

Obligaciones de control de proveedores externos

Seguridad de la información y ciberseguridad (ICS)

Título / Área de control	Descripción del control	Por qué es importante
<p>1. Marco y gobernanza en materia de seguridad de la información o ciberseguridad</p>	<p>El proveedor dispondrá de un marco de seguridad con estándares industriales consistente y establecido para la gobernanza de la ciberseguridad y la seguridad de la información que garantice el conocimiento de su personal, procesos y 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 de las amenazas de ciberseguridad con arreglo a los códigos de prácticas recomendados (por ejemplo, NIST, ISO/IEC 27001) y los requisitos industriales aplicables.</p> <p>El marco de gobernanza de la seguridad debe desarrollarse, documentarse, aprobarse y aplicarse, lo que incluye medidas administrativas, técnicas y físicas para proteger los activos y los datos de la pérdida, acceso indebido, acceso no autorizado, revelación, alteración y destrucción.</p> <p>El programa de seguridad debe incluir, entre otras cosas, las siguientes áreas:</p> <ul style="list-style-type: none"> • Una política, procedimientos y un programa de estándares que cree, aplique y mida de manera continuada y efectiva la efectividad de la aplicación de los estándares y políticas de seguridad de la información y ciberseguridad. • Un programa de seguridad completo con una estructura de liderazgo clara y supervisión ejecutiva para crear una cultura de la responsabilidad y conocimiento en materia de seguridad. • Políticas y procedimientos de seguridad de la información y ciberseguridad apropiados aprobados y comunicados en toda la organización. • Garantizar que las políticas y procedimientos/estándares de seguridad de la información y ciberseguridad se revisen de manera rutinaria (como mínimo cada año o cuando se produzcan cambios sustanciales). • El proveedor garantizará que exista una responsabilidad individual relativa a los sistemas y la información procurando que haya la responsabilidad apropiada de los entornos empresariales críticos, la información y los sistemas, y que se asigne a personas capacitadas. • El proveedor coordinará y alineará las funciones y responsabilidades del personal, aplicando, gestionando y supervisando la efectividad de la estrategia y el marco de seguridad con socios internos y externos. • Deben llevarse a cabo evaluaciones y revisiones independientes como mínimo cada año para garantizar que la organización aborde las no conformidades de las políticas, estándares, procedimientos y obligaciones de cumplimiento establecidos. <p>El proveedor garantizará que Barclays sea notificado (por escrito) en cuanto se pueda hacer legalmente si es objeto de una fusión, adquisición o cualquier otro cambio de propiedad.</p>	<p>De no aplicarse este principio, Barclays o sus proveedores podrían no disponer de (y no ser capaces de demostrar) una supervisión adecuada de la seguridad de la información o la ciberseguridad. Un marco de gobernanza de la seguridad fuerte establece el tono de seguridad para toda la organización.</p>

<p>2. Gestión de riesgos de seguridad de la información/ciberseguridad</p>	<p>El proveedor establecerá un programa de gestión de riesgos de seguridad que evalúe, mitigue y controle de manera efectiva los riesgos de seguridad en todo el entorno controlado del proveedor.</p> <p>El programa de gestión de riesgos debe incluir, entre otras cosas, las siguientes áreas:</p> <ul style="list-style-type: none"> • El proveedor debe contar con un marco de gestión de riesgos de seguridad de la información y ciberseguridad aprobado por la autoridad competente correspondiente (por ejemplo, el Consejo o uno de sus comités). Este debería incorporarse a la estrategia de negocio general y el marco de gestión de riesgos. • Deben llevarse a cabo evaluaciones de riesgos formales alineadas con el marco de riesgos como mínimo anualmente o a intervalos planificados, 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) 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). • Los resultados de las evaluaciones de riesgos incluirán actualizaciones de las políticas, procedimientos, estándares y controles de seguridad para garantizar que siguen siendo relevantes y efectivos y, si procede, que están alineados con los procedimientos recomendados del sector. • Selección de opciones apropiadas de tratamiento de los riesgos de seguridad de la información que tengan en cuenta los resultados de las evaluaciones de riesgos. • Formulación de un plan de tratamiento de los riesgos de seguridad de la información y los criterios de aceptación de riesgos a través de personas debidamente cualificadas y responsables. • El proveedor garantizará que los riesgos identificados se minimicen o eliminen en el entorno a través de la priorización del riesgo y la aplicación de contramedidas. • Los riesgos deben mitigarse a un nivel aceptable. Deben establecerse y documentarse niveles de aceptación basados en criterios de riesgos de acuerdo con marcos temporales de resolución aceptables y con la aprobación de las partes interesadas. • Las evaluaciones de riesgos asociadas a los requisitos de gobernanza de los datos deben tener en cuenta los siguientes elementos: <ul style="list-style-type: none"> ○ 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. 	<p>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.</p> <p>Si este principio no se implementa, podría revelarse de manera inapropiada información de Barclays y/o producirse la pérdida del servicio. Esto tendría como consecuencia una sanción legal o normativa, o daños en la reputación.</p>
--	---	--

	<ul style="list-style-type: none"> El proveedor llevará a cabo como mínimo anualmente una evaluación de los riesgos de seguridad en relación con la seguridad de la información y la ciberseguridad y, en función de los entornos específicos, con una frecuencia mayor. <p>El proveedor debe notificar a Barclays si no es capaz de remediar o reducir cualesquiera áreas de riesgo sustanciales que podrían afectar al servicio que presta a Barclays.</p>	
<p>3. Uso autorizado</p>	<p>El proveedor elaborará y publicará un documento con los requisitos de uso aceptable, en el que informará a su personal de sus responsabilidades.</p> <p>Deberán considerarse los siguientes temas:</p> <ul style="list-style-type: none"> el uso de internet; el uso basado en software como servicio (SaaS); el uso de depósitos de códigos públicos; el uso plugins basados en navegadores y freeware/shareware; el uso de las redes sociales; el uso del correo electrónico corporativo; el uso de la mensajería instantánea; el uso de equipos informáticos facilitados por el proveedor; el uso de equipos informáticos no facilitados por el proveedor (por ejemplo, el uso de dispositivos propios para trabajar); el uso de dispositivos de almacenamiento portátiles o extraíbles; las responsabilidades relativas al tratamiento de los activos de información de Barclays; y la salida de canales de filtración de datos. <p>El proveedor emprenderá las acciones necesarias para garantizar el cumplimiento de estos requisitos.</p>	<p>Los requisitos en cuanto a uso aceptable contribuyen a respaldar el entorno de control que protege los activos de información.</p>
<p>4. Educación y conocimiento</p>	<p>El proveedor contará con un programa de formación de conocimiento en seguridad para todos sus empleados, contratistas y usuarios terceros de los sistemas de la organización y dará instrucciones cuando proceda. Todas las personas con acceso a datos/información de Barclays deberán recibir formación de conocimiento apropiada y actualizaciones regulares en procedimientos, procesos y políticas organizativas correspondientes a su función profesional en lo que atañe a la organización. Los niveles de formación y conocimiento deben ser acordes a las funciones desarrolladas y consignarse en una plataforma de gestión del aprendizaje adecuada.</p> <p>El proveedor garantizará que todo el personal bajo su control siga la formación en seguridad de la información obligatoria, que deberá incluir procedimientos óptimos de ciberseguridad y protección de datos de Barclays en el plazo de un mes desde que pasen a formar parte de la organización y reciclarse luego como mínimo anualmente. Deben incluirse los siguientes elementos cuando proceda:</p> <p>Los grupos de alto riesgo, como las personas con acceso privilegiado a los sistemas o en funciones sensibles (incluyendo usuarios privilegiados, altos ejecutivos, personal de seguridad de la información)</p>	<p>En la educación y el conocimiento se basan todos los demás controles de este anexo.</p> <p>De no aplicarse este principio, los empleados pertinentes no conocerán los ciberriesgos ni los vectores de ataque y serán incapaces de detectar o evitar ataques.</p>

	<p>y ciberseguridad y terceras partes interesadas) deben recibir formación de conocimiento relativa a situaciones de seguridad de acuerdo con sus funciones y responsabilidades.</p>	
<p>5. Gestión de incidentes de ciberseguridad</p>	<p>El proveedor establecerá un marco de gestión de incidentes de ciberseguridad que valide, contenga y elimine/mitigue efectivamente los incidentes de seguridad del entorno del proveedor.</p> <p>El proveedor garantizará que existan planes escritos de respuesta a los incidentes que definan las funciones del personal así como fases de gestión/tratamiento de incidentes:</p> <ul style="list-style-type: none"> • Validación de incidentes - Establecer un proceso de validación de incidentes que potencie distintas fuentes de datos y esté integrado en la empresa para validar de manera efectiva los incidentes de seguridad. • Clasificación de incidentes - Establecer un proceso de clasificación de incidentes que clasifique de manera efectiva y rápida los incidentes validados para todos los tipos de eventos, permitiendo actividades de respuesta rápida a los incidentes. • Contención de incidentes - Utilizar a las personas, procesos y capacidades tecnológicas para contener de forma efectiva y rápida los incidentes de seguridad 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. <p>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.</p> <p>El proveedor se asegurará de que se efectúen pruebas, como mínimo de carácter anual, de los procesos y equipos de respuesta a incidentes para garantizar que puede responder a los incidentes de ciberseguridad identificados.</p> <ul style="list-style-type: none"> • Las pruebas incluirán una validación de la capacidad para notificar a Barclays, demostrando la capacidad de ponerse en contacto con las personas apropiadas. • Comunicación – El proveedor deberá nombrar un punto de contacto para los incidentes de seguridad que será el enlace con Barclays en caso de producirse algún incidente. 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. <p>Dichos datos deben incluir: -Nombre, responsabilidades dentro de la organización, función, correo electrónico y/o teléfono</p> <p>El proveedor informará a Barclays, dentro de unos plazos razonables, tras tener conocimiento de cualquier incidente que pueda afectar al servicio prestado a Barclays o la información/datos de Barclays no más tarde de dos (2) horas después del momento en el que tenga conocimiento del incidente.</p>	<p>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.</p>

