Supplier Control Obligation (SCO)

Requisitos de control de la dirección –

Información, seguridad física y cibernética, tecnología, planificación de recuperación, privacidad de datos, gestión de datos y EUDA

Control 1.0 – Gobernanza y rendición de cuentas

El proveedor debe contar con un marco estándar del sector establecido y coherente para la gestión de tecnologías de la información, seguridad de tecnologías de la información, seguridad física, planificación de recuperación, gestión de datos y gestión de información personal (privacidad/protección de datos) (NIST, ISO/IEC 27001, COBIT, BS10012, SSAE 18, ITIL), o un marco estándar similar de procedimientos recomendados del sector, para garantizar que las medidas de seguridad o contramedidas de su proceso, tecnología y entorno físico estén certificadas para funcionar de forma eficaz. Un programa de gobernanza bien estructurado a nivel empresarial debe garantizar que los conceptos básicos de disponibilidad, integridad y confidencialidad estén respaldados por controles adecuados. Los controles deben diseñarse para mitigar o reducir los riesgos de pérdida, interrupción o corrupción de la información, y el proveedor debe garantizar que los controles de requisitos de Barclays se aplican y funcionan de forma eficaz para proteger los servicios prestados a Barclays.

Debe desarrollarse un marco de gobernanza que incluya medidas de seguridad administrativas, técnicas y físicas para proteger los activos y la información/los datos de pérdidas accidentales o deliberadas, divulgación, alteración o destrucción, robo, uso inadecuado o uso indebido y acceso, uso o divulgación no autorizados.

El programa de gobernanza y rendición de cuentas debe incluir, entre otras cosas, las siguientes áreas:

- Políticas de gobernanza: se definirá, aprobará y mantendrá un conjunto de políticas de gobernanza, que se publicará y comunicará a los empleados del proveedor y a las partes correspondientes.
    - Políticas, procedimientos y programas estándar que crean, aplican y miden de manera efectiva la eficacia de la aplicación de políticas y estándares.
    - Un programa de gobernanza completo con una clara estructura de liderazgo y supervisión ejecutiva para crear una cultura de responsabilidad y conocimiento.
    - Comunicación continua de las políticas y los procedimientos aprobados a nivel organizativo.
    - Adaptación de los requisitos legales a las políticas y prácticas, protección de datos desde el diseño y otros controles para garantizar que las políticas y los procesos se implementan de forma eficaz.
- Las políticas para todas las áreas de dominio se revisarán a intervalos planificados o si se producen cambios significativos para asegurar su idoneidad, adecuación y eficacia continuas.
    - Debe comprobarse que las políticas y los procedimientos/estándares se revisan de forma rutinaria (al menos una vez al año o en el momento de producirse cualquier cambio importante, lo que ocurra antes).
    - Designar a una persona o personas/equipo con experiencia y debidamente cualificados que puedan actuar de enlace con Barclays para cumplir los requisitos de SCO, incluidos aquellos relacionados con la seguridad física y del edificio, la información y la ciberseguridad y la gestión de la información personal (privacidad de datos/protección de datos), la planificación de la recuperación, la gestión de datos y a la vez sean responsables de que se implementen y supervisen de forma eficaz los requisitos de control de Barclays o del proveedor.

    - El proveedor debe coordinar y alinear las funciones y responsabilidades del personal que implementa, gestiona y supervisa la eficacia de los controles con los subcontratistas/subencargados y el resto del personal interno.
- El proveedor deberá implementar un marco de control e infraestructuras seguro para proteger la organización frente a cualquier amenaza (incluyendo la ciberseguridad).
- El proveedor establecerá un programa de auditoría independiente para evaluar si se implementan y mantienen los controles del proveedor y deberá realizarse al menos una al año.

Orientación para el cliente de servicios en la nube (proveedor)

Una política de seguridad de la información para la computación en la nube debe definirse como una política específica del cliente de servicios en la nube. La política de seguridad de la información para la computación en la nube del cliente de servicios en la nube debe ser coherente con los niveles aceptables de riesgos de seguridad de la información de la organización en lo que concierne a su información y otros activos. Al definir la política de seguridad de la información para la computación en la nube, el cliente de servicios en la nube debe considerar lo siguiente:

- La información almacenada en el entorno de computación en la nube puede estar sujeta al acceso y la gestión por parte del proveedor de servicios en la nube.
- Los activos se pueden mantener en el entorno de computación en la nube; por ejemplo, programas de aplicaciones.
- Los procesos se pueden ejecutar en un servicio de nube virtualizado multiusuario.
- Los usuarios del servicio en la nube y el contexto en el que utilizan el servicio en la nube.
- Los administradores de servicios en la nube con acceso privilegiado al cliente del servicio en la nube.
- Las ubicaciones geográficas de la organización del proveedor de servicios en la nube y los países en los que el proveedor de servicios en la nube puede almacenar los datos del cliente de servicios en la nube (incluido el almacenamiento temporal).

La política de seguridad pertinente del cliente de servicios en la nube debe identificar al proveedor de servicios en la nube como un tipo de proveedor y gestionarlo de acuerdo con la política de seguridad. El objetivo de este proceso es mitigar los riesgos que introduce el acceso y la gestión de los datos del cliente de servicios en la nube asociados con el proveedor de servicios en la nube.

El cliente de servicios en la nube debe tener en cuenta las leyes y normativas pertinentes de las jurisdicciones que rigen la actuación del proveedor de servicios en la nube, además de las respectivas que le resultan vinculantes a él mismo. El cliente de servicios en la nube debe obtener pruebas del cumplimiento por parte del proveedor de servicios en la nube de las normativas y los estándares pertinentes necesarios para su negocio. Estas pruebas pueden ser también las declaraciones/los certificados que emitan auditores externos.

El proveedor notificará a Barclays por escrito, en cuanto se pueda hacer legalmente, si es objeto de una fusión, adquisición o cualquier otro cambio de propiedad.

Control 2.0 – Gestión de riesgos

El proveedor establecerá un programa de gestión de riesgos que evalúe, mitigue y controle de manera efectiva los riesgos de seguridad en todo el entorno controlado del proveedor.

