirán usando sistemas, métodos o proveedores aprobados por la organización. • Los activos solo se distribuirán a personas empleadas por la organización (o con una obligación contractual apropiada) o como parte de una necesidad comercial claramente reconocida, como una negociación de contrato.	• Los activos en papel llevarán una etiqueta de información visible. La etiqueta irá como mínimo en la página que lleve el título. • Los sobres que contengan activos en papel llevarán una etiqueta de información visible en la parte delantera. • Los activos electrónicos llevarán una etiqueta informativa clara. Las copias electrónicas de documentos de varias páginas llevarán una etiqueta de información visible en todas sus páginas. • Los activos solo se distribuirán usando sistemas, métodos o proveedores aprobados por la organización. • Los activos solo se distribuirán a personas empleadas por la organización (o con una obligación contractual apropiada) o como parte de una necesidad comercial claramente reconocida, como una negociación de contrato. • Los activos solo se distribuirán a personas que necesiten recibirlos por razones del negocio.	• Los activos en papel llevarán una etiqueta de información visible en cada página. • Los sobres que contengan activos en papel llevarán una etiqueta de información visible en la parte delantera e irán cerrados con un precinto de seguridad. Se introducirán dentro de otro sobre sin etiquetas antes de su distribución. • Los activos electrónicos llevarán una etiqueta informativa clara. Las copias electrónicas de documentos de varias páginas llevarán una etiqueta de información visible en todas sus páginas. • Los activos solo se distribuirán usando sistemas, métodos o proveedores aprobados por la organización. • Los activos solo se distribuirán a personas empleadas por la organización (o con una obligación contractual apropiada) o como parte de una necesidad comercial claramente reconocida, como una negociación de contrato. • Los activos solo se distribuirán a personas específicamente autorizadas por el propietario de la información.

		• Los activos no se enviarán por fax a no ser que el remitente haya confirmado que los destinatarios están listos para recibirlos. • Los activos electrónicos se cifrarán utilizando un mecanismo de protección criptográfico cuando transiten fuera de la red interna.	• Los activos no se enviarán por fax. • Los activos electrónicos se cifrarán utilizando un mecanismo de protección criptográfico cuando transiten fuera de la red interna. • Se mantendrá la cadena de custodia de los activos electrónicos.
Archivo y eliminación	• Los activos en papel se eliminarán utilizando un servicio de gestión de residuos confidencial. • Las copias de los activos electrónicos también se eliminarán de las «papeleras de reciclaje» del sistema de manera oportuna.	• Los activos en papel se eliminarán utilizando un servicio de gestión de residuos confidencial. • Las copias de los activos electrónicos también se eliminarán de las «papeleras de reciclaje» del sistema de manera oportuna.	• Los activos en papel se eliminarán utilizando un servicio de gestión de residuos confidencial. • Las copias de los activos electrónicos también se eliminarán de las «papeleras de reciclaje» del sistema de manera oportuna. • Los soportes en los que se hayan almacenado activos electrónicos «secretos» se limpiarán adecuadamente antes o durante la eliminación.

Apéndice C: Espacio dedicado al banco (EDB). Requisitos de control (Nota: se debe consultar con el representante de suministro para determinar si es necesario)

Área de control	Título del control	Descripción del control
Espacio dedicado al banco	Separación física	El área física ocupada debe dedicarse a Barclays, y no se debe compartir con otras empresas / proveedores.
Espacio dedicado al banco	Control de acceso físico	Deben activarse controles automáticos seguros para el acceso al EDB, como: 1) Para el personal autorizado; i) Tarjeta de identificación con foto siempre visible