	<p>Si se sospecha o conoce que se ha producido una infracción de la seguridad de los datos, el vendedor deberá notificar a Barclays dichos incidentes de acuerdo con los requisitos de protección de datos de los países afectados.</p> <p>El proveedor entregará a Barclays un informe con respecto a cualquier incidente que afecte al servicio o la información/datos de Barclays. Dicho informe deberá incluir la siguiente información:</p> <ul style="list-style-type: none"> • Fecha y hora • Ubicación • Tipo de incidente • Impacto • Estado • Mitigación o acción emprendida <p>Esos incidentes deben comunicarse al responsable de proveedores de Barclays y al centro de operaciones conjuntas de Barclays dentro del Centro de Operaciones Conjuntas (JOC) de la Dirección General de Seguridad de Barclays (CSO) - gcsojoc@barclays.com.</p>	
<p>6. Clasificación y protección de la información</p>	<p>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:</p> <ul style="list-style-type: none"> • Asignar el Plan de etiquetado de la información correcto. • Gestionar la información de forma segura en línea con su nivel de clasificación asignado. • 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. <p>El proveedor deberá remitirse al Plan del etiquetado de la información y los requisitos de tratamiento (Apéndice B, Tabla B1 y B2) de Barclays, o un plan alternativo para garantizar que protege la información de Barclays que mantiene o trata. Este requisito se aplica a todos los activos de información que se mantengan o traten en nombre de Barclays.</p>	<p>Es necesario aplicar eficazmente los controles adecuados para asegurarse de que la información confidencial de Barclays solo es accesible para las personas autorizadas (confidencialidad), está protegida contra cambios no autorizados (integridad) y puede recuperarse y presentarse cuando se requiera (disponibilidad).</p> <p>Si estos requisitos no se aplican se podría poner en peligro información confidencial de Barclays, dejándola expuesta a modificaciones no autorizadas, filtraciones, accesos no autorizados, daños, pérdidas o destrucción, lo que podría conllevar sanciones en el marco jurídico o normativo, daños en la reputación, pérdidas o interrupción del negocio.</p>
<p>7. Gestión de activos (hardware y software)</p>	<p>El proveedor garantizará que se establezca un programa de gestión de activos efectivo durante todo el ciclo de vida de los activos. La gestión de activos debe gobernar el ciclo de vida de los activos desde su adquisición hasta su retirada, aportando visibilidad y seguridad a todas las clases de activos en el entorno.</p>	<p>Resulta esencial disponer de un inventario completo y exacto de activos de información para garantizar la</p>

	<p>El proveedor mantendrá un inventario exacto y preciso 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 del vendedor o suministrados por Barclays, y garantizar que se efectúe como mínimo una prueba anual para validar que el inventario está actualizado, está completo y es correcto.</p> <p>Todo el proceso de gestión de activos debe incluir las siguientes áreas:</p> <ul style="list-style-type: none"> • Activos e infraestructuras de información protegidos en función de su clasificación, criticidad y valor empresarial. • Mantener un inventario actualizado y preciso de todos los activos tecnológicos con potencial para almacenar o tratar información. Dicho inventario deberá incluir todos los activos, tanto conectados a la red de la organización como no. (Específico del servicio de Barclays). • 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). • Garantizar que los activos no autorizados se retiren de la red, se pongan en cuarentena o que el inventario se actualice de manera regular. • Mantener una lista actualizada de todo el software autorizado que sea necesario para prestar servicio a Barclays. • Garantizar que solo se añadan al inventario de software autorizado de la organización aplicaciones de software y sistemas operativos compatibles en la actualidad y que sean objeto de actualizaciones. El software no compatible debe etiquetarse como no compatible en el sistema de inventario. <p>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.</p>	<p>implantación de los controles pertinentes.</p> <p>Si no se aplica este principio, los activos de Barclays o los activos utilizados por proveedores para prestar servicio a Barclays podrían estar en peligro, lo que podría generar pérdidas económicas, pérdida de datos, daños a la reputación y sanciones reglamentarias.</p>
<p>8. Destrucción/eliminación /Desmantelamiento de información lógica y física</p>	<p>Cuando se destruyan o eliminen activos de información de Barclays que se guarden en formato físico o electrónico, dicha destrucción o eliminación se efectuará utilizando medidas de seguridad adecuadas al riesgo asociado y garantizando que no puedan recuperarse.</p> <p>El proveedor debe establecer políticas y procedimientos con procesos empresariales que los respalden además de implementar medidas técnicas para la retirada segura y la eliminación completa de información de Barclays de cualquier medio de almacenamiento, garantizando que los datos no puedan recuperarse por ningún medio forense informático.</p>	<p>La destrucción segura de los activos de información ayuda a garantizar que los activos de información de Barclays no puedan recuperarse mediante una vulneración de la seguridad de los datos o de actividades malintencionadas.</p>
<p>9. Seguridad de la red y límites</p>	<p>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 protejan contra el desplazamiento lateral de amenazas dentro de la red del proveedor (y de cualquier subcontratista pertinente). El proveedor</p>	<p>Si este servicio no se implementa, los atacantes podrían debilitar la seguridad de las redes externas o internas para</p>

	<p>detectará/evitará/corregirá el flujo de información que se transfiere entre redes con distintos niveles de confianza centrándose especialmente en los datos que perjudiquen la seguridad.</p> <p>Los mecanismos de integridad de la red deben incluir las siguientes áreas:</p> <ul style="list-style-type: none"> • Mantener un inventario actualizado de todos los límites de la red de la organización (a través de una arquitectura/diagrama de red). • El diseño e implementación de la red deben revisarse como mínimo anualmente o si surge un requisito motivado por un acontecimiento que provoque cambios. • Las conexiones externas a la red del proveedor deben documentarse, enrutarse a través de un firewall y ser comprobadas y aprobadas antes de establecerse, a fin de evitar infracciones de seguridad. • Las redes de los proveedores se protegen aplicando principios de defensa en profundidad (como segmentación de red, firewalls, controles de los accesos físicos a los equipos de red, etc.). • El proveedor deberá contar con tecnologías que eviten las intrusiones en la red para detectar y evitar la entrada de tráfico malicioso en la red. • El uso de capacidades de firewall de red fuertes que ofrezcan una capa de defensa perimetral frente a los ataques maliciosos contra las redes. • Todo el tráfico de red con origen o destino en internet debe pasar a través de un proxy de capa de aplicaciones autenticado configurado para filtrar las conexiones no autorizadas. • Los dispositivos de red deben endurecerse de forma segura para evitar los ataques maliciosos. • Separación lógica de los puertos/las interfaces de gestión de dispositivos del tráfico de usuarios; controles de autenticación apropiados. • Todas las normas de configuración que permitan que el tráfico fluya a través de dispositivos de red deben documentarse en un sistema de gestión de la configuración con una justificación empresarial específica para cada una. • Denegar la comunicación o el tráfico de aplicaciones sobre puertos TCP o UDP no autorizados para garantizar que solo se permita cruzar el límite de la red a protocolos autorizados en cada uno de los límites de la red de la organización. • Realizar lecturas regulares desde fuera de cada límite de red de confianza para detectar las conexiones no autorizadas accesibles a través del límite. • Comunicaciones seguras entre dispositivos y estaciones/consolas de gestión. • Configurar sistemas de seguimiento para registrar los paquetes de red que pasen a través del límite en cada uno de los límites de la red de la organización. • La conexión de red entre centros de datos/proveedores de servicios de red/interoficina debe encriptarse sobre un protocolo seguro. Los datos de Barclays en tránsito dentro de la red de área amplia (WAN) del proveedor deben estar encriptados. • El proveedor debe revisar las reglas del firewall (externo e interno) cada año. • Todo acceso inalámbrico a la red se somete a protocolos de autorización, autenticación, segmentación y cifrado para evitar infracciones de seguridad 	<p>obtener acceso al servicio o a los datos que contiene.</p>
--	---	---

	<ul style="list-style-type: none"> • El proveedor se asegurará de que se lleve un control del acceso a la red interna y de que solo se permitan dispositivos autorizados, por medio de controles de acceso a la red pertinentes. • El acceso de inicio de sesión remoto a la red del proveedor debe utilizar autenticación multifactor. <p>El proveedor debe garantizar que ningún servidor empleado para prestar servicio a Barclays se despliegue en redes que no sean de confianza (redes fuera de su perímetro de seguridad, que escapen a su control administrativo, por ejemplo, con acceso a internet) sin controles de seguridad apropiados.</p> <p>El proveedor que aloje información de Barclays (incluyendo subcontratistas) en los centros de datos o la nube deben contar con un certificado ISO/IEC 27001 y/o SOC 1 o 2 válido para la gestión de la seguridad (o certificados que demuestren controles equivalentes respaldados por el informe de un auditor independiente).</p> <p>Redes T2 y T3 -</p> <ul style="list-style-type: none"> • La red T2 debe estar separada lógicamente de la red corporativa del proveedor por un firewall, y todo el tráfico de entrada y salida debe estar restringido y controlado. • La configuración de enrutamiento debe garantizar que solo se establezcan conexiones con la red de Barclays y evitar el enrutamiento a otras redes del proveedor • El router periférico del proveedor que se conecte con las pasarelas de la extranet de Barclays debe configurarse de forma segura con un concepto de controles de limitación de puertos, protocolos y servicios; <ul style="list-style-type: none"> ○ Garantizar que el registro y la monitorización estén habilitados. <p><i>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.</i></p>	
<p>10. Detección de denegación de servicio</p>	<p>El proveedor mantendrá una capacidad de detección y protección frente a los ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS).</p> <p>El proveedor se asegurará de que los canales externos o conectados a internet que se empleen para prestar servicios a Barclays cuenten con una adecuada protección contra ataques de denegación de servicio, a fin de garantizar la disponibilidad.</p>	<p>De no aplicarse este principio, Barclays y sus proveedores podrían no ser capaces de evitar que un ataque por denegación de servicio alcance su objetivo.</p>
<p>11. Acceso remoto</p>	<p>El acceso remoto a la red de Barclays a través de una aplicación Citrix de Barclays y/o datos de Barclays residentes/almacenados en un entorno gestionado del proveedor no se suministra por defecto y no se conecta desde ubicaciones no aprobadas/fuera de la oficina/desde casa, y cualquier acceso remoto debe ser aprobado y autorizado por Barclays (Dirección General de Seguridad - equipo ECAM).</p>	<p>Los controles de acceso remoto ayudan a garantizar que los dispositivos no autorizados y no seguros no se conecten a distancia al entorno de Barclays.</p>