El programa de gestión de riesgos debe incluir, entre otras cosas, las siguientes áreas:

- El proveedor debe contar con un marco de gestión de riesgos debidamente aprobado (p. ej., información personal si procesa datos de IP, información, ciberseguridad, seguridad física, tecnología, datos y recuperación de la planificación) y es capaz de demostrar su incorporación a la estrategia empresarial
- Deben llevarse a cabo evaluaciones de riesgos formales alineadas con el marco de riesgos como mínimo anualmente o a intervalos planificados, empleando un enfoque basado en el riesgo, o activarse cuando se produzcan determinados acontecimientos; por ejemplo, como respuesta a un incidente o las lecciones aprendidas asociadas (y junto con cualquier cambio en los sistemas de información o en el edificio o espacio físico) para determinar la probabilidad y el impacto de todos los riesgos identificados empleando métodos cualitativos y cuantitativos. La probabilidad y el impacto asociados a los riesgos inherentes y residuales se determinarán de forma independiente, teniendo en cuenta todas las categorías de riesgo (por ejemplo, resultados de auditoría, análisis de amenazas y vulnerabilidades y cumplimiento normativo).
- Deben establecerse y mantenerse criterios de riesgo, como:
  - los criterios de aceptación del riesgo, y
  - los criterios para realizar evaluaciones de riesgos.
- Se han de identificar los riesgos:
  - aplicando el proceso formal de evaluación de riesgos para identificar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información en el ámbito del marco de riesgos, e
  - identificando a los propietarios de los riesgos.
- Se deben analizar los riesgos:
  - evaluando las posibles consecuencias que se producirían si se identificasen los riesgos,
  - sopesando la probabilidad real de que se produzcan los riesgos identificados, y
  - determinando los niveles de riesgo.
- Se han de evaluar los riesgos:
  - comparando los resultados del análisis de riesgos con los criterios de riesgo establecidos, y
  - priorizando los riesgos analizados para su tratamiento
- Tratamiento de riesgos:
  - selección de opciones apropiadas de tratamiento de los riesgos que tengan en cuenta los resultados de las evaluaciones de riesgos,

  - determinación de los controles necesarios para aplicar las opciones de tratamiento de riesgos escogidas,
  - elaboración de una declaración de aplicabilidad que contenga los controles y la justificación necesarios para inclusiones, tanto si se implementan como si no, y
  - garantía del proveedor de que los riesgos identificados se minimicen o eliminen en el entorno a través de la priorización del riesgo y la aplicación de contramedidas. El proveedor debe supervisar continuamente las contramedidas para que sean eficaces.
- El proveedor debe realizar, como mínimo, una evaluación anual de los riesgos relacionados con la información, seguridad cibernética, seguridad física, gestión de la información personal (privacidad/protección de datos) y planificación de la recuperación. En función de los entornos específicos con amenazas actuales y emergentes, el proveedor debe considerar una frecuencia mayor.
  - Evaluar al menos anualmente los sitios críticos para el funcionamiento de los procesos/servicios proporcionados a Barclays (incluidos los centros de datos).
- La organización conservará información documentada sobre el proceso de evaluación de riesgos de seguridad de la información.
- Las evaluaciones de riesgos asociadas a los requisitos de gobernanza de datos (incluida la información personal si se tratan datos de IP) deben tener en cuenta lo siguiente:
  - Clasificación y protección de los datos frente al uso y acceso no autorizados, así como frente a la pérdida, destrucción y falsificación.
  - Conocimiento de los lugares en los que se almacenan y transmiten datos sensibles entre aplicaciones, bases de datos, servidores e infraestructuras de redes.
  - Cumplimiento de los períodos de retención definidos y requisitos de eliminación al final de la vida útil.
- El proveedor, mientras actúa como responsable o encargado del tratamiento, debe evaluar el posible riesgo para la privacidad al procesar grandes volúmenes de datos confidenciales de Barclays para garantizar que cualquier cambio en la manipulación/tratamiento de los datos de Barclays no suponga un riesgo a la privacidad.
- El proveedor debe desarrollar e implementar la estructura de gobernanza de la organización para permitir una comprensión continua de las prioridades de gestión de riesgos de la organización, fundamentadas con base en el riesgo de privacidad.

Control 3.0 – Funciones y responsabilidades

El proveedor es responsable de garantizar que todos sus empleados, incluidos, entre otros, los contratistas, subcontratistas y subencargados implicados en la prestación de servicios a Barclays, conozcan y cumplan los requisitos de control de Barclays. El proveedor debe asegurarse de que un equipo adecuado de especialistas y/o personas con las habilidades apropiadas, funciones y responsabilidades definidas para apoyar y/o gestionar los requisitos de control de Barclays trabajen de forma eficaz para proteger los servicios de Barclays.

El proveedor definirá y comunicará las funciones y responsabilidades para ofrecer un soporte eficaz a los requisitos de control de Barclays. Estas funciones y responsabilidades 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.

Es responsabilidad del proveedor asegurarse de que sus empleados, contratistas, subcontratistas/subencargados estén familiarizados con los requisitos de control de este estándar y las políticas y estándares asociados, y los cumplan. El proveedor debe designar un punto de contacto para que se comunique con Barclays en caso de que alguna apelación se derive del incumplimiento de los requisitos de control. Los requisitos contractuales específicos se deben remitir por escrito a los subcontratistas/subencargados del proveedor.

Orientación para el cliente de servicios en la nube (proveedor)

El cliente de servicios en la nube debe acordar con el proveedor de servicios en la nube una asignación adecuada de las funciones y responsabilidades de seguridad de la información, y confirmar que puede cumplir las funciones y responsabilidades asignadas. Las funciones y responsabilidades de ambas partes deben establecerse en un acuerdo. El cliente de servicios en la nube debe identificar y gestionar su relación con la función de atención y asistencia al cliente del proveedor de servicios en la nube.

El cliente de servicios en la nube debe definir o ampliar sus políticas y procedimientos existentes de acuerdo con su uso de servicios en la nube, así como informar a sus usuarios de servicios en la nube acerca de sus funciones y responsabilidades en el uso del servicio en la nube.

Control 4.0 – Educación y conocimiento

El proveedor debe ejecutar de forma continua un programa de formación para todos sus empleados, incluidos contratistas, empleados temporales y consultores. Todos los empleados del proveedor que trabajen para los servicios de Barclays o tengan acceso a datos/información u otros activos físicos de Barclays deberán recibir formación y conocimiento apropiado, y actualizaciones regulares en procedimientos, procesos y políticas organizativos correspondientes a su función profesional en lo que atañe a la organización. Los niveles de formación y concienciación deben preparar a los empleados del proveedor para que desempeñen sus funciones de forma segura y garantizar que los empleados del proveedor comprendan sus responsabilidades al acceder o procesar cualquier dato de Barclays, incluidos los datos personales. Los registros del programa que se está llevando a cabo deben registrarse en una plataforma adecuada de gestión del aprendizaje o mediante un proceso manual.

El proveedor debe asegurarse de que todos sus empleados completen la formación obligatoria y una formación de conocimiento, que incluirá información sobre ciberseguridad, seguridad física, planificación de recuperación, gestión de información personal (privacidad/protección de datos), gestión de datos, gestión de servicios informáticos, EUDA y protección de los datos de Barclays en el plazo de un mes desde su incorporación a la organización y/o al unirse a los servicios de Barclays. Además de actualizar la formación anualmente, el proveedor debe asegurarse de realizar pruebas para verificar que sus empleados comprenden sus responsabilidades y son conscientes de los riesgos asociados con los datos de Barclays, las leyes y normativas aplicables, así como otros factores que podrían afectar al

rendimiento o suponer un riesgo para el banco. Toda la formación impartida se debe registrar y mantener para todos los empleados del proveedor que trabajen en los servicios de Barclays y deberá entregarse a Barclays para su inspección previa solicitud.