		ii) Implementación de lectores de tarjeta por proximidad iii) Activación de mecanismo antirretorno 2) Controles de visitas/proveedores i) Libros de registro de visitas i) Tarjeta de identificación de uso limitado siempre visible
Espacio dedicado al banco	Control de acceso físico	Hay que configurar alarmas que avisen a través de un sistema de acceso centralizado con control de acceso auditable
Espacio dedicado al banco	Control de acceso físico y orden y limpieza	Supervisión de los controles que garantice un acceso adecuado al EDB y a otras áreas de gran importancia Solo se debe permitir el acceso al EDB a personal autorizado de mantenimiento y soporte, como electricistas, mantenimiento de CA, etc.
Espacio dedicado al banco	Acceso remoto - ID&V	Cada usuario individual debe autenticarse únicamente en la red de Barclays desde el EDB con un token de autenticación multifactor suministrado por Barclays
Espacio dedicado al banco	Acceso remoto - Tokens de software	La instalación de cualquier software RSA y de tokens de software debe ser realizada por personal autorizado en equipos de escritorio del EDB aprobado
Espacio dedicado al banco	Acceso remoto - Soporte fuera del horario laboral	De manera predeterminada no se proporciona acceso remoto al entorno EDB para soporte fuera del horario laboral. Todo acceso remoto debe ser aprobado por los equipos pertinentes de Barclays (incluida la Dirección General de Seguridad).
Espacio dedicado al banco	Correo electrónico e Internet	La conexión de red debe configurarse de forma segura para restringir el correo electrónico y la actividad de Internet en la red del EDB
Espacio dedicado al banco	Desarrollo de software, entorno de pruebas y desarrollo	El proveedor se asegurará de que el desarrollo de software se realice únicamente para programas que son propiedad de Barclays dentro del espacio dedicado al banco (EDB).
Espacio dedicado al banco	Controles de red - Transmisión	Toda la información debe transmitirse de forma segura entre el entorno del EDB y Barclays, y la gestión de los dispositivos de red debe realizarse con protocolos seguros
Espacio dedicado al banco	Controles de red - Enrutamiento	La configuración de enrutamiento debe garantizar que solo se establezcan conexiones con la red de Barclays y evitar el enrutamiento a otras redes

Espacio dedicado al banco	Controles de red - Acceso inalámbrico	No se deben utilizar redes inalámbricas en el segmento de red de Barclays para suministrar servicios.

Secreto bancario

Controles adicionales exclusivos de los jurisdicciones con secreto bancario (Suiza/Mónaco)

Título / Área de control	Descripción del control	Por qué es importante
1. Funciones y responsabilidades	El proveedor definirá y comunicará las funciones y las responsabilidades en relación con el tratamiento de datos que identifiquen a los clientes (en adelante CID). El proveedor revisará los documentos en los que se señalen las funciones y responsabilidades en relación con los CID cuando se introduzca algún cambio importante en la actividad o el modelo operativo (o el negocio) del proveedor, o al menos una vez al año, y los distribuirá en la jurisdicción con secreto bancario pertinente. Las funciones principales incluirán a un ejecutivo sénior que será responsable de proteger y supervisar todas las actividades relacionadas con los CID (consúltese la definición de CID en el Apéndice A)	Una definición clara de las funciones y las responsabilidades contribuye a la implantación del Anexo sobre las obligaciones de control de proveedores externos.
2. Notificación de violaciones de la seguridad de los CID	Existirán controles y procesos documentados que garanticen la notificación y la gestión de cualquier violación de la seguridad que repercuta en los CID. El proveedor responderá a toda vulneración de los requisitos de gestión (definidos en la tabla B2) y se comunicará a la jurisdicción con secreto bancario correspondiente de forma inmediata (como mínimo en el plazo de 24 horas). Es necesario establecer un proceso de respuesta a incidentes para tratar y notificar de forma oportuna y periódica los incidentes que afecten a los CID. 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 la jurisdicción con secreto bancario correspondiente para su aprobación.	Un proceso de respuesta en caso de incidentes contribuye a garantizar que estos se contengan rápidamente y a evitar tener que remitirlos a instancias superiores. Toda vulneración de la seguridad que repercuta en los CID podría causar importantes daños a la reputación de Barclays y podría derivar en la imposición de multas y en la pérdida de la licencia bancaria en Suiza y Mónaco.