	<p>El proveedor se asegurará de que los siguientes componentes estén establecidos para el acceso remoto:</p> <ul style="list-style-type: none"> • El acceso de inicio de sesión remoto a la red del proveedor debe encriptarse durante los datos en tránsito y utilizar autenticación multifactor. • El acceso a la red de Barclays debe realizarse a través de una aplicación Citrix de Barclays con un token RSA (hard y soft) suministrado por Barclays • El proveedor mantendrá un inventario de todos los tokens RSA (hard y soft) suministrados por Barclays y un proceso de gestión que incluya la revisión y el seguimiento de la asignación, el uso y la devolución de los tokens (hard). • El proveedor mantendrá registros de las personas que han pedido trabajar a distancia y la justificación de dicha solicitud • El proveedor reconciliará todos los usuarios remotos de forma trimestral y lo certificará a Barclays (Dirección General de Seguridad - equipo ECAM). • Barclays desactivará las credenciales de autenticación una vez que se notifique que el acceso ya no es necesario (por ejemplo, despido de empleados, reasignación de proyectos, etc.) en el plazo de veinticuatro (24) horas. • Barclays desactivará inmediatamente las credenciales de autenticación si no se han utilizado durante cierto tiempo (dicho período no deberá superar un mes). • El proveedor garantizará que el extremo empleado para conectar a distancia sistemas de información de Barclays debe configurarse de manera segura (por ejemplo, nivel de los parches, estado de las soluciones contra el software malintencionado, etc.). • Los servicios con acceso de impresión a distancia a través de una aplicación Citrix de Barclays deben ser aprobados y certificados por Barclays (Dirección General de Seguridad - Equipo ECAM). El proveedor mantendrá registros y realizará reconciliaciones trimestrales. • No se debe permitir que dispositivos personales/BYOD accedan al entorno de Barclays y/o a datos de Barclays que residan/estén almacenados en el entorno gestionado del proveedor (incluido el personal del proveedor, consultores, trabajadores temporales, contratistas y socios de servicios gestionados). <p>NOTA: El acceso remoto a la red y los datos de Barclays no está permitido a menos que Barclays lo haya aprobado y autorizado específicamente.</p>									
<p>12. Gestión de registros de seguridad</p>	<p>El proveedor garantizará que exista una auditoría y un marco de gestión de registros que confirme que los sistemas informáticos clave, incluyendo aplicaciones, equipos de red, dispositivos de seguridad y servidores, estén configurados para registrar eventos clave y el proveedor debe centralizar, asegurar apropiadamente y conservar los registros durante un período mínimo de 12 meses.</p> <table border="1" data-bbox="478 1336 1465 1421"> <thead> <tr> <th data-bbox="478 1336 680 1421">Categoría</th> <th data-bbox="680 1336 917 1421">Sistemas/servicio de bajo impacto</th> <th data-bbox="917 1336 1173 1421">Sistemas/servicio de impacto medio</th> <th data-bbox="1173 1336 1465 1421">Sistemas/servicio de alto impacto</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Categoría	Sistemas/servicio de bajo impacto	Sistemas/servicio de impacto medio	Sistemas/servicio de alto impacto					<p>Si este control no se implementa, los proveedores no podrán detectar y contrarrestar en un plazo de tiempo razonable un uso inapropiado o malintencionado de su servicio o de sus datos.</p>
Categoría	Sistemas/servicio de bajo impacto	Sistemas/servicio de impacto medio	Sistemas/servicio de alto impacto							

Conservación de registros	3 meses	6 meses	12 meses
<p>El proceso de gestión de registros debe incluir las siguientes áreas:</p> <ul style="list-style-type: none"> • El proveedor debe establecer políticas y procedimientos para la gestión de registros. • El proveedor debe crear y mantener una infraestructura de gestión de registros. • El proveedor debe definir las funciones y responsabilidades de las personas y equipos que se espera que participen en la gestión de registros. • Recopilar, gestionar y analizar los registros de auditoría de eventos que puedan ayudar a detectar, comprender y recuperarse de los ataques. • Activar registros de sistemas que incluyan información pormenorizada como el origen de los eventos, la fecha, el usuario, la marca horaria, las direcciones de origen, y otros elementos útiles. • Registros de eventos de muestra: <ul style="list-style-type: none"> ○ IDS/IPS, router, firewall, proxy web, software de acceso remoto (VPN), servidores de autenticación, aplicaciones, registros de bases de datos. ○ Accesos exitosos, intentos de registro fallidos (por ejemplo, ID de usuario o contraseña incorrectos), creación, modificación y eliminación a/de cuentas de usuario ○ Registros de cambio de configuración. • Los servicios de Barclays vinculados a aplicaciones empresariales y sistemas de infraestructuras técnicas deben estar activados, incluidos aquellos que se hayan externalizado o estén 'en la nube'. • Análisis de registros de eventos vinculados a la seguridad (incluida la normalización, agregación y correlación). • Sincronización de marcas horarias en registros de eventos con un origen común y de confianza • Protección de registros de eventos vinculados a la seguridad (por ejemplo, mediante encriptado, control del acceso y copias de seguridad). • Realización de acciones necesarias para remediar los problemas identificados y responder a los incidentes de ciberseguridad de manera rápida y efectiva. • Despliegue de herramientas analíticas de registro o gestión de eventos e información de seguridad (SIEM) para la correlación y análisis de los registros. • Despliegue de herramientas como correspondera para realizar la agregación y correlación central en tiempo real de actividades anómalas, alertas de red y sistema e inteligencia de ciberamenazas, y eventos vinculados desde múltiples fuentes, tanto internas como externas, para detectar y prevenir mejor ciberataques multiformes. <p>Los incidentes clave registrados incluirán aquellos que puedan afectar a la confidencialidad, la integridad y la disponibilidad de los servicios prestados a Barclays y que pueden ayudar a identificar o</p>			

	<p>investigar incidentes importantes y/o vulneraciones de los derechos de acceso que se hayan producido en relación con los sistemas del proveedor.</p>	
<p>13. Defensas contra malware</p>	<p>El proveedor debe contar con políticas y procedimientos establecidos y procesos empresariales y medidas técnicas implementados para evitar la ejecución de malware en dispositivos extremos de usuario gestionados o propiedad de la organización (como estaciones de trabajo, ordenadores portátiles y dispositivos móviles emitidos) y componentes de sistemas y redes de infraestructuras informáticas.</p> <p>El proveedor deberá garantizar que la protección contra malware se aplique a todos los activos informáticos aplicables en todo momento para evitar las perturbaciones de servicio o las violaciones de la seguridad.</p> <p>La protección contra malware debe incluir los siguientes elementos:</p> <ul style="list-style-type: none"> • Soluciones contra el software malintencionado gestionado centralmente para controlar y defender continuamente cada estación de trabajo y servidor de la organización. • Garantizar que las soluciones contra el software malintencionado de la organización actualizan su motor de lectura y base de datos de firmas de manera regular. • Enviar todos los eventos de detección de malware a herramientas de administración contra malware y servidores de registros de eventos de la empresa para su análisis y alerta. • El proveedor aplicará controles apropiados para proteger frente al malware y los ataques los dispositivos móviles que se conecten a las redes de Barclays o del proveedor y que accedan a los datos de Barclays. <p>NOTA: Las soluciones contra el software malintencionado deben incluir (entre otros), código móvil no autorizado, virus, programas espía, software key logger, botnets, gusanos, troyanos, etc.</p>	<p>Las soluciones contra el software malintencionado resultan esenciales para proteger los activos de información de Barclays contra el código malintencionado.</p>
<p>14. Estándares de configuración segura</p>	<p>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 estándares del sector (como NIST, SANS, CIS).</p> <p>El proceso de estándares de configuración debe incluir las siguientes áreas:</p> <ul style="list-style-type: none"> • Establece políticas, procedimientos y herramientas para los estándares de configuración de seguridad de todos los dispositivos de red y sistemas operativos autorizados. • Realiza comprobaciones de cumplimiento regulares (anuales) para garantizar que los incumplimientos de los estándares de seguridad básicos se rectifiquen inmediatamente. Existen 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 y software no autorizado). 	<p>Los controles sobre revisiones de versiones estándar ayudan a proteger los activos de información contra accesos no autorizados.</p> <p>El cumplimiento respecto de los controles y las normas sobre revisiones de versiones que garanticen que los cambios se autoricen contribuye a asegurar la protección de los activos de información de Barclays.</p>