El proveedor debe asegurarse de que su programa de formación de conocimiento incluye los siguientes temas sobre ciberseguridad: ingeniería social y amenazas internas. Se recomienda que el proveedor realice pruebas de simulación de ataques de ingeniería social utilizando técnicas como simulaciones de phishing para todos los empleados a nivel empresarial con supervisión continua para asegurar que la amenaza de tales riesgos se entienda claramente y mitigar los problemas identificados.

Los grupos de alto riesgo, como las personas con acceso privilegiado a los sistemas o en funciones sensibles (incluyendo usuarios privilegiados, desarrolladores y personal de asistencia, altos ejecutivos, personal de seguridad de la información y terceras partes interesadas) deben recibir formación de conocimiento relativa a situaciones de seguridad de la información y seguridad física de acuerdo con sus funciones y responsabilidades.

Todo el personal de seguridad física (ya sea empleado del proveedor, un propietario de la propiedad o un proveedor externo) debe contratarse a través de un proveedor de servicios acreditado y con licencia de acuerdo con la legislación local y, cuando así lo requiera la jurisdicción, debe tener licencia personal para asumir obligaciones de seguridad. El personal de seguridad física debe recibir formación en materia de seguridad acorde con su función y responsabilidades. Toda la formación impartida debe documentarse y se debe mantener un registro de formación para todo el personal de seguridad, que deberá entregarse a Barclays para su inspección previa solicitud.

El proveedor debe asegurarse de que su personal externo con acceso a datos que contengan información personal sea consciente de los riesgos para la privacidad y cumpla sus obligaciones y responsabilidades de acuerdo con las políticas, procesos, procedimientos, acuerdos y valores de privacidad de la organización relacionados. Toda la formación impartida debe documentarse y se debe mantener un registro de formación para todo el personal, que deberá entregarse a Barclays para su inspección previa solicitud.

El proveedor debe formar a los empleados para que realicen de forma eficaz sus tareas en materia de gestión de datos (gestión de elementos de datos críticos o aplicaciones gestionadas por terceros).

El propietario de la EUDA del proveedor debe identificar a los empleados del proveedor con responsabilidades de EUDA y asegurarse de que completan la formación y poseen el conocimiento adecuado para cumplir con su función al menos una vez al año, así como de que conservan pruebas que demuestren la conformidad con el control.

Orientación para el cliente de servicios en la nube (proveedor)

El cliente de servicios en la nube debe añadir los siguientes elementos a los programas de conocimiento, educación y formación para los gestores empresariales del servicio en la nube, los administradores de servicios en la nube, los integradores de servicios en la nube y los usuarios de servicios en la nube, incluidos los empleados y contratistas pertinentes:

- Estándares y procedimientos para el uso de servicios en la nube.
- Riesgos de seguridad de la información relacionados con los servicios en la nube y cómo gestionarlos.
- Riesgos del sistema y del entorno de red con el uso de servicios en la nube.
- Consideraciones legales y reglamentarias aplicables.

Se deben proporcionar programas de conocimiento, educación y formación sobre la seguridad de la información acerca de los servicios en la nube a los directores y supervisores, incluidos los de las unidades de negocio. Estos esfuerzos apoyan una coordinación eficaz de las actividades de seguridad de la información.

Control 5.0 – Gestión de incidentes

El proveedor debe disponer de un marco de gestión de incidentes establecido que gestione, contenga y elimine o mitigue de forma eficaz un incidente y su causa subyacente del entorno del proveedor.

El proveedor contará con un procedimiento de gestión de crisis e incidentes que incluya el proceso para remitir incidentes o crisis a instancias superiores en Barclays. El proveedor se asegurará de que se efectúen pruebas, como mínimo de carácter anual, de los procesos y equipos de respuesta a incidentes/crisis para asegurarse de que el proveedor pueda responder a cualquier incidente de manera eficaz y eficiente. El proveedor también debe probar su capacidad para notificar dentro de los plazos definidos a los contactos apropiados acerca de un incidente y demostrarlo a Barclays cuando así se le solicite.

El proveedor debe disponer de planes de respuesta documentados a los incidentes que definan las funciones del personal del proveedor, así como fases de gestión/tratamiento de incidentes:

- Responsabilidades y procedimientos: se establecerán responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes.
- Notificación de incidentes: los incidentes se notificarán a través de los canales de gestión adecuados lo antes posible y el mecanismo de notificación debe ser sencillo y accesible para todos los empleados y contratistas del proveedor.
- Evaluación de incidentes: los incidentes deben evaluarse para determinar la criticidad, clasificación y respuesta necesarias.
    - Clasificación de incidentes: se ha de establecer una escala de clasificación de incidentes y decidir si el evento debe clasificarse como incidente. La clasificación y priorización de incidentes puede ayudar a identificar el impacto y el alcance de un incidente.
- Respuesta a incidentes: los incidentes se responderán de acuerdo con los procedimientos documentados de gestión de incidentes del proveedor.

  - Contención de incidentes: utilizar personas, procesos y capacidades tecnológicas para contener de forma efectiva y rápida los incidentes en el entorno.
  - Eliminación/mitigación de amenazas: potenciar al personal, los procesos y las capacidades tecnológicas para eliminar/mitigar de manera efectiva las amenazas de seguridad y/o sus componentes en el entorno.
- Aprendizaje de incidentes: el conocimiento obtenido del análisis y la resolución de incidentes se utilizará para reducir la probabilidad o el impacto de incidentes futuros.
- Recopilación de pruebas: el proveedor definirá y aplicará procedimientos para la identificación, recopilación, adquisición y conservación de la información, que puede servir como prueba.

Información posterior al incidente: tras la alteración del servicio, se le presentará a Barclays un informe posterior al incidente en el plazo máximo de cuatro semanas naturales desde que se restaurase el nivel de funcionamiento habitual del servicio. Requisitos mínimos del informe posterior al incidente:

- los acontecimientos relacionados con la situación;
- la forma en que se gestionó el incidente o la crisis;
- el análisis de la raíz del problema;
- si el proveedor o Barclays lo clasifican como un «evento de riesgo» (es decir, suficientemente importante para notificarlo o remitirlo a las partes interesadas pertinentes de acuerdo con las políticas aplicables que le consten al proveedor);
- si representa un «riesgo de comportamiento» (es decir, si el proveedor está tratando directamente con clientes de Barclays);
- cualquier sistema de reparación para los clientes de Barclays que le conste al proveedor;
- una mejora continua para evitar que se repita, y
- el proveedor procurará determinar que las actividades de respuesta se mejoren en la medida de lo posible incorporando las lecciones aprendidas de las actividades de detección/respuesta actuales y anteriores.

Comunicación: el proveedor deberá nombrar un punto de contacto para los incidentes de seguridad que será el enlace con Barclays en caso de producirse alguna crisis. El proveedor notificará a Barclays los datos de contacto de dicha persona y cualquier cambio en los mismos, incluido el horario de contacto y los números de teléfono.

Dichos datos deben incluir: - Nombre, responsabilidades dentro de la organización, función, correo electrónico y teléfono

Si en cualquier momento el proveedor confirma que algún incidente afecta a los servicios, sistemas o datos de Barclays, lo notificará inmediatamente.