3. Educación y conocimiento	Los empleados del proveedor que tengan acceso a los CID o los gestionen deberán realizar un curso de formación* que aplique los requisitos de secreto bancario de los CID tras cualquier nuevo cambio en la normativa, o al menos una vez al año. El proveedor se asegurará de que todos sus empleados nuevos (que tengan acceso a los CID o los gestionen), en un plazo razonable (aproximadamente tres meses) realicen un curso de formación que garantice que entienden sus responsabilidades con respecto a los CID. El proveedor llevará un seguimiento de los empleados que han realizado el curso de formación. * las jurisdicciones con secreto bancario ofrecerán información sobre el contenido previsto para los cursos de formación.	En la educación y el conocimiento se basan todos los demás controles de este anexo.
4. Plan de etiquetado de la información	***Cuando proceda****, el proveedor deberá aplicar el Plan del etiquetado de la información de Barclays (Tabla D1 del Apéndice D), o un plan alternativo acordado con la jurisdicción de secreto bancario, a todos los activos de información custodiados o procesados en nombre de la jurisdicción de secreto bancario. Los requisitos de gestión de los CID se incluyen en la Tabla D2 del Apéndice D. * «***cuando proceda***» *se refiere a las ventajas del etiquetado frente a los costes asociados. Por ejemplo, sería inapropiado etiquetar un documento si ello infringe los requisitos normativos para evitar su manipulación.*	Resulta esencial disponer de un inventario completo y exacto de activos de información para garantizar la implantación de los controles pertinentes.
5. Almacenamiento externo/computación en la nube	Todo uso de computación en la nube o almacenamiento externo de CID (en servidores situados fuera de la jurisdicción con secreto bancario o fuera de la infraestructura del proveedor) que se realice como parte del servicio a dicha jurisdicción debe ser aprobado por los equipos locales pertinentes (incluida la Dirección General de Seguridad, Cumplimiento y Asesoría Jurídica); y se implantarán controles con arreglo a la jurisdicción con secreto bancario correspondiente para proteger información de los CID con deficiencias con respecto al perfil de riesgo elevado que presentan.	Si este principio no se implementa correctamente, la seguridad de los datos de los clientes (CID) protegidos podría verse afectada. Esto tendría como consecuencia una sanción legal o reglamentaria, o daños en la reputación.

** Los datos que identifican a clientes son datos especiales debido a las leyes en materia de secreto bancario que se encuentran en vigor en Suiza y Mónaco. Por lo tanto, los controles aquí expuestos complementan a los enumerados anteriormente.

Término	Definición
CID	Datos que identifican al cliente
CIS	Ciberseguridad y seguridad de la información
Empleado del proveedor	Toda persona cedida directamente al proveedor como empleado permanente o cualquier persona que preste servicios al proveedor durante un espacio de tiempo limitado (como un consultor, por ejemplo)
Activo	Cualquier parte individual o grupo de información que tenga un valor para la organización
Sistema	Un sistema, en el contexto del presente documento, está formado por las personas, los procedimientos, el equipo informático y el software. Los elementos de esta entidad compuesta se usan conjuntamente en el entorno operativo o de soporte previsto para realizar una tarea determinada o lograr una finalidad específica, un servicio o un requisito de una misión.
Usuario	Una cuenta designada para un empleado, consultor, contratista o trabajador de una agencia del proveedor que posee acceso autorizado a un sistema propiedad de Barclays sin tener más privilegios.

Apéndice D: DATOS QUE IDENTIFICAN AL CLIENTE

Los CID directos (CIDD) pueden definirse como identificadores únicos (propiedad del cliente), que permiten, tal cual están y por sí solos, identificar a un cliente sin acceder a las aplicaciones bancarias de Barclays. No serán ambiguos ni dependerán de la interpretación y podrán incluir información tal como el nombre, el apellido, el nombre de la empresa, la firma, el identificador en redes sociales, etc. Los CID directos se refieren a datos de clientes que no son propiedad del banco ni ha creado este.

Los CID indirectos (CIDI) se dividen en un máximo de tres niveles

- **Los CIDI N1** pueden definirse como identificadores únicos (propiedad del Banco) que permiten identificar de manera única a un cliente en caso de que se otorgue acceso a aplicaciones bancarias u otras **aplicaciones de terceros**. El identificador no será ambiguo ni dependerá de la interpretación y puede incluir por ejemplo el número de cuenta, el código IBAN, el número de la tarjeta de crédito, etc.