	<p>Garantizar 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.</p>	
<p>15. Seguridad en los extremos</p>	<p>El proveedor reforzará los dispositivos utilizados para acceder a la red de Barclays o procesar/acceder a datos de Barclays, a fin de protegerlos contra los ataques.</p> <p>Las revisiones de las versiones de seguridad en los extremos deben contar con: -</p> <ul style="list-style-type: none"> • Encriptado de disco. • Deshabilitar todo el software/servicios/puertos innecesarios. • Deshabilitar el acceso con derechos de administración para el usuario local. • El personal del proveedor no podrá realizar cambios en la configuración básica, como el pack de servicios, la partición de sistemas y los servicios por defecto, etc. • El puerto USB debe estar deshabilitado para prohibir las copias de datos de Barclays a soportes externos • Actualización con las últimas firmas antivirus y parches de seguridad. • Prevención de la pérdida de datos limitada a no cortar-copiar-pegar e imprimir pantalla de los datos de Barclays • Por defecto, el acceso a las impresoras debe estar deshabilitado. • El proveedor debe limitar la capacidad para acceder a sitios de redes sociales, servicios de webmail y sitios que puedan almacenar información en internet como Google Drive, Dropbox, iCloud. • La compartición/transmisión de datos de Barclays debe estar deshabilitada utilizando herramientas/software de mensajería instantánea. • Capacidad y procesos para detectar el software no autorizado identificado como malicioso y evitar la instalación de software no autorizado. <p>NOTA: Los soportes extraíbles/dispositivos portátiles deben estar deshabilitados por defecto o habilitarse solamente por razones empresariales legítimas.</p> <p>El proveedor debe mantener imágenes o plantillas seguras para todos los sistemas de la empresa basados en los estándares de configuración aprobados por la organización. Cualquier despliegue de un nuevo sistema o de sistemas existentes que se hayan visto comprometidos debe representarse empleando una de esas imágenes o plantillas.</p> <p>Dispositivos móviles empleados para los servicios de Barclays -</p> <ol style="list-style-type: none"> 1. El proveedor garantizará que implementa capacidades de gestión de dispositivos móviles (MDM) para controlar y gestionar de forma segura los dispositivos móviles que tengan acceso y/o contengan información de Barclays clasificada, reduciendo el riesgo de comprometer los datos. 2. El proveedor garantizará la implementación de capacidades de bloqueo y borrado a distancia para los dispositivos móviles que protejan la información en caso de que un dispositivo se robe, pierda o vea comprometido. 	<p>De no aplicarse este control, la red de Barclays y la red del proveedor, así como sus extremos podrían ser vulnerables a los ciberataques.</p>

	<ol style="list-style-type: none"> 3. Encriptado de datos en dispositivos móviles (datos de Barclays). 4. Ningún servicio en la nube debe estar permitido por defecto en los dispositivos móviles suministrados por el proveedor. 	
<p>16. Prevención de las filtraciones de datos</p>	<p>El proveedor contará con un marco establecido para garantizar que exista protección frente a las fugas de datos inapropiadas que garantice la protección, incluidos los siguientes canales de fugas de información (entre otros):</p> <ul style="list-style-type: none"> • transferencia no autorizada de información fuera de la red interna o la red del proveedor; <ul style="list-style-type: none"> ○ Correo electrónico ○ pasarela web/de internet (incluyendo almacenamiento online y webmail) • pérdida o robo de activos de información de Barclays en medios electrónicos portátiles (como puede ser la información electrónica de ordenadores portátiles, dispositivos móviles y soportes portátiles); • transferencia no autorizada de información a soportes portátiles; • intercambio no seguro de información con terceros (subcontratistas); • impresión o copia inadecuadas de información; 	<p>Es necesario aplicar eficazmente los controles adecuados para asegurarse de que la información confidencial de Barclays: solo es accesible para las personas autorizadas (confidencialidad), está protegida contra cambios no autorizados (integridad) y puede recuperarse y presentarse cuando se requiera (disponibilidad).</p> <p>Si estos requisitos no se aplican se podría poner en peligro información confidencial de Barclays, dejándola expuesta a modificaciones no autorizadas, filtraciones, acceso no autorizado, daños, pérdidas o destrucción, que podrían conllevar sanciones en el marco jurídico o normativo, daños en la reputación, pérdidas o interrupción del negocio.</p>
<p>17. Protección de Datos</p>	<p>El proveedor garantizará que los datos de Barclays bajo su custodia/su red estén debidamente protegidos a través de una combinación de técnicas de encriptado, protección de la integridad y prevención de la pérdida de datos. Es importante extremar el cuidado para limitar el acceso a los datos de Barclays.</p> <p>Los controles de protección de datos deben incluir las siguientes áreas:</p> <ol style="list-style-type: none"> 1. Deben establecerse políticas y procedimientos, así como procesos empresariales que los respalden y medidas técnicas aplicadas, con el fin de inventariar, documentar y mantener los flujos de datos que residan (temporal o permanentemente) en las aplicaciones distribuidas geográficamente (física y virtualmente) dentro del servicio y la red de infraestructuras y los componentes de los sistemas y/o que se compartan con otros terceros. 2. Mantener un inventario de toda la información sensible (datos de Barclays) almacenada, tratada o transmitida por el proveedor. 3. Establecer un estándar de clasificación de los datos para garantizar que la información sensible (datos de Barclays) se clasifique y proteja apropiadamente. 4. Garantizar que todos los datos dentro de la organización se etiqueten de acuerdo con el estándar de clasificación de datos. 5. Política de uso de datos - acceso a los datos 6. Protección de los datos en reposo; <ol style="list-style-type: none"> a. Encriptar los datos en reposo para evitar que se explote información sensible a través de accesos no autorizados. 7. Supervisión de la actividad de las bases de datos; 	

	<ul style="list-style-type: none"> a. Supervisar el acceso y la actividad de las bases de datos para identificar de manera rápida y efectiva la actividad maliciosa. <p>8. Protección de los datos en uso;</p> <ul style="list-style-type: none"> a. Garantizar que la visualización y uso de la información sensible se controle a través de capacidades de gestión de acceso para proteger de la explotación de la información sensible. b. Uso de tecnologías de enmascaramiento y ofuscación de datos para proteger de manera efectiva los datos sensible en uso de las revelaciones accidentales y/o la explotación maliciosa. <p>9. Protección de los datos en tránsito;</p> <ul style="list-style-type: none"> a. Aprovechamiento de capacidades de encriptado fuerte para garantizar la protección de los datos en tránsito. b. El encriptado de los datos en tránsito suele lograrse a través del encriptado de transporte o carga (mensaje o campo selectivo). Los mecanismos de encriptado de transporte incluyen, entre otros: <ul style="list-style-type: none"> • Seguridad de la capa de transporte (TLS) • Tunnelización segura (IPsec) • Secure Shell (SSH) c. Deben configurarse protocolos de seguridad de transporte para evitar la negociación de algoritmos más débiles y/o longitudes de clave más cortas cuando ambos extremos admitan la opción más fuerte. <p>10. Copia de seguridad de los datos –</p> <ul style="list-style-type: none"> a. Se aplicarán las disposiciones necesarias para garantizar que se haga una copia de seguridad de la información y que esta pueda recuperarse de forma adecuada, cumpliendo los requisitos acordados con Barclays. b. Garantizar que las copias de seguridad estén adecuadamente protegidas por medios de seguridad física o encriptado cuando estén almacenadas, así como cuando se muevan por la red. Esto incluye las copias de seguridad remotas y los servicios en la nube. c. Garantizar que se realicen copias de seguridad con regularidad de todos los datos de Barclays. 	
<p>18. Seguridad de software de aplicaciones</p>	<p>El proveedor desarrollará aplicaciones utilizando procedimientos de programación seguros y en entornos seguros. Si el proveedor desarrolla aplicaciones para que Barclays las utilice, o que se utilicen para respaldar el servicio prestado a Barclays, deberá establecer un marco de desarrollo seguro para prevenir las infracciones de seguridad e identificar y corregir las vulnerabilidades en el código durante el proceso de desarrollo.</p> <p>La seguridad del seguridad de software de aplicaciones debe incluir las siguientes áreas:</p>	<p>Los controles que protegen el desarrollo de aplicaciones contribuyen a garantizar que se mantiene la seguridad de estas durante su despliegue.</p>

	<ul style="list-style-type: none">• Deben establecerse y adoptarse estándares de codificación seguros en línea con los procedimientos recomendados del sector para evitar vulnerabilidades e interrupciones del servicio y que al mismo tiempo defiendan frente a posibles vulnerabilidades ya conocidas.• Establecer prácticas de codificación seguras apropiadas al lenguaje de programación.• Todo el desarrollo debe llevarse a cabo en un entorno no productivo.• Mantener entornos separados para los sistemas productivos y no productivos. Los desarrolladores no deben acceder sin control a los entornos productivos.• Separación de tareas para los sistemas productivos y no productivos.• Sistemas desarrollados en línea con los procedimientos recomendados del desarrollo seguro (como OWASP).• El código debe almacenarse de manera segura y someterse a controles de calidad.• El código debe protegerse adecuadamente de las modificaciones no autorizadas una vez que las pruebas se hayan validado y se haya entregado a producción.• Utilizar solo componentes de terceros actualizados y de confianza para el software desarrollado por el proveedor.• Aplicar herramientas analíticas estáticas y dinámicas para comprobar que se cumplen las prácticas de codificación seguras.• El proveedor debe asegurarse de que los datos activos (incluyendo datos personales) no se utilizarán en entornos que no sean de producción.• Las aplicaciones e interfaces de programación (API) se diseñarán, desarrollarán, desplegarán y probarán de acuerdo con los estándares del sector (como OWASP para las aplicaciones web). <p>El proveedor debe proteger las aplicaciones web desarrollando firewalls de aplicaciones web (WAF) que inspeccionen todo el tráfico a dichas aplicaciones para evitar ataques habituales. En el caso de las aplicaciones no web, se deberán desplegar firewalls específicos de las aplicaciones si dichas herramientas están disponibles para el tipo de aplicación en cuestión. Si el tráfico está encriptado, el dispositivo debe quedar detrás del encriptado o poder desencriptar el tráfico antes del análisis. Si ninguna de estas opciones resulta apropiada, se deberá desplegar un firewall de aplicaciones web basado en el host.</p>	
--	--	--