Cuando el proveedor tenga conocimiento de un incidente cibernético, incluido mediante notificación de una entidad de Barclays, deberá, de inmediato y en ningún caso más tarde de lo exigido por la ley aplicable, o bien, en defecto de tal requisito, en un plazo de 48 horas, tras conocer la existencia del incidente cibernético por primera vez, notificar a Barclays enviando un correo electrónico a gcsojoc@barclays.com. Dicho correo incluirá toda la información relevante, dentro de lo posible, como (a) las categorías y el número aproximado de registros de datos de Barclays

afectados y, si procede, las categorías y el número aproximado de interesados afectados; (b) el impacto y las potenciales consecuencias del incidente cibernético para Barclays y, en su caso, los interesados afectados, y (c) las medidas correctivas y atenuantes adoptadas o que debe poner en marcha el proveedor.

En caso de robo, uso o divulgación no autorizados, ya sean supuestos reales o presuntos, de cualquier dato personal protegido debido a un incumplimiento de las garantías de seguridad del proveedor (o de su personal), o bien en caso de acceso no autorizado a los datos personales protegidos desde o mediante el proveedor (o su personal), o si se pierden, dañan o destruyen los datos personales protegidos en posesión o control del proveedor o su personal, o en caso de darse otro tipo de tratamiento no autorizado de cualquier dato personal protegido, el proveedor notificará la situación a Barclays tan pronto como sea posible y, en cualquier caso, en un plazo de 24 horas tras ser consciente del incidente, enviando un correo electrónico a gcsojoc@barclays.com. Además, el proveedor cooperará plenamente con Barclays y prestará toda la ayuda necesaria en relación con tal evento, lo que incluye facilitar toda la información relevante, como datos, tiempo, ubicación, tipo de incidente, impacto, estado y acciones de mitigación puestas en marcha.

Si se recurre a un subcontratista/subencargado para prestar el servicio, si este mantiene o trata datos/información o activos de Barclays, el proveedor deberá obtener el consentimiento de Barclays. El proveedor debe tener una relación contractual con los subcontratistas/subencargados y ha de asegurarse de que estos están acreditados con un marco estándar de procedimientos recomendados del sector similar que funcione de forma eficaz para proteger los datos/la información de Barclays que tratan o almacenan. En caso de incidentes con el subcontratista/subencargado, el proveedor debe asegurarse de que se sigue el proceso de notificación de incidentes anteriormente expuesto.

Orientación para el cliente de servicios en la nube (proveedor)

El cliente de servicios en la nube debe verificar la asignación de responsabilidades para la gestión de incidentes y ha de asegurarse de que se cumplen todos sus requisitos. El cliente de servicios en la nube debe solicitar al proveedor de servicios en la nube información sobre los mecanismos para que:
– el cliente de servicios en la nube informe al proveedor de servicios en la nube de un incidente/evento que haya detectado;
– el cliente de servicios en la nube reciba informes sobre incidentes/eventos que detecte el proveedor de servicios en la nube;
– el cliente de servicios en la nube realice un seguimiento del estado de un evento de seguridad de la información que se haya notificado.

Control 6.0 – Gestión de activos informáticos (hardware y software)

El proveedor debe tener y operar un programa de gestión de activos eficaz durante todo el ciclo de vida de estos. La gestión de activos debe gobernar el ciclo de vida de los activos desde su adquisición hasta su retirada o eliminación segura, aportando visibilidad y seguridad a todas las clases de activos en el entorno.

El proveedor mantendrá un inventario exacto, preciso y actualizado de activos críticos para la empresa ubicados en todos los centros y/o ubicaciones geográficas que presten servicio a Barclays, incluyendo los equipos de Barclays alojados en instalaciones del proveedor, un subcontratista/subencargado facilitado por Barclays, y garantizar que se efectúe como mínimo una prueba anual para validar que el inventario está actualizado, está completo y es correcto, además de demostrar los resultados ante Barclays cuando se solicite.

El proceso de gestión de activos debe incluir las siguientes áreas:

- Inventario de activos: se identificarán los activos asociados a la información y los centros de tratamiento de la información, y se elaborará y mantendrá un inventario de dichos activos.
    - El proveedor debe mantener un inventario actualizado y preciso de todos los activos tecnológicos con potencial para almacenar o tratar información.
    - El proveedor debe disponer de un inventario de activos de información preciso y actualizado para los equipos de Barclays alojados en sus instalaciones y/o para los activos informáticos que Barclays le proporcione.
    - Los proveedores con una configuración de Nivel 1, 2 y 3 deben mantener inventarios de activos actualizados, completos y precisos (incluyendo ordenadores de sobremesa, portátiles, equipos de red, tokens RSA y cualquier activo suministrado por Barclays).
    - El proveedor reconciliará todos los activos de Barclays (hardware y software) con una periodicidad anual y lo certificará a Barclays (Dirección General de Seguridad - equipo TPSecM).
    - Se mantendrá un inventario actualizado de todos los productos de software implementados y autorizados necesarios para la prestación de servicios de Barclays y para el cumplimiento de los términos y condiciones de las respectivas licencias.
    - El inventario de activos del cliente de servicios en la nube debe tener en cuenta la información y los activos asociados, almacenados en el entorno de computación en la nube. Los registros del inventario deben indicar dónde se mantienen los activos; por ejemplo, mediante la identificación del servicio en la nube.
- Uso aceptable de los activos: se identificarán, documentarán e implementarán las reglas para el uso aceptable de la información y los activos asociados con las instalaciones de tratamiento de la información.
    - Los activos no autorizados deben eliminarse de la red.
    - El proveedor debe garantizar que se apliquen procesos eficientes y efectivos para mitigar las tecnologías no compatibles y el final de la vida útil, retirada y destrucción de activos y datos para eliminar el riesgo de comprometer los datos.
    - Se han de etiquetar el software y el hardware no compatibles como tales en el sistema de inventario.
- Devolución de activos: todos los empleados y subcontratistas/subencargados del proveedor (en el ámbito de la prestación de servicios a Barclays) devolverán todos los activos de Barclays en su posesión al término de su relación laboral, contrato o acuerdo.
    - Los supuestos de activos de Barclays «perdidos o robados» deben investigarse adecuadamente y comunicarse a Barclays de conformidad con el control de gestión de incidentes.
    - En caso de pérdida o robo de activos del proveedor que contengan información de Barclays, este supuesto deberá notificarse a Barclays conforme al control de gestión de incidentes.

El proveedor informará de inmediato a Barclays de los cambios conocidos en su capacidad para prestar servicios de asistencia técnica, ya sean directos o indirectos, para los activos informáticos utilizados para prestar los servicios a Barclays, incluso cuando los productos presenten aspectos de seguridad vulnerables. Asimismo, se asegurará de actualizar o retirar dichos activos cuando proceda.

Transporte de activos de Barclays: el proveedor deberá garantizar que todos los activos y los datos de Barclays se transportan de manera segura con controles proporcionales acordes al valor y la clasificación de los activos y datos en cuestión (tanto desde una perspectiva de daños económicos como para la reputación) y el entorno de amenazas en el que se esté produciendo el transporte.