- **Los CIDI N2** pueden definirse como información (propiedad del cliente) a partir de la cual se podría llegar a identificar a un cliente combinándola con otra. Aunque esta información no puede utilizarse por sí sola para identificar a un cliente, cuando se emplea junto con otra información sí que podría identificarlo. Los CIDI N2 deben protegerse y gestionarse con el mismo rigor que los CIDD.

- **Los CIDI N3** pueden definirse como identificadores únicos pero anonimizados (propiedad del Banco) que permiten identificar a un cliente en caso de que se otorgue acceso a aplicaciones bancarias. La diferencia con los CIDI N1 es la clasificación de la información que les corresponde, como Restringida – Externa en lugar de secreto bancario, lo que significa que no están sujetos a los mismos controles.

Consulte en la Figura 1 Árbol de decisión sobre CID un esquema del método de clasificación.

Los CIDI N1 directos e indirectos no se compartirán con ninguna persona externa al banco y se respetará en todo momento el principio basado en la necesidad de conocerlos. Los CIDI N2 pueden compartirse con quienes necesiten conocerlos, pero no en combinación con otros CID. Si se comparten varios CID, existe la posibilidad de crear una «combinación tóxica» que pudiera llegar a revelar la identidad de un cliente. Definimos una combinación tóxica cuando se combinan al menos dos CIDI N2. Los CIDI N3 se

pueden compartir, ya que no están clasificados como información con el nivel de secreto bancario, a menos que un uso recurrente del mismo identificador pueda provocar una recopilación de datos CIDI N2 suficientes para revelar la identidad de un cliente.

Clasificación de la información	Secreto bancario		Restringida – Interna	
Clasificación	**CID directos (CIDD)**	**CID indirectos (CIDI)**		
		Indirectos (N1)	**Posiblemente indirectos (N2)**	**Identificador impersonal (N3)**
Tipo de información	Nombre del cliente	Número de contenedor / ID de contenedor	Nombre	ID de proceso interno
	Nombre de la compañía	Número MACC (cuenta de dinero con un ID de contenedor Avaloq)	Fecha de nacimiento	Identificador único estático
	Extracto de cuenta	Dirección	Nacionalidad	Identificador dinámico
	Firma	IBAN	Cargo	ID de contenedor externo
	ID de red social	Datos de inicio de sesión en banca electrónica	Situación familiar	
	Número de pasaporte	Número de depósito seguro	Código Postal	
	Número de teléfono	Número de la tarjeta de crédito	Situación patrimonial	

Dirección de correo electrónico		Apellidos	
Nombre del puesto o cargo de persona políticamente expuesta:		Última visita del cliente	
Nombre artístico		Idioma	
Dirección IP		Sexo	
Número de fax		Fecha de caducidad CC	
		Persona de contacto principal	
		Fecha de nacimiento	
		Fecha de apertura de la cuenta	
		Valor de la transacción/posición general	

Ejemplo: Si envía un correo electrónico o comparte algún documento con personas externas (incluidos terceros de Suiza/Mónaco) o compañeros internos de otra filial/empresa afiliada situada en Suiza/Mónaco u otros países (por ejemplo, Reino Unido)

