Obligaciones de control de proveedores (SCO)

Seguridad de la información y ciberseguridad (ICS)

Versión 12.0 Octubre 2022

Título / Área de control	Descripción del control	Por qué es importante
1. Uso autorizado	El proveedor debe distribuir los requisitos de uso aceptable para informar de sus responsabilidades a todos sus empleados, incluidos contratistas, subcontratistas y subencargados del tratamiento. Deberán considerarse los siguientes temas: • el uso de internet; • el uso basado en software como servicio (SaaS); • el uso de depósitos de códigos públicos; • el uso de 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, la preservación y el almacenamiento de los activos de información de Barclays; • la salida de canales de filtración de datos; y • el riesgo y las consecuencias de un uso indebido de los mencionados elementos y/o cualquier resultado ilícito, nocivo u ofensivo derivado de dicho uso indebido. El proveedor emprenderá las acciones necesarias para garantizar el cumplimiento de estos requisitos de uso aceptable.	Los requisitos en cuanto a uso aceptable contribuyen a respaldar el entorno de control que protege los activos de información.
2. Seguridad de la red y límites	El proveedor debe asegurarse de que todos los sistemas y aplicaciones que opere, o bien que operen sus subcontratistas o subencargados, a fin de prestar soporte al servicio (o los servicios) de Barclays estén protegidos frente a **amenazas de red entrantes y salientes.** Se deben implementar controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados frente a accesos no autorizados. El proveedor debe detectar e identificar cualquier alerta o infracción de seguridad, protegerse en consecuencia y responder ante cada situación específica.	Si este servicio no se implementa, los atacantes podrían debilitar la seguridad de las redes externas o internas para obtener acceso al servicio o a los datos que contiene.

	Los controles de seguridad de la red garantizan la protección de la información en las redes y en las instalaciones complementarias de tratamiento de información, y deben incluir, entre otras cuestiones, los siguientes aspectos: • Mantener un inventario actualizado de todos los límites de la red de la organización (a través de una arquitectura/diagrama de red), que deberá revisarse al menos una vez al año. • Las conexiones externas a la red del proveedor deben documentarse, comprobarse y aprobarse 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 debe disponer de tecnologías de prevención de intrusiones en la red para detectar y evitar el tráfico malicioso entrante o saliente, así como para actualizar las bases de datos de firmas de acuerdo con los procedimientos recomendados del sector y aplicar las actualizaciones del proveedor de soluciones de forma oportuna. • El uso de capacidades de firewall de red fuertes que ofrezcan una capa de defensa perimetral frente a los ataques maliciosos contra las redes. • El tráfico de la red de Internet debe pasar a través de un proxy que esté configurado para filtrar conexiones no autorizadas. • Los dispositivos de red deben endurecerse de forma segura para evitar los ataques maliciosos. • 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. • Separación lógica de los puertos/las interfaces de gestión de dispositivos del tráfico/LAN de usuarios; controles de autenticación apropiados. • Realizar lecturas regulares desde fuera de cada límite de red para detectar las conexiones no autorizadas accesibles a través del límite. • Comunicaciones seguras entre dispositivos y estaciones/consolas de gestión. • Comprobación de que el registro y la supervisión incluyen la detección y alerta de actividades sospechosas (mediante el uso de controles de patrones de comportamiento e indicadores de compromiso); p. ej., a través de la gestión de eventos e información de seguridad (SIEM). • La conexión de red entre centros de datos/proveedores de servicios de red/interoficina debe encriptarse sobre un protocolo seguro. Los datos/activos de	

	información de Barclays en tránsito dentro de la red de área amplia (WAN) del proveedor deben estar encriptados. • El proveedor debe revisar las reglas de firewall (firewall externo e interno) al menos una vez al año. • El proveedor debe asegurarse de que el acceso a la red interna se supervisa mediante los controles de acceso a la red adecuados. • Únicamente debe permitirse la conexión a la red del proveedor a los dispositivos autorizados (dispositivos de terceros con diseño seguro y sin BYOD). • Todo acceso inalámbrico a la red se somete a protocolos de autorización, autenticación, segmentación y cifrado seguro para evitar infracciones de seguridad. • El acceso de inicio de sesión remoto a la red del proveedor debe utilizar autenticación multifactor. • El proveedor debe tener una red segregada (lógicamente) para el servicio (o los servicios) de Barclays. El proveedor debe garantizar que ningún servidor ni ninguna aplicación empleados para prestar servicio a Barclays se desplieguen 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. El proveedor que aloje información de Barclays (incluyendo subcontratistas y subencargados) en un centro de datos o en la nube debe contar con un certificado de procedimientos recomendados del sector para la gestión de la seguridad de la red. Redes T2 y T3 - • 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/local 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; o Comprobación de que el registro y la supervisión incluyen la detección y alerta de actividades sospechosas (mediante el uso de controles de patrones de comportamiento e indicadores de compromiso); p. ej., a través de la gestión de eventos e información de seguridad (SIEM).	