Gestión de la asistencia técnica (proveedor)

El proveedor informará de inmediato a Barclays de los cambios conocidos en su capacidad para prestar servicios de asistencia técnica, ya sean directos o indirectos, para los activos informáticos utilizados para prestar los servicios a Barclays, incluso cuando los productos presenten aspectos de seguridad vulnerables. Asimismo, se asegurará de actualizar o retirar dichos activos cuando proceda.

El proveedor deberá asegurarse de que se identifiquen y comuniquen a Barclays los posibles cambios en los acuerdos de asistencia técnica de terceros clave en relación con los activos afectados con el fin de garantizar que la información de los productos se mantenga actualizada.

Orientación para el cliente de servicios en la nube (proveedor)

El inventario de activos del cliente de servicios en la nube debería tener en cuenta la información y los activos asociados, almacenados en el entorno de computación en la nube. Los registros del inventario deberían indicar dónde se mantienen los activos; por ejemplo, mediante la identificación del servicio en la nube.

La instalación de software con licencia comercial en un servicio en la nube puede provocar un incumplimiento de los términos de licencia del software. El cliente de servicios en la nube debe disponer de un procedimiento para identificar los requisitos de licencia específicos de la nube antes de permitir la instalación de cualquier software con licencia en un servicio en la nube. Se debe prestar especial atención a los casos en los que el servicio en la nube es flexible y ampliable, y si el software se puede ejecutar en más sistemas o núcleos de procesador de los permitidos por los términos de licencia.

Control 7.0 – Eliminación/destrucción segura de activos físicos y mantenimiento de datos de información electrónica

La destrucción o el borrado seguros de los activos de información de Barclays, incluidas las imágenes utilizadas para el servicio, almacenadas en forma física y/o electrónica, deben realizarse con un método seguro adecuado y verificar que los datos de Barclays no son recuperables.

El proveedor debe establecer procedimientos con procesos empresariales y medidas técnicas de apoyo para desechar lo oportuno de forma segura mediante métodos de separación adecuados, incluidos, entre otros, la limpieza, purga y destrucción para la retirada/el borrado y la recuperación de forma segura de datos de Barclays de todos los medios de almacenamiento, de manera que los datos de Barclays sean irrecuperables por medios informáticos conocidos.

Los datos de Barclays almacenados en medios de almacenamiento deben borrarse hasta un nivel suficiente como para que no sean recuperables, preferiblemente utilizando técnicas de borrado de datos apropiadas como borrado seguro, purga, eliminación o destrucción de datos, o métodos basados en software para sobrescribir los datos o utilizar el marco estándar del sector para la eliminación de datos (NIST). Todos los equipos (activos de información) deben desecharse al final de su vida útil (defectuosos, descartados debido a la retirada del servicio o puesto que ya no se necesitan, utilizados en un ensayo o una prueba de concepto, los servicios de borrado de datos pueden utilizarse para equipos que se van a reutilizar, etc.).

Los requisitos de eliminación se aplican a los subcontratistas/subencargados del proveedor a los que se recurre para prestar el servicio a Barclays.

La eliminación de información impresa deberá ser triturada hasta el mínimo de la norma P4 DIN66399 utilizando una trituradora de corte transversal (esto incluye información de tarjetas de pago) o bien se podrá incinerar de conformidad con BS EN15713:2009.

Para Barclays, la evidencia de la eliminación de los datos debe mantenerse, proporcionando un registro de auditoría, evidencia y seguimiento, y debe incluir lo siguiente:

- La prueba de la destrucción y/o eliminación (incluyendo la fecha en que se realizó y el método utilizado).
- Registros de auditoría del sistema para la eliminación.
- Certificados de eliminación de datos.
- Identificación de la parte encargada de la eliminación (incluyendo cualquier socio de eliminación, terceras partes o contratistas).
- Informe de destrucción y verificación para confirmar el éxito o el fracaso de cualquier proceso de destrucción o eliminación (es decir, si se sobrescriben los datos, por ejemplo, se debe proporcionar un informe que detalle los sectores que no se han podido borrar).

Durante la salida del servicio a Barclays, el proveedor debe asegurarse de que los datos de Barclays se han destruido de forma segura tras la notificación y autorización de Barclays.

Orientación para el cliente de servicios en la nube (proveedor)

El cliente de servicios en la nube debe solicitar la confirmación de que el proveedor de servicios en la nube cuenta con políticas y procedimientos para la eliminación segura o la reutilización de los recursos. Asimismo, el cliente de servicios en la nube debe solicitar una descripción documentada del proceso de terminación del servicio que cubra la devolución y eliminación de sus activos, seguida del borrado de todas las copias de dichos activos de los sistemas del proveedor del servicio en la nube. Dicha descripción debe enumerar todos los activos y documentar el calendario para la terminación del servicio, que debe ocurrir de manera oportuna.

Control 8.0 – Clasificación de la información y gestión de datos

El proveedor contará con un marco/plan apropiado y establecido de clasificación y gestión de la información (alineado con los procedimientos recomendados del sector y/o los requisitos de Barclays) que incluya los siguientes elementos:

- Clasificación de la información: la información se clasificará en términos de criticidad y sensibilidad a la divulgación o modificación no autorizada.
- Etiquetado de la información: se elaborará y aplicará un conjunto apropiado de procedimientos para el etiquetado de la información de conformidad con el plan de clasificación de la información adoptado por el proveedor.
- Gestión de activos: los procedimientos de gestión de activos se desarrollarán y aplicarán de conformidad con el plan de clasificación de la información adoptado por el proveedor.

El proveedor también debe garantizar que todo el personal conozca los requisitos de tratamiento y etiquetado de proveedores/Barclays y cómo aplicar correctamente la clasificación de la información correcta.

El proveedor deberá remitirse al Plan del etiquetado de la información y los requisitos de tratamiento (Apéndice A, Tabla A1 y A2) de Barclays, o un plan alternativo para garantizar que protege la información de Barclays que mantiene y/o trata. Este requisito se aplica a todos los activos de información que se mantengan o traten en nombre de Barclays, e incluye a subcontratistas y subencargados.

Orientación para el cliente de servicios en la nube (proveedor)

El cliente de servicios en la nube debe etiquetar la información y los activos asociados mantenidos en el entorno de computación en la nube de acuerdo con los procedimientos de etiquetado adoptados. Si procede, se puede adoptar la funcionalidad proporcionada por el proveedor de servicios en la nube que admite el etiquetado.

Control 9.0 – Copia de seguridad de información/datos

El proveedor debe contar con un proceso de copia de seguridad de los datos establecido para garantizar que se realiza una copia de seguridad de la infraestructura de forma regular y precisa con el fin de evitar la pérdida de datos. Se debe realizar una copia de seguridad de la información almacenada en formato electrónico para mantenerla segura en caso de fallo del sistema, desastre o incidente. Los planes de copia de seguridad se deben desarrollar, probar e implementar para abordar la política específica del tema sobre copias de seguridad.