<p>19. Gestión de accesos lógicos (LAM)</p>	<p>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.</p> <ul style="list-style-type: none"> • 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. <p>Se definirán procesos de gestión del acceso de acuerdo con los procedimientos recomendados del sector que incluirán lo siguiente:</p> <ul style="list-style-type: none"> • El proveedor debe asegurarse de que los procesos de gestión de acceso están documentados y son aplicables a todos los sistemas informáticos (que almacenan o procesan activos de información de Barclays) y que, una vez implementados, deben ofrecer controles apropiados para: Empleados nuevos/que cambian de puesto/dejan la empresa/con acceso remoto. • Deben existir controles para la autorización, para asegurarse de que el proceso de concesión, modificación y retirada del acceso incluye un nivel de autorización que se ajuste al nivel de privilegios otorgados. • Deben existir controles que garanticen que los procesos de gestión de acceso incluyen los mecanismos apropiados para la verificación de identidades. • Cada cuenta debería estar asociada a una sola persona, que responderá de toda actividad que se lleve a cabo usando la cuenta. • Recertificación del acceso - Deben existir controles para garantizar que los permisos de acceso se revisen al menos cada 12 meses, para garantizar que se ajustan a su propósito. • Todos los permisos de acceso privilegiado deben revisarse al menos cada (6) meses y deben implantarse los controles adecuados para los requisitos del acceso privilegiado. • Controles del personal que cambia de puesto - Modificación del acceso en el plazo 24 horas desde la fecha de traslado; 	<p>Los controles de LAM pertinentes ayudan a garantizar la protección de los activos de información contra un uso inadecuado.</p> <p>Es necesario aplicar eficazmente los controles adecuados para asegurarse de que la información de Barclays: solo es accesible para las personas autorizadas (confidencialidad), está protegida contra cambios no autorizados (integridad) y puede recuperarse y presentarse cuando se requiera (disponibilidad). Si estos requisitos no se aplican se podría poner en peligro información confidencial de Barclays, dejándola expuesta a modificaciones no autorizadas, filtraciones, accesos no autorizados, daños, pérdidas o destrucción, lo que podría conllevar sanciones en el marco jurídico o normativo, daños en la reputación, pérdidas o interrupción del negocio.</p>
---	--	--

	<ul style="list-style-type: none"> • 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; • Acceso remoto - Los controles de acceso remoto solo se permitirán a través de mecanismos acordados por Barclays (Dirección General de Seguridad - equipo ECAM) y el acceso remoto debe usar autenticación multifactor. • Autenticación - Deben seguirse controles de la longitud y complejidad apropiada de las contraseñas, frecuencia del cambio de estas, autenticación multifactor, gestión segura de las credenciales de las contraseñas, entre otros, de acuerdo con los procedimientos recomendados del sector • Cuentas inactivas - Las cuentas inactivas que no se usen durante 60 días consecutivos o más deben suspenderse/desactivarse. • 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. 	
<p>20. Gestión de las vulnerabilidades</p>	<p>El proveedor debe contar con políticas y procedimientos establecidos y procesos y medidas técnicas implementados para la detección puntual de las vulnerabilidades dentro de aplicaciones gestionadas o propiedad de la organización, redes de infraestructuras y componentes de sistema para garantizar la eficiencia de los controles de seguridad implementados.</p> <p>La gestión de vulnerabilidades debe incluir las siguientes áreas:</p> <ul style="list-style-type: none"> • Deben establecerse políticas y procedimientos, así como procesos y medidas técnicas implementados para la detección puntual de las vulnerabilidades dentro de aplicaciones gestionadas o propiedad de la organización, redes de infraestructuras y componentes de sistema para garantizar la eficiencia de los controles de seguridad implementados. • Funciones y responsabilidades definidos. • Herramientas e infraestructura apropiadas para el análisis de vulnerabilidades. • Desarrollar análisis de vulnerabilidades de manera rutinaria que identifiquen de manera efectiva vulnerabilidades conocidas y desconocidas en todas las clases de activos del entorno. • Utilizar un proceso de evaluación del riesgo para priorizar la remediación de las vulnerabilidades descubiertas. • Establecer un proceso de remediación de vulnerabilidades que verifique de manera rápida y efectiva la remediación de estas en todas las clases de activos del entorno. • Garantizar que las vulnerabilidades se resuelven de manera efectiva a través de actividades de remediación y gestión de parches robustas para reducir el riesgo de explotación de vulnerabilidad. 	<p>De no aplicarse este control, los atacantes podrían aprovechar las vulnerabilidades de los sistemas para atacar a Barclays y a sus proveedores.</p>

	<ul style="list-style-type: none"> • Comparar regularmente los resultados de análisis consecutivos de vulnerabilidades para comprobar que estas se han remediado de forma puntual. <p>Todos los problemas y vulnerabilidades de seguridad que pudieran afectar de forma importante a la infraestructura de alojamiento/aplicaciones web de Barclays suministradas por el proveedor y cuyo riesgo el proveedor haya decidido aceptar se comunicarán de inmediato a Barclays y se acordarán por escrito con Barclays (Dirección General de Seguridad - equipo ECAM).</p>	
<p>21. Gestión de revisiones</p>	<p>El proveedor debe contar con políticas y procedimientos establecidos y procesos empresariales y medidas técnicas implementados para desplegar parches de seguridad en los dispositivos de extremos de usuario gestionados (por ejemplo, estaciones de trabajo, ordenadores portátiles y dispositivos móviles emitidos) y componentes de sistemas y redes de infraestructuras de informáticas.</p> <p>El proveedor garantizará que se apliquen a los sistemas/activos/redes/aplicaciones los últimos parches de seguridad de forma que se garantice que:</p> <ul style="list-style-type: none"> • El proveedor probará que todos los parches en los sistemas representan de manera precisa la configuración de los sistemas de producción objetivo antes de desplegar el parche en los sistemas de producción y que el correcto funcionamiento del servicio con el parche se comprueba después de la actividad de parcheado. Si un sistema no puede parchearse, desplegar contra medidas apropiadas. • Todos los cambios informáticos importantes deben ser registrados, probados y autorizados antes de la implementación mediante un proceso sólido y aprobado de gestión de cambios, a fin de evitar interrupciones del servicio o infracciones de seguridad. • El proveedor se asegurará de que los parches se reflejen en entornos de producción y DR. 	<p>Si este control no se implementa, los servicios también pueden ser vulnerables a problemas de seguridad que podrían poner en riesgo los datos de los consumidores, provocar pérdidas de servicio o permitir otras actividades malintencionadas.</p>
<p>22. Simulación de amenazas/ Pruebas de penetración/ Evaluación de la seguridad informática</p>	<p>El proveedor contratará a un proveedor de seguridad cualificado e independiente para realizar una simulación de amenazas o una evaluación de la seguridad informática de la infraestructura informática que incluya el centro de recuperación tras desastres y las aplicaciones web en relación con los servicios que preste a Barclays.</p> <p>Se realizará una vez al año como mínimo para identificar vulnerabilidades que se podrían aprovechar para violar la confidencialidad de los datos de Barclays mediante ciberataques. Hay que asignar prioridades a las vulnerabilidades, y se debe hacer un seguimiento de su resolución. La prueba debe ser realizada de conformidad con los procedimientos recomendados del sector.</p> <p>En el caso de los servicios de proveedor relacionados con la infraestructura de alojamiento/aplicaciones en nombre de Barclays,</p> <ul style="list-style-type: none"> • El proveedor informará a Barclays del alcance de la evaluación de seguridad, y lo determinará de acuerdo con este, en especial en lo que se refiere a las horas/fechas de inicio y finalización, para no interferir en las actividades clave de Barclays. 	<p>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.</p> <p>Podría revelarse información de Barclays o producirse una pérdida de servicio. Esto tendría como consecuencia una sanción legal o normativa o daños en la reputación.</p>

	<ul style="list-style-type: none"> • Todos los problemas cuyo riesgo se haya decidido aceptar se comunicarán a Barclays para acordarlos con el banco (Dirección General de Seguridad - equipo ECAM). 	
<p>23. Criptografía</p>	<ul style="list-style-type: none"> • Justificación de la criptografía - El proveedor documentará la justificación para utilizar tecnología criptográfica y la revisará para garantizar que siga siendo adecuada para su finalidad. • Procedimientos de ciclo de vida de la criptografía - El proveedor conservará y mantendrá una serie documentada de procedimientos de gestión de ciclo de vida de la criptografía que detallen los procesos de extremo a extremo para la gestión de claves desde la generación, carga y distribución a la destrucción. • Aprobación de operaciones manuales - El proveedor garantizará que todos los eventos gestionados por humanos para las claves y certificados digitales, incluyendo el registro y generación de nuevas claves y certificados, sean objeto de aprobación al nivel adecuado y se conserve un registro de dichas aprobaciones. • Certificados digitales - El proveedor garantizará que todos los certificados se obtengan de una serie de autoridades certificadoras (CA) aprobadas y validadas con servicios de revocación y políticas de gestión de certificados, y deberá garantizar que solo se utilicen certificados autofirmados cuando no sea técnicamente capaz de compatibilizar una solución basada en CA, y deberá contar con controles manuales implementados para garantizar la integridad, autenticidad de las claves y revocación y renovación puntual. • Generación de claves y criptoperiodo - El proveedor deberá garantizar que todas las claves se generen aleatoriamente a través de hardware certificado o un generador de números pseudoaleatorios criptográficamente seguro (CSPRNG) en forma de software. <ul style="list-style-type: none"> ○ El proveedor deberá garantizar que todas las claves se sometan a una vida de criptoperiodo definida y limitada tras el cual se sustituyan o desactiven. Esto también debe ser acorde a los requisitos del National Institute of Standards and Technology (NIST) y de la industria aplicables • Protección del almacenamiento de claves - El proveedor deberá garantizar que solo existan claves criptográficas secretas/privadas en las siguientes formas: <ul style="list-style-type: none"> ○ En el límite criptográfico de un dispositivo/módulo con hardware certificado. ○ En forma encriptada bajo otra clave establecida o derivada de una contraseña. ○ En partes de componentes divididos entre grupos de custodia diferentes. ○ No encriptadas en la memoria host durante el período de operación criptográfica, salvo que se precise en la protección de HSM. • El proveedor garantizará que las claves se generen y mantengan dentro del límite de la memoria de HSM para las claves de alto riesgo. Esto incluye: <ul style="list-style-type: none"> ○ Claves para servicios regulados donde los HSM sean obligatorios. ○ Certificados que representen a Barclays de CA públicos. ○ Certificados raíz, de emisión, OCSP y RA (autoridad de registro) empleados para emitir certificados que protejan los servicios de Barclays. ○ Claves que protejan depósitos agregados almacenados de claves, credenciales de acreditación o datos PII. 	<p>Si este control no se implementa, puede que no se establezcan los controles físicos y técnicos apropiados. Esto tendría como consecuencia retrasos o interrupciones del servicio, o infracciones de ciberseguridad.</p>