1. Nombre del cliente

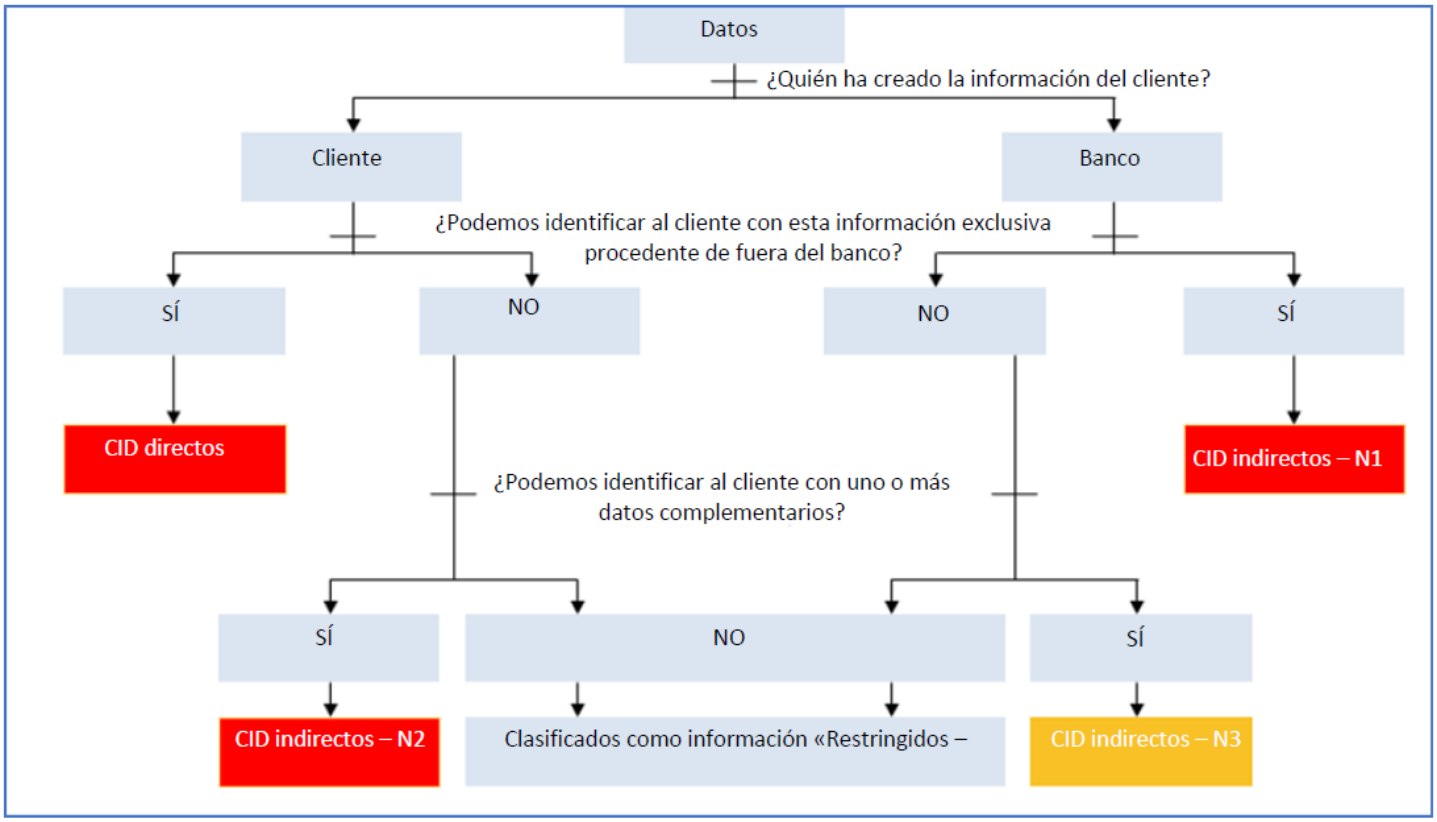
   (CIDD) = Vulneración del secreto bancario

2. ID de contenedor

(CIDI N1) = Vulneración del secreto bancario

3. Situación patrimonial + Nacionalidad

(CIDI N2) + (CIDI N2) = Vulneración del secreto bancario



Apéndice E: Plan del etiquetado de la información de Barclays

Tabla E1: **Plan del etiquetado de la información de Barclays**

** La etiqueta Secreto bancario es específica de las jurisdicciones con secreto bancario.

Etiqueta	Definición	Ejemplos
Secreto bancario	La información relacionada con cualesquiera datos que identifiquen a un cliente (CID) directa o indirectamente de Suiza.La clasificación «Secreto bancario» se aplica a la información relacionada con cualesquiera datos que identifiquen a un cliente (CID) directa o indirectamente. Por lo tanto, no resulta adecuado un acceso por parte de todos los empleados, ni siquiera de los que se encuentran en la propia jurisdicción. El acceso a esta información solo lo requieren aquellas personas que lo necesiten para desempeñar sus funciones oficiales o responsabilidades contractuales. Ninguna divulgación, acceso o uso compartido autorizados tanto interna como externamente de dicha información por parte de la entidad podría tener una repercusión crítica y podría dar lugar a procesos penales y tener consecuencias civiles y administrativos, tales como multas y pérdida de licencias bancarias, si se le revela a personal no autorizado tanto interno como externo.	• Nombre del cliente • Dirección del cliente • Firma • Dirección IP del cliente (otros ejemplos en el Apéndice D)