Para los planes de copia de seguridad se deben tener en cuenta los siguientes elementos:

- Determinación de los requisitos de copia de seguridad: los requisitos de las copias de seguridad de los datos se definen, registran y acuerdan claramente con la empresa.
- Elaboración de registros precisos y completos de las copias de seguridad e implementación de procedimientos de restauración documentados.
- Frecuencia de las copias de seguridad (por ejemplo, copia de seguridad completa o diferencial).
- Almacenamiento seguro de las copias de seguridad.

    - Almacenamiento de las copias de seguridad en una ubicación remota segura, a una distancia suficiente que permita evitar cualquier daño causado por un desastre en el sitio principal.
- Comprobación periódica de los soportes para las copias de seguridad para garantizar que se puedan utilizar en caso de emergencia cuando sea necesario. Comprobación de la capacidad de restauración de los datos de las copias de seguridad en un sistema de prueba, sin sobrescribir el soporte de almacenamiento original en caso de que el proceso de copia de seguridad o restauración falle y provoque daños o pérdidas irreparables en los datos.
- Detección de cualquier pérdida accidental de datos antes de realizar la copia de seguridad.
- Validación de que la copia de seguridad es adecuada para su finalidad.

Se ha de comprobar que las copias de seguridad estén adecuadamente protegidas por medios de seguridad físicos o encriptados cuando estén almacenadas, así como cuando se muevan por la red. Esto incluye las copias de seguridad remotas y los servicios en la nube.

Se ha de comprobar que se realiza una copia de seguridad de todos los datos de Barclays de forma periódica según los requisitos de servicio.

Si el proveedor de servicios en la nube proporciona la capacidad de copia de seguridad como parte del servicio en la nube, el cliente de servicios en la nube debe solicitar las especificaciones de esta capacidad de copia de seguridad al referido proveedor de servicios en la nube. El cliente de servicios en la nube también debe verificar que se cumplen sus requisitos de copia de seguridad. El cliente de servicios en la nube deberá encargarse de implementar capacidades de copia de seguridad cuando el proveedor de servicios en la nube no las proporcione.

El proveedor se asegurará de que todos los servicios y sistemas informáticos utilizados en la prestación de servicios a Barclays cuenten con procesos de copia de seguridad y restauración adecuados que funcionen conforme a las necesidades de Barclays y cuya eficacia se demuestre periódicamente.

El proveedor se asegurará de que todos los soportes para copias de seguridad vinculados a la prestación de servicios a Barclays, así como los sistemas de gestión y almacenamiento de dichos soportes, sigan siendo seguros y fiables en todo momento.

Control 10.0 – Gestión de la configuración

El proveedor debe definir e implementar procesos y herramientas para aplicar las configuraciones definidas (incluidas las configuraciones de seguridad) para el hardware, el software, los servicios (incluidos los servicios en la nube) y las redes, para los sistemas recién instalados y para los sistemas operativos a lo largo de su vida útil.

Gestión de las configuraciones: el proveedor deberá contar con un conjunto de configuraciones aprobadas y probadas para hardware, software y redes. Se deben registrar y se debe mantener un registro de todos los cambios en la configuración. Estos registros deben almacenarse de forma segura. Esto se puede lograr de varias formas, como bases de datos de configuración o plantillas de configuración.

Supervisión de las configuraciones: se deben supervisar las configuraciones con un conjunto completo de herramientas de gestión de sistemas (por ejemplo, servicios de mantenimiento, asistencia remota, herramientas de gestión empresarial, software de copia de seguridad y restauración) y deben revisarse periódicamente para verificar los ajustes de configuración, evaluar la fortaleza de las contraseñas y analizar las actividades realizadas. Las configuraciones reales se pueden comparar con las plantillas objetivo definidas. Se deberá abordar cualquier desviación, ya sea mediante la aplicación automática de la configuración objetivo definida o mediante un análisis manual de la desviación seguido de acciones correctivas.

Registro y mantenimiento de elementos de configuración: el proveedor mantendrá un registro exacto y completo de todos los artículos de configuración dentro de este ámbito que se utilicen para prestar servicios a Barclays (lo que incluye las responsabilidades y las dependencias o asignaciones superiores o inferiores). El proveedor implantará controles para garantizar el mantenimiento continuado de la precisión e integridad de los datos.

Aislamiento del entorno de producción: el proveedor se asegurará de que los servicios de producción prestados a Barclays no dependan de ningún componente no productivo, a fin de evitar una falta de seguridad o fiabilidad en la prestación del servicio.

Configuración segura: el proveedor contará con un marco establecido para garantizar que todos los sistemas/equipos de red configurables se configuran de forma segura de acuerdo con los procedimientos recomendados del sector (como NIST, SANS, CIS).

- Establece políticas, procedimientos/medidas organizativas y herramientas que permiten la implementación de las normas de configuración de seguridad conforme a los procedimientos recomendados del sector para todos los dispositivos de red y sistemas operativos autorizados, aplicaciones y servidores.
- Realiza comprobaciones de cumplimiento regulares (anuales como mínimo) para garantizar que los incumplimientos de los estándares de seguridad básicos se rectifiquen inmediatamente. Se establecen comprobaciones y seguimientos apropiados para garantizar que se mantenga la integridad de los equipos/dispositivos.
- Los sistemas y dispositivos de red están configurados para funcionar de acuerdo con principios de seguridad (por ejemplo, concepto de controles de limitación de puertos, protocolos y servicios, software no autorizado, eliminación y desactivación de cuentas de usuario innecesarias, cambio de contraseñas por defecto de las cuentas, eliminación de software innecesario, etc.).
- Realiza auditorías periódicas de la configuración al menos una vez al año para garantizar que el entorno de producción real no tenga ninguna configuración no autorizada.
- Garantiza que la gestión de la configuración rija los estándares de configuración segura y detecte, alerte y responda de manera efectiva a los cambios en la configuración o las desviaciones.

Orientación para el cliente de servicios en la nube (proveedor) utilizados para prestar servicio(s) a Barclays

El cliente de servicios en la nube (CSC) debe asegurarse de que se implementan los controles de configuración segura adecuados para proteger el servicio de Barclays.

- Al configurar máquinas virtuales, los clientes de servicios en la nube deben asegurarse de que se han reforzado los aspectos adecuados (por ejemplo, solo los puertos, protocolos y servicios necesarios) y de que se han adoptado las medidas técnicas apropiadas (por ejemplo, antimalware, registro) para cada máquina virtual utilizada.

Control 11.0 – Requisitos de seguridad de la inteligencia artificial (IA)

El proveedor debe consultar con Barclays (Dirección General de Seguridad - equipo TPSecM, externalcyberassurance@barclayscorp.com) si está utilizando herramientas de IA para cualquier parte del ciclo de vida de los servicios o para tratar datos de Barclays.