	<ul style="list-style-type: none"> • Copia de seguridad y almacenamiento de claves - El proveedor mantendrá una copia de seguridad de todas las claves para evitar que el servicio se vea interrumpido si estas se corrompen o deben restaurarse. El acceso a las copias de seguridad está restringido a centros seguros sometidos a conocimiento distribuido y control dual. Las copias de seguridad de las claves deben disponer de una protección criptográfica como mínimo igual de fiable que la de las claves en uso. • Inventario - El proveedor mantendrá un inventario completo y actualizado del uso criptográfico en los servicios que preste a Barclays que detalle todas las claves criptográficas, certificados digitales, software criptográfico y hardware criptográfico gestionado por el proveedor para evitar daños en caso de producirse un incidente. Esto se evidencia mediante la firma del inventario revisado al menos trimestralmente y suministrado a Barclays. Los inventarios deberán incluir, cuando proceda: <ul style="list-style-type: none"> ○ Equipo de soporte informático ○ Activos relacionados ○ Algoritmos, longitud de claves, entorno, jerarquía de las claves, autoridad de los certificados, huellas digitales, protección del almacenamiento de las claves y objetivo operativo y técnico. • Objetivo funcional y operativo - Las claves deben contar con un solo objetivo operativo y funcional y no compartirse entre diferentes servicios o fuera de los servicios de Barclays. • Pistas de auditoría - El proveedor llevará a cabo y conservará pruebas de la revisión de registros auditable cada trimestre como mínimo para todos los eventos de gestión del ciclo de vida de los certificados y las claves que demuestren una cadena completa de custodia para todas las claves, incluyendo la generación, distribución, carga y destrucción para detectar los usos no autorizados. • Hardware - El proveedor almacena los dispositivos de hardware en áreas seguras y conserva una pista de auditoría durante todo el ciclo de vida para garantizar que la cadena de custodia de los dispositivos criptográficos no se vea comprometida. Esta pista se revisa trimestralmente. <ul style="list-style-type: none"> ○ El proveedor debe garantizar que el hardware criptográfico cuente como mínimo con una certificación FIPS140-2 de nivel 2 y que alcance el nivel 3 en gestión de claves criptográficas y seguridad física o PCI HSM. El proveedor podrá optar por permitir tarjetas inteligentes de chip o tokens electrónicos con la certificación FIPS como hardware aceptable para almacenar claves que representen y mantengan personas o clientes individuales fuera de las instalaciones. • Compromiso de claves - El proveedor mantendrá y controlará un plan de compromiso de claves para garantizar que se generen independientemente claves de sustitución para evitar que las claves comprometidas ofrezcan información relativa a su sustitución. Si se produce un incidente de compromiso, Barclays debe ser notificada en el Centro de Operaciones Conjuntas (JOC) de la Dirección General de Seguridad de Barclays (CSO) - gcsojoc@barclays.com. • Fortaleza de los algoritmos y claves - El proveedor garantiza que los algoritmos y la longitud de las claves empleadas cumple los requisitos aplicables del National Institute of Standards and Technology (NIST) y del sector. 	
--	---	--

	<ul style="list-style-type: none"> ○ Los algoritmos fuertes y la longitud de las claves minimiza el riesgo de que los datos sensibles se pierdan o se vean comprometidos por los hackers con capacidades de procesamiento sofisticadas. ○ La intensidad del encriptado aplicado será acorde a la tolerancia al riesgo, ya que puede tener un impacto operativo o de rendimiento. 	
<p>24. Computación en la nube</p>	<p>El proveedor debe contar con la certificación ISO/IEC 27017 o 27001 o SOC 1 o 2 o con procesos empresariales establecidos y que los sustenten, así como con medidas técnicas aplicadas para garantizar que el uso de tecnologías en la nube esté sometido a los controles de seguridad apropiados aplicables.</p> <p>Los datos de Barclays almacenados en la nube como parte del servicio prestado a Barclays deben ser aprobados por Barclays (Dirección General de Seguridad - equipo ECAM).</p> <p>Los controles en la nube deben incluir los siguientes modelos de despliegue (IaaS/PaaS/SaaS):</p> <ul style="list-style-type: none"> • Gestión de identidad y acceso/control de acceso • Conectividad de red • Protección de datos (en tránsito/reposo/almacenados) • Registro y monitorización de seguridad • Gestión de encriptado y claves • Seguridad de las aplicaciones e interfaces • Seguridad de las infraestructuras y virtualización • Segregación de servicios 	<p>Si este control no se implementa correctamente, la seguridad de los datos de Barclays protegidos podría verse afectada. Esto tendría como consecuencia una sanción legal o normativa, o daños en la reputación.</p>
<p>25. Espacio dedicado al banco (EDB)</p>	<p>Para servicios suministrados que requieran Espacio dedicado al banco (EDB), deben establecerse requisitos físicos y técnicos de EDB. (Si el EDB fuera un requisito del servicio, se aplicarían los requisitos de control).</p> <p>Los diferentes tipos de EDB son:</p> <p>Nivel 1 (primera clase) - Toda la infraestructura informática es gestionada por Barclays a través de la provisión de una LAN, WAN y Desktop gestionadas por Barclays hasta una sede del proveedor con un espacio exclusivo de Barclays.</p> <p>Nivel 2 (clase empresarial) - Toda la infraestructura informática es gestionada por el proveedor y se conecta a las pasarelas de Barclays - dispositivos LAN, WAN y Desktop - es propiedad y está gestionada por el proveedor.</p> <p>Nivel 3 (clase económica) - Toda la infraestructura informática es gestionada por el proveedor y se conecta a las pasarelas de internet de Barclays - los dispositivos de LAN, WAN y Desktop son propiedad y están gestionados por el proveedor.</p>	<p>Si este control no se implementa, puede que no se establezcan los controles físicos y técnicos apropiados. Esto tendría como consecuencia retrasos o interrupciones del servicio, o infracciones de ciberseguridad.</p>

25.1 EDB - Separación física	El área física ocupada debe dedicarse a Barclays, y no se debe compartir con otras empresas / proveedores. Debe estar lógica y físicamente separada.
25.2 EDB - Control del acceso físico	<ul style="list-style-type: none"> • El proveedor debe contar con un proceso de acceso físico que incluya métodos de acceso y autorización del EDB en el que se prestan los servicios. • La entrada y salida en las zonas EDB debe limitarse y controlarse mediante mecanismos de control del acceso físico para garantizar que solo se permita el acceso al personal autorizado. • Una tarjeta electrónica de acceso autorizado para acceder a las áreas EDB de las instalaciones. • El proveedor debe llevar a cabo trimestralmente comprobaciones para garantizar que solo personas autorizadas cuenten con acceso EDB. Las excepciones se investigan en profundidad hasta su resolución. • Los derechos de acceso se retiran en el plazo de 24 horas para todas las personas que se trasladan y dejan la empresa. • Utilizar protecciones para controlar rutinariamente el interior de los EDB con el fin de identificar de manera efectiva los accesos no autorizados o las actividades potencialmente maliciosas • Deben activarse controles automáticos seguros para el acceso al EDB, como: <ul style="list-style-type: none"> Para el personal autorizado: <ul style="list-style-type: none"> ○ Tarjeta de identificación con foto siempre visible ○ Implementación de lectores de tarjeta por proximidad ○ Habilitación de un mecanismo antirretorno • El proveedor contará con procesos y procedimientos para controlar y monitorizar a las personas externas, incluyendo terceros con acceso físico a las áreas EDB para realizar tareas de mantenimiento y limpieza.
25.3 EDB - Videovigilancia	<ul style="list-style-type: none"> • Implementación de videovigilancia en las áreas EDB para detectar de manera efectiva el acceso no autorizado o las actividades maliciosas y ayudar en las investigaciones. • Todos los puntos de entrada y salida de las EDB deben contar con videovigilancia. • Las cámaras de seguridad se colocarán apropiadamente y ofrecerán imágenes claras e identificables en todo momento para capturar las actividades maliciosas y ayudar en las investigaciones. <p>El proveedor almacenará las imágenes capturadas por los CCTV durante 30 días y las grabadoras deben estar adecuadamente colocadas para evitar la modificación, eliminación o visualización 'casual' de las pantallas de CCTV asociadas, y el acceso a las grabaciones debe estar controlado y limitado solo a personas autorizadas.</p>
25.4 EDB - Acceso a la red de Barclays y tokens de autenticación de Barclays	<ul style="list-style-type: none"> • Cada usuario individual debe autenticarse únicamente en la red de Barclays desde el EDB con un token de autenticación multifactor suministrado por Barclays • El proveedor mantendrá registros de las personas que han pedido tokens de autenticación de Barclays y realizará una reconciliación trimestral. • Barclays desactivará las credenciales de autenticación una vez que se notifique que el acceso ya no es necesario (por ejemplo, después de empleados, reasignación de proyectos, etc.) en el plazo de veinticuatro (24) horas. • Barclays desactivará inmediatamente las credenciales de autenticación si no se han utilizado durante cierto tiempo (dicho período no deberá superar un mes). • Los servicios con acceso de impresión a distancia a través de una aplicación Citrix de Barclays deben ser aprobados y certificados por Barclays (Dirección General de Seguridad - equipo ECAM). El proveedor mantendrá registros y realizará reconciliaciones trimestrales.