Etiqueta	Definición	Ejemplos
Secreta	Se clasificará la información como «secreta» si su divulgación no autorizada causara un perjuicio a Barclays, valorado de acuerdo con el marco de gestión de riesgos empresariales (ERMF) como «crítico» (financiero o no financiero). Esta información está restringida a un público específico y no debe distribuirse sin el permiso de la persona de la que se haya obtenido. El público puede incluir destinatarios externos con autorización explícita del responsable de información.	• Información sobre posibles fusiones o adquisiciones. • Información de planificación estratégica: empresarial y organizativa. • Determinada configuración de la seguridad de la información. • Determinados resultados de auditorías e informes. • Actas del Comité Ejecutivo. • Datos de autenticación o identificación y verificación: cliente y compañero. • Volúmenes generales de información de los titulares de tarjetas.

		• Pronósticos de beneficios o resultados financieros anuales (antes de hacerse públicos). • Cualquier elemento cubierto por un Acuerdo de confidencialidad formal.
Restringida – Interna	La información deberá clasificarse como Restringida – Interna si los destinatarios previstos son solo empleados de Barclays autenticados y Proveedores de servicios gestionados de Barclays con un contrato en vigor y restringida a un público específico. La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero). Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla.	• Estrategias y presupuestos. • Evaluaciones del personal. • Remuneración de los empleados y datos del personal. • Evaluaciones de la vulnerabilidad. • Resultados de auditorías e informes.
Restringida – Externa	La información deberá clasificarse como Restringida – Externa si los destinatarios previstos son empleados autenticados de Barclays y Proveedores de servicios gestionados de Barclays con un contrato en vigor y que esté restringida a un público específico o partes externas autorizadas por el responsable de la información. La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero). Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla.	• Planes de nuevos productos. • Contratos de clientes. • Contratos legales. • Información de clientes individuales o de escaso volumen que deba enviarse externamente. • Comunicaciones de clientes. • Materiales de oferta de nuevas emisiones (por ejemplo, folleto, nota sobre la oferta). • Documento de investigación definitivo. • Información no pública de carácter material no perteneciente a Barclays (MNPI). • Todos los informes de investigación. • Determinados materiales de marketing. • Comentario de marketing.
Sin restricción	Información destinada a su distribución general o que no causaría ninguna repercusión en la organización si se distribuyera.	• Material de marketing. • Publicaciones. • Anuncios públicos. • Anuncios de ofertas de trabajo.

		• Información sin impacto para Barclays.

Tabla E2: Plan del etiquetado de la información – Requisitos de tratamiento

** Requisitos de manipulación específicos para datos CID, a fin de garantizar su confidencialidad de acuerdo con los requisitos regulatorios