En estos casos, el proveedor debe utilizar un sistema de gestión de IA que debe documentar, como mínimo, los procesos o procedimientos relacionados con los siguientes aspectos:

- Gobernanza de IA: el proveedor debe definir y establecer un marco de gobernanza para el uso de las herramientas de IA (incluidas las herramientas de IA de terceros). Este marco de gobernanza debe garantizar que las herramientas de IA se diseñen, implementen o integren en los procesos existentes de forma que se ofrezca protección contra la pérdida de datos, los daños en el sistema, las interrupciones del servicio y las consecuencias normativas. Un programa de gobernanza bien estructurado debe garantizar que los conceptos básicos de disponibilidad, integridad y confidencialidad estén respaldados por controles adecuados. Los controles deben diseñarse para mitigar o reducir los riesgos de pérdida, interrupción o corrupción de la información a través del sistema de IA, y el proveedor debe garantizar que los controles de seguridad se aplican y funcionan de forma eficaz para proteger los datos de Barclays y los servicios prestados a Barclays cuando estos interactúen con el sistema de IA.

- Seguridad de IA: el proveedor debe definir y establecer un marco de seguridad de IA que incluya, entre otras, las siguientes áreas:
  - Políticas relacionadas con la IA: el proveedor debe documentar una política de IA que detalle los requisitos para el uso o desarrollo seguro y responsable de los sistemas de IA.
  - Organización interna: el proveedor debe asegurarse de establecer responsabilidades dentro de la organización para mantener su enfoque responsable en lo que respecta a la implementación, el funcionamiento y la gestión de los sistemas de IA.
  - Recursos para sistemas de IA: el proveedor debe asegurarse de que la organización tenga en cuenta los recursos del sistema de IA (incluidos sus componentes y activos) para comprender y abordar plenamente los riesgos y los impactos.
  - Datos para sistemas de IA: el proveedor debe asegurarse de que la organización comprende el papel y el impacto de los datos (incluidos los datos de Barclays) en los sistemas de IA en lo que se refiere a la aplicación y el desarrollo, el suministro o el uso de sistemas de IA a lo largo de sus ciclos de vida.
  - Información sobre los sistemas de IA para las partes interesadas: el proveedor se asegurará de que cualquier parte interesada pertinente (incluido Barclays) disponga de la información necesaria para comprender y evaluar los riesgos del sistema de IA y sus impactos (tanto positivos como negativos).

- Relaciones con terceros y clientes: el proveedor debe garantizar que la organización comprende sus responsabilidades y sigue siendo responsable con respecto al sistema de IA, y que los riesgos se distribuyen adecuadamente cuando diversos terceros participan en cualquier fase del ciclo de vida del sistema de IA.

EUDA: cuando los servicios del proveedor o la capacidad o la funcionalidad de los productos del proveedor que se proporcionen a Barclays utilicen EUDA y la IA se implemente o despliegue para implantar o servir de apoyo a estas EUDA, el proveedor deberá informar a Barclays y asegurarse de que el uso de la IA no entra en conflicto con los requisitos de SCO de EUDA de Barclays.

Nota: El requisito de control de seguridad anterior no solo se aplica a la inteligencia artificial (IA), sino también al aprendizaje automático (ML), ya que la inteligencia artificial y el aprendizaje automático están muy estrechamente relacionados y conectados. El proveedor debe implementar todos los requisitos de control anteriores para el uso de herramientas de ML en cualquier parte del ciclo de vida de los servicios o del tratamiento de datos de Barclays.

Definición de IA/ML: IA significa un sistema basado en máquinas diseñado para funcionar con un nivel de autonomía y capaz de generar resultados para un conjunto determinado de objetivos, como predicciones, recomendaciones o decisiones que influyen en entornos físicos o virtuales. ML es un subconjunto de IA que hace referencia a la capacidad de una máquina para mejorar su propio rendimiento desde la experiencia hasta las iteraciones sin estar explícitamente programada con reglas.

Un método/una aplicación/una herramienta que se ajuste a la definición anterior se considera IA/ML si demuestra características de IA/ML[1] o si utiliza un algoritmo de IA/ML enumerado[2].

1. Un método/una aplicación/una herramienta tiene características de IA/ML si contiene parámetros que se entrenan con datos y la idoneidad de esos parámetros no puede evaluarse individualmente por parte de un experto en la materia. Esto puede deberse al elevado número de parámetros, a la complejidad del cálculo o a la frecuencia con la que se actualizan. A los efectos de esta definición, «parámetros» significa variables numéricas en el algoritmo que pueden variarse para afectar su producción; «idoneidad» significa que la producción del modelo es adecuada para su uso, y «experto en la materia» significa propietario o desarrollador del modelo (si actúa como delegado para el desarrollo del modelo).

2. Los algoritmos de IA/ML incluyen embolsado (bosque aleatorio, etc.), refuerzo (GBM, XGBoost, etc.), agrupación (K-medias, DBSCAN, etc.), aprendizaje profundo/red neuronal, aprendizaje basado en instancias (KNN, etc.), regresión regularizada (por ejemplo, Lasso, Ridge), aprendizaje de refuerzo o compatibilidad con máquinas vectoriales.

Derecho de inspección

El proveedor debe permitir que Barclays, previa notificación por escrito con una antelación mínima de diez (10) días hábiles, pueda llevar a cabo una revisión de seguridad de cualquier instalación o tecnología utilizada por el proveedor o sus subcontratistas/subencargados 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 para con Barclays. El proveedor también debe permitir a Barclays realizar una inspección al menos cada año o inmediatamente después de producirse un incidente de seguridad.

Todo incumplimiento de controles identificado por Barclays durante una inspección debe someterse 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 debe prestar a Barclays toda la asistencia que solicite en términos razonables en relación con cualquier inspección y documentación presentada durante una inspección. La documentación debe cumplimentarse y devolverse a Barclays con prontitud. El proveedor también debe apoyar a Barclays con el interlocutor de la evaluación junto con las pruebas solicitadas durante cualquier revisión de garantía. Cada parte asumirá sus propios costes con respecto a cualquier examen/auditoría/evaluación.

Apéndice A: Plan del etiquetado de la información y requisitos de gestión de datos de Barclays

Tabla A1: 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 empleado. • 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 (NDA).
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
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).	• Planes de nuevos productos • Contratos de clientes • Contratos legales • Información de clientes individuales o de escaso volumen que deba enviarse externamente. • Comunicaciones de clientes.

	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 • Resultados de auditorías e informes
Sin restricción	La información debe clasificarse como Sin restricción si está 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 A2: Plan del etiquetado de la información de Barclays: requisitos de gestión de datos

*** 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	Secreta	Restringida – Interna	Restringida – Externa
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 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 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.

	• 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	• 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.	• 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.
Uso compartido	• 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 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 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.		• 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.
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 soportes en los que se hayan almacenado activos electrónicos «secretos» se limpiarán adecuadamente antes o durante la 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.