	Consulte la sección 11 - Seguridad de los accesos remotos
25.5 EDB - Soporte fuera del horario laboral	Por defecto no se proporciona acceso remoto al entorno EDB para labores de soporte fuera del horario laboral/teletrabajo. Todo acceso remoto debe ser aprobado por los equipos pertinentes de Barclays (incluida la Dirección General de Seguridad - equipo ECAM).
25.6 EDB - Seguridad de la red	<ul style="list-style-type: none"> • Mantener un inventario actualizado de todos los límites de la red de la organización (a través de una arquitectura/diagrama de red). • El diseño e implementación de la red debe revisarse como mínimo anualmente. • La red EDB debe estar segregada lógicamente de la red corporativa del proveedor por un firewall y todo el tráfico de entrada y salida debe estar restringido y controlado. • La configuración de enrutamiento debe garantizar que solo se establezcan conexiones con la red de Barclays y evitar el enrutamiento a otras redes del proveedor • El router periférico del proveedor que se conecte con las pasarelas de la extranet de Barclays debe configurarse de forma segura con un concepto de controles de limitación de puertos, protocolos y servicios; <ul style="list-style-type: none"> ○ Garantizar que el registro y el seguimiento deben estar activados. • La red EDB debe ser monitorizada y solo deben permitirse dispositivos autorizados por medio de controles de acceso a la red pertinentes. <p>Consulte la sección 9 - Seguridad de la red y límites</p>
25.7 EDB - Red inalámbrica	Las redes inalámbricas deben estar deshabilitadas para el segmento de la red de Barclays que preste servicios al banco.
25.8 EDB - Seguridad de los extremos	<p>Deben configurarse equipos de escritorio seguros según los procedimientos recomendados del sector para los ordenadores de la red EDB</p> <p>Los equipos de seguridad de los dispositivos de extremo EDB deben contar con:</p> <ul style="list-style-type: none"> • Encriptado de disco; • Desactivación del arranque desde otros dispositivos activos; • Deshabilitación de todo el software/servicios/puertos innecesarios. • Deshabilitación del acceso con derechos de administración para el usuario local. • El personal del proveedor no podrá realizar cambios en la configuración básica, como el pack de servicios y los servicios por defecto, etc. • El puerto USB debe estar deshabilitado para prohibir las copias de datos de Barclays a soportes externos • Actualización con las últimas firmas antivirus y parches de seguridad. • Prevención de la pérdida de datos limitada a no cortar-copiar-pegar o imprimir pantalla o la herramienta de captura de impresión de datos de Barclays • Por defecto, el acceso a las impresoras debe estar deshabilitado. • La compartición/transmisión de datos de Barclays debe estar deshabilitada utilizando herramientas/software de mensajería instantánea; • Capacidad y procesos para detectar el software no autorizado identificado como malicioso y evitar la instalación de software no autorizado; <p>Consulte la sección 15 - Control de la seguridad en los extremos</p>

<p>25.9 EDB - Correo electrónico e internet</p>	<ul style="list-style-type: none"> • La conexión de red debe configurarse de forma segura para restringir el correo electrónico y la actividad de Internet en la red del EDB. • El proveedor debe limitar la capacidad para acceder a sitios de redes sociales, servicios de webmail y sitios que puedan almacenar información en internet como Google Drive, Dropbox, iCloud. • La transmisión no autorizada de datos de Barclays fuera de la red EDB debe protegerse de las fugas de datos: <ul style="list-style-type: none"> • Correo electrónico • pasarela web/de internet (incluyendo almacenamiento online y webmail) • Aplicar filtros URL basados en la red que limiten la capacidad del sistema para conectarse solo a sitios internos o de internet de una organización proveedora • bloquear todos los adjuntos y/o función de carga en sitios web • Garantizar que solo se permiten navegadores web y clientes de correo electrónico totalmente compatibles. 	
<p>25.10 EDB - BYOD/Dispositivo personal</p>	<p>Los dispositivos personales/ BYOD no deben tener permitido el acceso al entorno y/o los datos de Barclays</p>	
<p>Derecho de inspección</p>	<p>El proveedor debe permitir 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 debe permitir a Barclays realizar una inspección al menos cada año o inmediatamente después de producirse un incidente de seguridad.</p> <p>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.</p> <p>El proveedor debe prestar a Barclays toda la asistencia que solicite en términos de razón en relación con cualquier inspección y documentación presentada durante una inspección que deba completarse y devolverse a Barclays.</p>	<p>Si no aceptan, los proveedores no podrán garantizar plenamente que se cumplen estas obligaciones de seguridad.</p>

Apéndice A. Glosario

Definiciones	
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.
Copia de seguridad, copia de seguridad	Una copia de seguridad o el proceso de copia de seguridad se refiere a la realización de copias de datos para poder recuperar el original tras un incidente de pérdida de datos.
Espacio dedicado al banco	Espacio dedicado al banco significa cualquier instalación propiedad de un miembro del grupo del proveedor o de cualquier subcontratista, o bajo su control, que se dedique exclusivamente a Barclays y desde la que se presten o realicen los servicios.
BYOD	Trae tus propios dispositivos
Criptografía	La aplicación de teoría matemática para desarrollar técnicas y algoritmos que pueden aplicarse a los datos para garantizar objetivos tales como la confidencialidad, la integridad de los datos y/o la autenticación.
Datos	Registro de datos, conceptos o instrucciones en un medio de almacenamiento para la comunicación, recuperación y tratamiento por medios automáticos y presentación como información comprensible por humanos.
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.
ECAM	Equipo externo de seguimiento y ciberseguridad que evalúa la posición de seguridad del proveedor
Cifrado	La transformación de un mensaje (datos, voz o vídeo) en un formato sin significado que no puedan entender lectores no autorizados. Esta transformación se realiza partiendo de texto sin formato a un formato de texto cifrado.
HSM	Módulo de seguridad de hardware. Dispositivo dedicado que ofrece generación, almacenamiento y uso de claves criptográficas seguras, incluyendo aceleración de los procesos criptográficos.
Activo de información	Toda información que tenga valor, considerado en términos de confidencialidad, integridad y requisitos de disponibilidad. O cualquier parte individual o grupo de información que tenga un valor para la organización.
Responsable de activos de información	La persona de la empresa responsable de clasificar un activo y asegurar que se maneja correctamente.
Privilegio mínimo	El nivel mínimo de acceso/permiso que permite al usuario o a una cuenta desempeñar su función empresarial.
Dispositivo/equipo de red	Cualquier dispositivo informático conectado a una red empleado para gestionar, ofrecer soporte o controlar una red. Esto podría incluir, entre otros, routers, switches, firewalls, equilibradores de carga.
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.
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).
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.
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.
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.
Debería/debe	Esta definición significa que las implicaciones serán totalmente comprendidas y se evaluarán cuidadosamente antes de elegir una opción diferente.
Incidente de seguridad	<p>Los incidentes de seguridad se definen como eventos que infringen una política de seguridad explícita o implícita.</p> <ul style="list-style-type: none"> • Los intentos (fallidos o exitosos) de obtener acceso no autorizado a un sistema o sus datos. • Perturbaciones no deseadas o denegaciones de servicio. • Uso no autorizado de un sistema para procesar o almacenar datos. • Cambios en las características de hardware, firmware o software del sistema sin el conocimiento, dirección o consentimiento del propietario. • Vulnerabilidades de una aplicación que dan lugar a un acceso no autorizado a datos.

Apéndice B. Plan del etiquetado de la información de Barclays

Tabla B1: Plan del etiquetado de la información de Barclays

Etiqueta	Definición	Ejemplos
Secreta	<p>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).</p> <p>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.</p>	<ul style="list-style-type: none"> • 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).

<p>Restringida – Interna</p>	<p>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.</p> <p>La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero).</p> <p>Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla.</p>	<ul style="list-style-type: none"> • Estrategias y presupuestos • Evaluaciones del personal • Remuneración de los empleados y datos del personal. • Evaluaciones de la vulnerabilidad
<p>Restringida- Externa</p>	<p>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.</p> <p>La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero).</p> <p>Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla.</p>	<ul style="list-style-type: none"> • 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 • Resultados de auditorías e informes
<p>Sin restricción</p>	<p>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.</p>	<ul style="list-style-type: none"> • Material de marketing • Publicaciones • Anuncios públicos • Anuncios de ofertas de trabajo • Información sin impacto para Barclays.

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

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

Fase del ciclo de vida	Secreta	Restringida – Interna	Restringida – Externa
Creación e introducción	<ul style="list-style-type: none"> A los activos se les asignará un responsable de la información. 	<ul style="list-style-type: none"> A los activos se les asignará un responsable de la información. 	<ul style="list-style-type: none"> A los activos se les asignará un responsable de la información.
Almacenamiento	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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.
Acceso y uso	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Los activos en papel llevarán una etiqueta de información visible en cada página. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Los activos en papel llevarán una etiqueta de información visible. La etiqueta irá como mínimo en la página que lleve el título.

	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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.
Archivo y eliminación	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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.