Fase del ciclo de vida	Requisitos del secreto bancario
Creación y etiquetado	De acuerdo con «Restringida-Externa» y: • A los activos se les asignará un responsable de CID.
Almacenamiento	De acuerdo con «Restringida-Externa» y: • Los activos se guardarán exclusivamente en soportes extraíbles durante el tiempo exigido explícitamente por una necesidad empresarial concreta, reguladores o auditores externos. • No deben guardarse en dispositivos/soportes portátiles grandes volúmenes de activos de información de secreto bancario. Para obtener más información, póngase en contacto con el equipo de ciberseguridad y seguridad de la información (en adelante CIS). • Los activos (físicos o electrónicos) no se almacenarán en lugares donde personas no autorizadas puedan verlos o acceder a ellos, de acuerdo con el principio basado en la necesidad de conocerlos y la necesidad de tenerlos. • Se emplearán prácticas seguras en el lugar de trabajo, como el bloqueo de los equipos de sobremesa y la política de no dejar nada sobre la mesa de trabajo, a fin de proteger los activos (ya sean en formato electrónico o físico). • Los activos de información en soportes extraíbles solo se utilizará para el almacenamiento durante el plazo exigido explícitamente y se guardarán y pondrán bajo llave cuando no se estén usando. • Las transferencias de datos ocasionales a soportes o dispositivos portátiles requieren la aprobación del responsable de los datos, el departamento de cumplimiento y el CIS.
Acceso y uso	De acuerdo con «Restringida-Externa» y: • No se eliminarán los activos ni se verán fuera de las instalaciones (de Barclays) sin una autorización formal del responsable del CID (o su delegado). • No se eliminarán los activos ni se verán fuera de la jurisdicción de reserva del cliente sin una autorización formal del responsable del CID (o su delegado) y del cliente (renuncia / Poder notarial limitado). • Se seguirán prácticas seguras de trabajo en emplazamientos remotos, para garantizar que nadie pueda espiar el trabajo por encima del hombro cuando se saquen de las instalaciones activos físicos.

	• Garantizar que las personas no autorizadas no puedan observar ni acceder a activos electrónicos que contengan CID utilizando un acceso restringido a aplicaciones empresariales.
Uso compartido	De acuerdo con «Restringida-Externa» y: • Los activos solo deben distribuirse de acuerdo con el «principio basado en la necesidad de conocerlos» Y dentro del personal y los sistemas de información de la jurisdicción con secreto bancario de origen. • La transferencia ocasional de activos en soportes extraíbles requiere la aprobación del responsable del activo de información y del CIS. • Se cifrarán las comunicaciones electrónicas en tránsito. • Los activos (en papel) enviados por correo deberán entregarse utilizando un servicio que exija un acuse de recibo. • Los activos solo deben distribuirse de acuerdo con el «principio basado en la necesidad de conocerlos».
Archivo y eliminación	De acuerdo con «Restringida-Externa»

*** La información de la configuración de seguridad de un sistema, resultados de auditorías y registros personales puede clasificarse como «Restringida - Interna» o «Secreta» según el impacto que pudiera tener para el negocio su revelación no autorizada.

Fase del ciclo de vida	Restringida – Interna	Restringida – Externa	Secreta
Creación e introducción	• A los activos se les asignará un responsable de la información.	• A los activos se les asignará un responsable de la información.	• A los activos se les asignará un responsable de la información.
Almacenamiento	• Los activos (físicos o electrónicos) no se almacenarán en áreas públicas (incluidas las áreas públicas de las instalaciones a las que puedan acceder visitantes sin supervisión).	• Los activos (físicos o electrónicos) no se almacenarán en lugares donde personas no autorizadas puedan verlos o acceder a ellos.	• Los activos (físicos o electrónicos) no se almacenarán en lugares donde personas no autorizadas puedan verlos o acceder a ellos.