Apéndice B: Definiciones

Información confidencial de Barclays alude a cualquier información que obtenga el responsable del proveedor, el proveedor o cualquier miembro de su personal (o cualquier información a la que estos puedan acceder) en relación con estas condiciones y/o cualquier contrato relacionado con los siguientes elementos, ya sean pasados, presentes o futuros: (i) actividades comerciales, productos y/o desarrollos de cualquier entidad de Barclays; (ii) empleados, clientes, contrapartes, terceros/proveedores y/o contratistas de cualquier entidad de Barclays (que no sean entidades proveedoras), incluida toda propiedad intelectual de cualquier entidad de Barclays (incluso en virtud de cualquier contrato) o cualquier proveedor/contratista de dicho tercero, datos personales protegidos, estas condiciones generales, cada módulo y contrato, y los registros mantenidos conforme a cualquier contrato y cualquier

información relacionada con los planes, los precios, las metodologías, los procesos, los datos financieros de la entidad o de las personas correspondientes, los derechos de propiedad intelectual, las investigaciones, los sistemas, los programas y/o la tecnología de la información.

Datos de Barclays alude a todos los datos, la información, el texto, los planos y demás materiales incorporados en cualquier medio, incluidos los electrónicos, ópticos, magnéticos o físicos, (i) a los que pueda acceder el proveedor en relación con cualquier contrato, (ii) que cualquier entidad de Barclays suministre al proveedor, o (iii) que el proveedor genere, recopile, trate, almacene o transmita en relación con cualquier contrato, excluyendo los materiales del proveedor.

Sistemas de Barclays alude a los sistemas informáticos que comprenden uno o más dispositivos de hardware/software, equipos, periféricos y redes de comunicaciones que cualquier entidad de Barclays controle, gestione, utilice o tenga en propiedad.

Incidente cibernético alude a cualquier evento, independientemente de si se ha confirmado que se ha producido realmente o si el proveedor o Barclays tienen motivos razonables para creer que ha tenido lugar (con base en una amenaza creíble, datos factibles u otro tipo de información), que haya puesto en peligro o pueda poner en peligro (i) la confidencialidad, integridad o plena disponibilidad de los datos de Barclays o (ii) la confidencialidad, integridad o plena disponibilidad y el normal funcionamiento de un sistema del proveedor o de Barclays.

Incidentes de seguridad: una interrupción no planificada de un servicio informático o una reducción en su calidad, lo que incluye, entre otros supuestos, el fallo de un artículo de configuración que aún no ha afectado a un servicio. **Incidente grave:** un incidente que supone un riesgo/impacto significativo para Barclays y puede tener consecuencias graves, como una pérdida significativa de productividad, daños a la reputación/infracción de la normativa e impacto en los procesos empresariales principales, controles o sistemas clave.

Evaluación de impacto de la protección de datos alude a una evaluación del impacto de las operaciones de tratamiento previstas en la protección de los datos personales, según lo exija la legislación aplicable en materia de protección de datos.

Legislación de protección de datos alude a la siguiente normativa, en la medida en que resulte aplicable al cumplimiento de cualquiera de las obligaciones del proveedor en virtud de cualquier contrato: (i) la Directiva 2002/58/CE de la UE sobre la privacidad y las comunicaciones electrónicas (según se modifique o sustituya oportunamente); (ii) el Reglamento 2016/679 o Reglamento General de Protección de Datos de la UE (**RGPD**), las decisiones y directrices de la Comisión Europea y toda la legislación aplicable a nivel nacional; (iii) el RGPD del RU; (iv) las disposiciones de la Ley Gramm–Leach–Bliley, relativas a la información personal privada; (v) la Ley de transferencia y responsabilidad de seguro médico de EE. UU. de 1996, y (vi) todas las demás leyes, normativas y directrices aplicables relacionadas con la protección de datos y la privacidad en (a) cualquier jurisdicción donde se encuentre la entidad de Barclays correspondiente, se cumplan las obligaciones de los proveedores, se localice al interesado correspondiente, se trate, almacene o use cualquier dato personal protegido, y (b) cualquier jurisdicción desde la que el proveedor cumpla cualquiera de sus obligaciones en virtud de cualquier contrato.

Obligaciones de control de la privacidad de los datos alude a cualquier programa de privacidad de los datos que forme parte del Anexo 7 (Obligaciones de control de proveedores externos).

Interesado alude al término definido en la legislación de protección de datos. Cuando dicho término no quede definido en la legislación de protección de datos, se entenderá que alude a una persona física identificada o identificable, cuya identidad puede determinarse directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de ubicación, un identificador en línea o uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona física.

Procedimientos recomendados del sector alude, en relación con cualquier empresa y circunstancia, al ejercicio del más alto grado de habilidad, diligencia, prudencia y previsión que se esperaría razonablemente de una persona altamente cualificada y con experiencia que se comprometiese en el mismo tipo de empresa en circunstancias idénticas o similares.

Datos personales alude al término definido en la legislación de protección de datos. Cuando dicho término no quede definido en la legislación de protección de datos, se entenderá que alude a cualquier información relacionada con un interesado o que permita identificarlo, ya sea directa o indirectamente.

Violación de datos personales alude al término definido en la legislación de protección de datos. Cuando dicho término no quede definido en la legislación de protección de datos, se entenderá que alude a cualquier incumplimiento de los requisitos de seguridad que provoque la destrucción, la pérdida, la alteración, la divulgación no autorizada o el acceso accidental o ilegal a datos personales que se hayan transmitido, almacenado o tratado.

Tratamiento alude al término definido en la legislación de protección de datos. Cuando dicho término no quede definido en la legislación de protección de datos, se entenderá que alude a cualquier operación o conjunto de operaciones que se realice sobre los datos personales, ya sea por medios automáticos o no, como (entre otros) la recopilación, el registro, la organización, el almacenamiento, la adaptación o alteración, la recuperación, la consulta, el uso, la divulgación por transmisión, difusión o puesta a disposición, la alineación o combinación, el bloqueo, el borrado o la destrucción. Los términos **tratar** y **tratado/a** tendrán significados acordes a esta definición.

Subcontratista alude a cualquier tercero que ocasionalmente proporcione bienes o preste servicios en relación con: (a) la provisión de productos, la prestación de servicios o la oferta de entregables, o (b) el tratamiento u otro uso de cualquier dato personal protegido según lo permita un contrato.

Personal del proveedor/de terceros/externo alude a todas y cada una de las personas o entidades que realizan cualquier parte de los servicios o proporcionan cualquier producto en virtud de cualquier contrato, lo que incluye empleados, subcontratistas o agentes del proveedor o de cualquiera de sus subcontratistas.

Sistemas del proveedor/de terceros/externos alude a cualquier sistema informático (lo que puede incluir uno o más dispositivos de hardware/software, equipos, periféricos y redes de comunicaciones) que (en todo o en parte): (i) se utilice para proporcionar cualquier producto o servicio a cualquier afiliado

de Barclays en relación con un contrato o (ii) se mantenga, gestione, supervise o quede bajo el control del proveedor o de un subcontratista en relación con un contrato.

Sistema alude a cualquier sistema informático (lo que puede incluir uno o más dispositivos de hardware/software, equipos, periféricos y redes de comunicaciones) que (en todo o en parte) se utilice para proporcionar cualquier producto o servicio a cualquier afiliado de Barclays en relación con un contrato.