Obligaciones de control de proveedores externos

Seguridad de la información y ciberseguridad

Para proveedores clasificados como de bajo riesgo de ciberdelito

Versión 9.0 con fecha de abril de 2019

Título del 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 la 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 para proteger al proveedor contra ataques a la seguridad de la información o ciberataques, con arreglo a los códigos de prácticas recomendadas del sector (por ejemplo, NIST, SANS, ISO27001) y los requisitos industriales aplicables. El proveedor realizará evaluaciones del riesgo relacionado con la ciberseguridad o la seguridad de la información periódicamente e implementará los controles y adoptará las medidas que hagan falta para mitigar los riesgos identificados. El proveedor mantendrá políticas aprobadas por la dirección ejecutiva, así como unas normas de gestión de los ciberriesgos o los riesgos de información. El proveedor definirá las funciones y las responsabilidades en relación con la ciberseguridad o la seguridad de la información,	De no aplicarse este control, o Barclays o sus proveedores podrían no ser capaces de demostrar y no disponer de 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. 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. • 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.	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.

3. 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.
4. Computación en la nube	Se protegerá convenientemente todo uso de la computación en la nube (pública/privada/comunitaria/híbrida), como SaaS/PaaS/IaaS, que forme parte de los servicios prestados a Barclays. 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.
5. Protección contra malware	Deben establecerse controles y herramientas antimalware que protejan adecuadamente contra ataques de software malintencionado, como virus y otros tipos de malware.	Las soluciones contra el software malintencionado resultan esenciales para proteger los activos de información de Barclays contra el código malintencionado.
6. 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 basándose en los servicios que preste a Barclays: **Conexiones externas:** Todas las conexiones externas a la red deben documentarse, enrutarse a través de un firewall y ser comprobadas y aprobadas antes de establecerse, a fin de evitar infracciones de seguridad que permitan la filtración de datos. **Acceso inalámbrico:** Todo acceso inalámbrico a la red debe estar sujeto a protocolos de autorización, autenticación, separación y cifrado para evitar infracciones de seguridad **Prevención/detección de intrusiones:**	Si este servicio no se implementa, los atacantes podrían debilitar la seguridad de las redes externas o internas para obtener acceso al servicio o a los datos que contiene.

	Hay que desplegar herramientas y sistemas de detección y prevención de intrusiones en todas las ubicaciones apropiadas de la red, y en este sentido se debe supervisar la salida para detectar infracciones de ciberseguridad, incluidas las Amenazas persistentes avanzadas (APT, Advanced Persistent Threats). **Denegación de servicio distribuido (DDoS):** Hay que implementar un sistema defensivo exhaustivo en la red y en los sistemas clave para protegerlos en todo momento contra la interrupción del servicio debida a ciberataques. *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.*	
7. Protección de aplicaciones	El desarrollo de aplicaciones o software del proveedor se asegurará de que se han incorporado todas las actividades clave de la seguridad en el proceso de desarrollo de software para evitar interrupciones del servicio, vulnerabilidades de seguridad e infracciones de ciberseguridad. 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. El proveedor se asegurará de que el código fuente se ejecute, almacene y envíe a Barclays de forma segura.	Los controles que protegen el desarrollo de aplicaciones contribuyen a garantizar que se mantiene la seguridad de estas durante su despliegue.
8. Simulación de amenazas/ Pruebas de penetración/ Evaluación de la seguridad informática	El proveedor contratará a un proveedor de seguridad cualificado independiente para que efectúe pruebas de penetración o una evaluación de la seguridad informática de las aplicaciones y las infraestructuras informáticas en relación con los servicios que el proveedor 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. El proveedor utilizará un mecanismo coherente para registrar, clasificar y responder a vulnerabilidades identificadas.	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.
9. Tecnologías de protección de la	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.	Si no se aplica este control, los activos de Barclays o los activos utilizados por

seguridad y los activos	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 activos o sistemas en los que se almacenen o proceses deben estar protegidos contra manipulaciones físicas, pérdidas, daños o embargo, así como contra cambios o configuraciones inapropiadas. 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 se puedan recuperarse. Se configurarán los sistemas de manera segura para evitar vulneraciones innecesarias Debe establecerse la supervisión, auditoría y registro de sistemas para detectar actividades inapropiadas o malintencionadas.	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.
10. 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.	Los controles de LAM pertinentes ayudan a garantizar la protección de los activos de información contra un uso inadecuado.

	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; • proceso de revisión periódica del 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. • 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. 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.).	
11. 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:	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.

	• 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); • Intercambio seguro de información con terceros; y • Impresión o copia inadecuadas de información	
12. 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 B2), 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.
13. 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.

Apéndice A. Glosario

Definición	
Activo de información	Toda información que tenga valor, considerado en términos de confidencialidad, integridad y requisitos de disponibilidad. cualquier parte individual o grupo de información que tenga un valor para la organización. Suelen agruparse a un nivel alto (proceso empresarial).
Amenazas avanzadas persistentes (APT)	Una amenaza avanzada persistente (APT) es un ataque sigiloso a una red informática en el que una persona o grupo logra acceder a la red sin autorización y no es detectado durante un amplio espacio de tiempo.
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).
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.
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.
Privilegio mínimo	El nivel mínimo de acceso/permiso que permite al usuario o a una cuenta desempeñar su función empresarial.
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. 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, restringida a un público específico o partes externas autorizadas por el responsable de la información.	• Planes de nuevos productos. • Contratos de clientes. • Contratos legales. • Información de clientes individuales o de escaso volumen que deba enviarse externamente. • Comunicaciones de clientes.

	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.	• 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 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). • 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. • 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 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 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 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 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. • 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.

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 alto ejecutivo 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 C2) y se comunicará a la jurisdicción de secreto bancario correspondiente con carácter inmediato (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 C1 del Apéndice C), 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 C2 del Apéndice C. * «***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 B. 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 directos (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 C: Plan del etiquetado de la información de Barclays

Tabla C1: 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 B)

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.

	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.	• 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 C2: 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). • No se dejará información en áreas públicas en las instalaciones a las que	• 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	• 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

	puedan acceder visitantes sin supervisión.	compensación apropiados, si hubiera un riesgo importante de que personal no autorizado pudiera acceder a ellos.	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 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 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 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. • 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.