	• No se dejará información en áreas públicas en las instalaciones a las que puedan acceder visitantes sin supervisión.	• Los activos almacenados en formato electrónico se protegerán mediante cifrado, o con controles de compensación apropiados, si hubiera un riesgo importante de que personal no autorizado pudiera acceder a ellos.	• Los activos almacenados en formato electrónico se protegerán mediante cifrado, o con controles de compensación apropiados, si hubiera un riesgo importante de que personal no autorizado pudiera acceder a ellos. • Todas las claves de cifrado privadas utilizadas para proteger los datos de Barclays, su identidad y/o reputación se protegerán mediante módulos de seguridad de hardware (HSM) con certificación FIPS 140-2 de Nivel 3 o superior.
Acceso y uso	• Los activos (físicos o electrónicos) no se dejarán en zonas públicas fuera de las instalaciones. • Los activos (físicos o electrónicos) no se dejarán en zonas públicas de las instalaciones a las que puedan acceder visitantes sin supervisión. • Los activos en formato electrónico se protegerán mediante controles de gestión de acceso lógico apropiados si fuera necesario.	• No se trabajará con activos (físicos o electrónicos) ni se dejarán desatendidos en lugares donde personas no autorizadas puedan verlos o acceder a ellos. Se puede trabajar con los activos si se han implantado los controles adecuados (por ejemplo: filtros de privacidad). • Los activos que se envíen a imprimir se recogerán inmediatamente de la impresora. Si no fuera posible, se usarán herramientas para la impresión segura. • Los activos en formato electrónico se protegerán mediante controles de gestión de acceso lógico apropiados.	• No se trabajará con activos (físicos o electrónicos) ni se dejarán desatendidos en lugares donde personas no autorizadas puedan verlos o acceder a ellos. Se puede trabajar con los activos si se han implantado los controles adecuados (por ejemplo: filtros de privacidad). • Para la impresión de activos se usarán herramientas de impresión segura. • Los activos en formato electrónico se protegerán mediante controles de gestión de acceso lógico apropiados.
Uso compartido	• Los activos en papel llevarán una etiqueta de información visible. La etiqueta irá como mínimo en la página que lleve el título. • Los activos electrónicos llevarán una etiqueta informativa clara.	• Los activos en papel llevarán una etiqueta de información visible. La etiqueta irá como mínimo en la página que lleve el título.	• Los activos en papel llevarán una etiqueta de información visible en cada página.

	• Los activos solo se distribuirán usando sistemas, métodos o proveedores aprobados por la organización. • Los activos solo se distribuirán a personas empleadas por la organización (o con una obligación contractual apropiada) o como parte de una necesidad comercial claramente reconocida, como una negociación de contrato.	• Los sobres que contengan activos en papel llevarán una etiqueta de información visible en la parte delantera. • Los activos electrónicos llevarán una etiqueta informativa clara. Las copias electrónicas de documentos de varias páginas llevarán una etiqueta de información visible en todas sus páginas. • Los activos solo se distribuirán usando sistemas, métodos o proveedores aprobados por la organización. • Los activos solo se distribuirán a personas empleadas por la organización (o con una obligación contractual apropiada) o como parte de una necesidad comercial claramente reconocida, como una negociación de contrato. • Los activos solo se distribuirán a personas que necesiten recibirlos por razones del negocio. • Los activos no se enviarán por fax a no ser que el remitente haya confirmado que los destinatarios están listos para recibirlos. • Los activos electrónicos se cifrarán utilizando un mecanismo de protección criptográfico cuando transiten fuera de la red interna.	• Los sobres que contengan activos en papel llevarán una etiqueta de información visible en la parte delantera e irán cerrados con un precinto de seguridad. Se introducirán dentro de otro sobre sin etiquetas antes de su distribución. • Los activos electrónicos llevarán una etiqueta informativa clara. Las copias electrónicas de documentos de varias páginas llevarán una etiqueta de información visible en todas sus páginas. • Los activos solo se distribuirán usando sistemas, métodos o proveedores aprobados por la organización. • Los activos solo se distribuirán a personas empleadas por la organización (o con una obligación contractual apropiada) o como parte de una necesidad comercial claramente reconocida, como una negociación de contrato. • Los activos solo se distribuirán a personas específicamente autorizadas por el propietario de la información. • Los activos no se enviarán por fax. • Los activos electrónicos se cifrarán utilizando un mecanismo de protección criptográfico cuando transiten fuera de la red interna. • Se mantendrá la cadena de custodia de los activos electrónicos.
Archivo y eliminación	• Los activos en papel se eliminarán utilizando un servicio de gestión de residuos confidencial.	• Los activos en papel se eliminarán utilizando un servicio de gestión de residuos confidencial.	• Los activos en papel se eliminarán utilizando un servicio de gestión de residuos confidencial.

	• Las copias de los activos electrónicos también se eliminarán de las «papeleras de reciclaje» del sistema de manera oportuna.	• Las copias de los activos electrónicos también se eliminarán de las «papeleras de reciclaje» del sistema de manera oportuna.	• Las copias de los activos electrónicos también se eliminarán de las «papeleras de reciclaje» del sistema de manera oportuna. • Los soportes en los que se hayan almacenado activos electrónicos «secretos» se limpiarán adecuadamente antes o durante la eliminación.