	<ul style="list-style-type: none">• 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 las jurisdicciones con secreto
bancario (Suiza/Mónaco)

Título / Área de control	Descripción del control	Por qué es importante
<p>1. Funciones y responsabilidades</p>	<p>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.</p> <p>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) El número de empleados con acceso a los CID debe mantenerse a un nivel mínimo basado en el principio de la necesidad de conocer.</p>	<p>Una definición clara de las funciones y las responsabilidades contribuye a la implantación del Anexo sobre las obligaciones de control de proveedores externos.</p>
<p>2. Notificación de violaciones de la seguridad de los CID</p>	<p>Existirán controles y procesos documentados que garanticen la notificación y la gestión de cualquier violación de la seguridad que repercuta en los CID.</p> <p>El proveedor responderá a toda vulneración de los requisitos de gestión (definidos en la tabla B2) y se comunicará a la entidad de Barclays correspondiente sujeto al secreto bancario de forma inmediata (como máximo 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.</p> <p>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.</p> <p>Si el proveedor externo ofrece servicios de consultoría y un empleado de dicho proveedor ha activado incidentes de prevención de la pérdida de datos, el banco notificará el incidente al proveedor y, llegado el caso, podrá solicitar la sustitución del empleado.</p>	<p>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.</p> <p>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.</p>

<p>3. Educación y conocimiento</p>	<p>Los empleados del proveedor que tengan acceso a los CID o los gestionen deberán realizar un curso de formación* que incluya los requisitos de secreto bancario de los CID tras cualquier cambio en la normativa, o al menos una vez al año.</p> <p>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.</p> <p>El proveedor llevará un seguimiento de los empleados que han realizado el curso de formación.</p> <p>* Las jurisdicciones con secreto bancario ofrecerán información sobre el contenido previsto para los cursos de formación.</p>	<p>En la educación y el conocimiento se basan todos los demás controles de este anexo.</p>
<p>4. Plan de etiquetado de la información</p>	<p>Cuando proceda*, el proveedor deberá aplicar el Plan del etiquetado de la información de Barclays (Tabla E1 del Apéndice E), 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.</p> <p>Los requisitos de gestión de los CID se incluyen en la Tabla E2 del Apéndice E.</p> <p>* «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.</p>	<p>Resulta esencial disponer de un inventario completo y exacto de activos de información para garantizar la implantación de los controles pertinentes.</p>
<p>5. Almacenamiento externo/computación en la nube</p>	<p>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 el evado que presentan.</p>	<p>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 normativa, o daños en la reputación.</p>

Apéndice C: Glosario

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

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

Apéndice D: DATOS QUE IDENTIFICAN AL CLIENTE

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

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

- **Los CIDI N1** pueden definirse como identificadores únicos (propiedad del Banco) que permiten identificar de manera única a un cliente en caso de que se otorgue acceso a aplicaciones bancarias u otras **aplicaciones de terceros**. El identificador no será ambiguo ni dependerá de la interpretación y puede incluir por ejemplo el número de cuenta, el código IBAN, el número de la tarjeta de crédito, etc.
- **Los CIDI N2** pueden definirse como información (propiedad del cliente) a partir de la cual se podría llegar a identificar a un cliente combinándola con otra. Aunque esta información no puede utilizarse por sí sola para identificar a un cliente, cuando se emplea junto con otra información sí que podría identificarlo. Los CIDI N2 deben protegerse y gestionarse con el mismo rigor que los CIDD.
- **Los CIDI N3** pueden definirse como identificadores únicos pero anonimizados (propiedad del Banco) que permiten identificar a un cliente en caso de que se otorgue acceso a aplicaciones bancarias. La diferencia con los CIDI N1 es la clasificación de la información que les corresponde, como Restringida – Externa en lugar de secreto bancario, lo que significa que no están sujetos a los mismos controles.

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

Los CIDI N1 directos e indirectos no se compartirán con ninguna persona externa al banco y se respetará en todo momento el principio basado en la necesidad de conocerlos. Los CIDI N2 pueden compartirse con quienes necesiten conocerlos, pero no en combinación con otros CID. Si se comparten varios CID, existe la posibilidad de crear una «combinación tóxica» que pudiera llegar a revelar la identidad de un cliente. Definimos una combinación tóxica cuando se combinan al menos dos CIDI N2. Los CIDI N3 se pueden compartir, ya que no están clasificados como información con el nivel de secreto bancario, a menos que un uso recurrente del mismo identificador pueda provocar una recopilación de datos CIDI N2 suficientes para revelar la identidad de un cliente.

Clasificación de la información	Secreto bancario			Restringida – Interna
Clasificación	CID directos (CIDD)	CID directos (CIDI)		
		Indirectos (N1)	Posiblemente indirectos (N2)	Identificador impersonal (N3)
Tipo de información	Nombre del cliente	Número de contenedor / ID de contenedor	Fecha de nacimiento	Cualquier identificador estrictamente interno de la aplicación de alojamiento/procesamiento de CID
	Nombre de la compañía	Número MACC (cuenta de dinero con un ID de contenedor Avaloq)	Fecha de nacimiento	Identificador dinámico
	Extracto de cuenta	ID de SDS	Nacionalidad	ID de función parte de CRM
	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	Mensaje SWIFT	Valor de la transacción/posición general	
	Nombre del puesto o cargo de persona políticamente expuesta:	ID interna de socio empresarial	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	

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

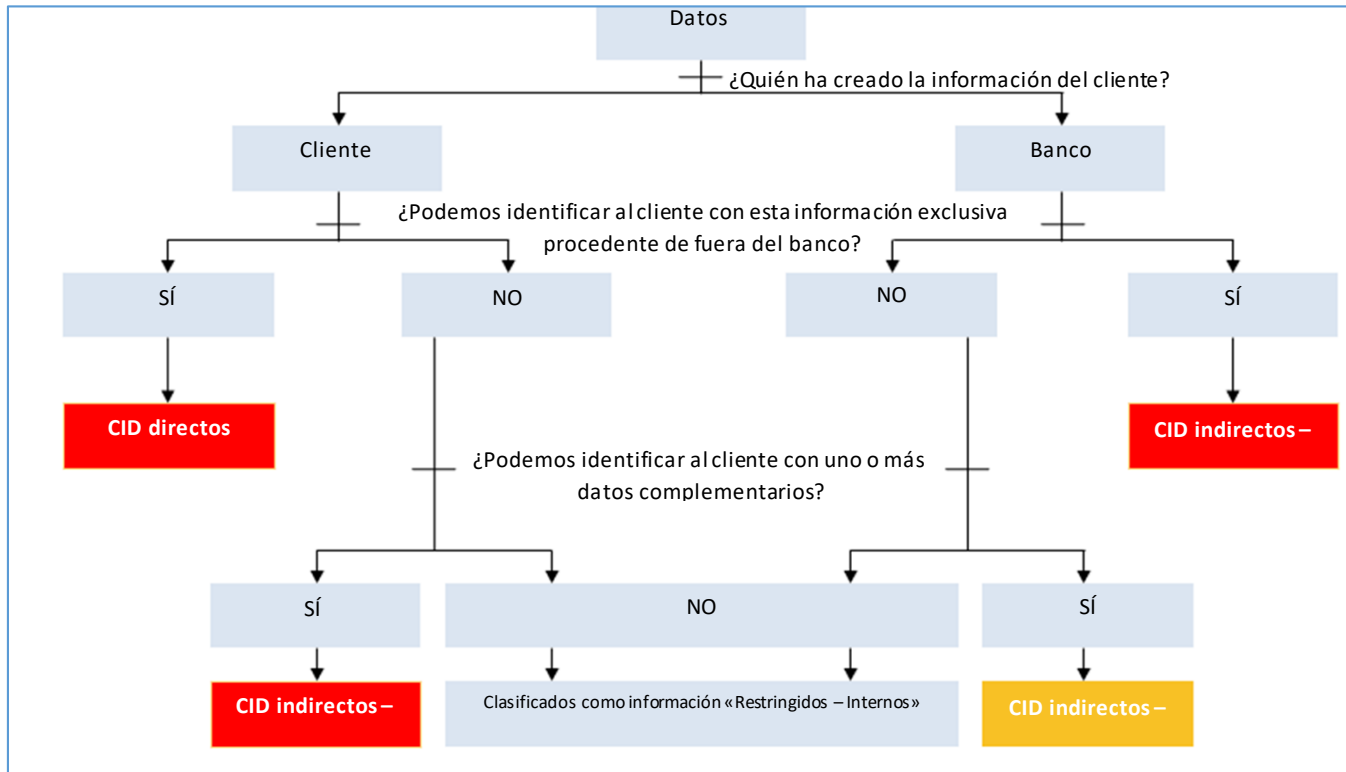
(DIDD) = Vulneración del secreto bancario

2. ID de contenedor

(N1CIDI) = Vulneración del secreto bancario

3. Situación patrimonial + Nacionalidad

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



Apéndice E: Plan del etiquetado de la información de Barclays

Tabla E1: Plan del etiquetado de la información de Barclays

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

Etiqueta	Definición	Ejemplos
----------	------------	----------

<p>Secreto bancario</p>	<p>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 administrativas, tales como multas y pérdida de licencias bancarias, si se le revela a personal no autorizado tanto interno como externo.</p>	<ul style="list-style-type: none"> • Nombre del cliente • Dirección del cliente • Firma • Dirección IP del cliente (otros ejemplos en el Apéndice D)
-------------------------	---	--

Etiqueta	Definición	Ejemplos
<p>Secreta</p>	<p>Se clasificará la información como «secretas» 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).</p> <p>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.</p>	<ul style="list-style-type: none"> • 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.

		<ul style="list-style-type: none"> • Pronósticos de beneficios o resultados financieros anuales (antes de hacerse públicos). • Cualquier elemento cubierto por un Acuerdo de confidencialidad formal.
Restringida – Interna	<p>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.</p> <p>La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero).</p> <p>Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla.</p>	<ul style="list-style-type: none"> • 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	<p>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.</p> <p>La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero).</p> <p>Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla.</p>	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Material de marketing. • Publicaciones. • Anuncios públicos. • Anuncios de ofertas de trabajo. • Información sin impacto para Barclays.
-----------------	--	---

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

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

Fase del ciclo de vida	Requisitos del secreto bancario
Creación y etiquetado	De acuerdo con «Restringida-Externa» y: <ul style="list-style-type: none"> • A los activos se les asignará un responsable de CID.
Almacenamiento	De acuerdo con «Restringida-Externa» y: <ul style="list-style-type: none"> • 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	<p>De acuerdo con «Restringida-Externa» y:</p> <ul style="list-style-type: none"> 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.
	<ul style="list-style-type: none"> 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	<p>De acuerdo con «Restringida-Externa» y:</p> <ul style="list-style-type: none"> 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	<p>De acuerdo con «Restringida-Externa»</p>

*** 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	<ul style="list-style-type: none"> A los activos se les asignará un responsable de la información. 	<ul style="list-style-type: none"> A los activos se les asignará un responsable de la información. 	<ul style="list-style-type: none"> A los activos se les asignará un responsable de la información.

Almacenamiento	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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.

		<ul style="list-style-type: none"> Los activos en formato electrónico se protegerán mediante controles de gestión de acceso lógico apropiados. 	<ul style="list-style-type: none"> Los activos en formato electrónico se protegerán mediante controles de gestión de acceso lógico apropiados.
Uso compartido	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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.

		<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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.