	El proveedor externo debe garantizar que todos los sistemas y las aplicaciones que presten servicios que Barclays considere de alto riesgo, lo que comunicará al proveedor, se segmentan en la red de acuerdo con los siguientes principios: i. Se debe adoptar un enfoque de segmentación para limitar la exposición al riesgo, inhibir el movimiento lateral a través de la red y reducir el riesgo de transmisión de la red. Las aplicaciones se deben desplegar en segmentos autónomos para ayudar a limitar el riesgo en la medida de lo razonablemente posible. Ejemplo: zona de pagos más rápidos. ii. Toda la infraestructura y los datos relacionados con las aplicaciones empresariales deben implementarse en una zona de aplicaciones segura y autónoma siempre que sea posible y separarse de la red interna de Barclays mediante una tecnología de aplicación aprobada por CSO (p. ej., firewalls de red, solución de segmentación aprobada). Nota: Algunas situaciones pueden justificar la división de componentes como la aplicación y la base de datos en varias zonas; por ejemplo, cuando se aprovechan las plataformas compartidas. Cada aplicación debe evaluarse individualmente, con el enfoque más apropiado, definido y acordado con un consultor de seguridad de CSO. iii. Los servicios deben estar separados física o lógicamente. La estructura de red subyacente (por ejemplo, cableado/conmutadores) se puede compartir con otras aplicaciones y servicios; es decir, los segmentos se pueden definir lógicamente sin necesidad de forzar la segmentación mediante la separación física del resto de la red de Barclays. iv. Las zonas de aplicación deben restringir los flujos de tráfico hacia y desde otras zonas (incluida la red CIPE interna), en función de las necesarias para el funcionamiento del servicio y de cualquier herramienta aprobada de gestión, supervisión y seguridad. Las configuraciones deben estipular puertos, protocolos y direcciones IP específicos para las rutas de comunicación permitidas; todas las demás comunicaciones deben estar restringidas de forma predeterminada. Las reglas con rangos se deben evitar y aprobar por excepción solo para garantizar que únicamente se habilitan los requisitos mínimos de conectividad. v. Los contenedores deben estar firmemente segregados con controles lógicos avanzados que impidan el movimiento lateral entre contenedores y, por lo tanto, refuercen el aislamiento. El compromiso de un contenedor no debe conducir al compromiso de otros contenedores que se ejecuten en el mismo host/clúster. vi. Todas las implementaciones de segmentación deben ofrecer una capacidad de gestión de políticas centralizada con funcionalidad (o integración) para verificar e	

	informar del cumplimiento de políticas (consulte el documento de cumplimiento de firewall) y proporcionar un registro auditable de los cambios. vii. Siempre que sea posible/factible, se deben realizar inspecciones/controles de estado. viii. Las capacidades de segmentación deben funcionar de forma segura; por ejemplo, si la capacidad falla, los conjuntos de reglas aprobados para bloquear/permitir el tráfico deben seguir aplicándose. ix. Cualquier tráfico entre sistemas de producción y no producción en zonas de aplicación solo se debe permitir por excepción y se debe registrar. **Orientación para el cliente de servicios en la nube (proveedor) utilizados para prestar servicio(s) a Barclays** El cliente de servicios en la nube (CSC) debe asegurarse de que se implementan los controles de seguridad de red adecuados para proteger el servicio de Barclays. • El cliente de servicios en la nube (CSC) debe definir sus requisitos para separar las redes con el fin de lograr el aislamiento de arrendatarios en el entorno compartido de un servicio en la nube y verificar que el proveedor de servicios en la nube cumple esos requisitos. • La política de control de acceso del cliente de servicios en la nube para el uso de servicios de red debe especificar los requisitos para el acceso de los usuarios a cada servicio en la nube independiente que se utilice. *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.*	
3. Detección de denegación de servicio	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). 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 DDoS/DoS, a fin de garantizar la disponibilidad. Si el proveedor aloja **sistemas y aplicaciones que prestan servicios** y mantienen datos de Barclays, o que respaldan un servicio de categoría de resiliencia 0 o 1, debe contar con una protección DoS adecuada para garantizar la disponibilidad.	De no aplicarse este principio, Barclays y sus proveedores podrían no ser capaces de evitar que un ataque de denegación de servicio alcance su objetivo.

4. Trabajo en remoto (acceso remoto)	**Acceso remoto a la red de Barclays** El acceso remoto a la red de Barclays a través de la aplicación Barclays Citrix no se suministra de forma predeterminada. Para acceder a la red de Barclays desde ubicaciones no autorizadas/desde fuera de la oficina/desde casa y para cualquier acceso remoto, deben obtenerse la aprobación y autorización previas de Barclays (Dirección General de Seguridad - equipo ECAM, externalcyberassurance@barclayscorp.com). El proveedor se asegurará de que los siguientes controles estén establecidos para el acceso remoto: • El inicio de sesión de acceso remoto a la red del proveedor debe estar cifrado de forma segura 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) proporcionados por Barclays. El uso de los tokens debe ser compatible con un proceso de gestión. El proceso debe incluir la revisión y supervisión de la asignación, la pérdida/el robo, el uso y la devolución de los tokens (hard). • El proveedor debe mantener un registro actualizado y correcto de sus empleados autorizados para trabajar de forma remota con justificación empresarial para cada empleado aprobado, incluidos los subcontratistas/subencargados. • **El proveedor deberá realizar la conciliación de todos los empleados con acceso remoto trimestralmente, seguida de una indicación de sus resultados a Barclays (Dirección General de Seguridad - equipo ECAM, externalcyberassurance@barclayscorp.com).** • 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	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.

	Seguridad - equipo ECAM, externalcyberassurance@barclayscorp.com). El proveedor mantendrá registros y realizará reconciliaciones trimestrales. • No se debe permitir que dispositivos personales/BYOD accedan al entorno de Barclays ni a los 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, subcontratistas/subencargados). 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. Acceso remoto a datos de Barclays en entorno/red de proveedores El acceso remoto a los datos de Barclays que se almacenan o tratan en el entorno gestionado del proveedor no se suministra de forma predeterminada. El proveedor deberá solicitar la autorización de Barclays (Dirección General de Seguridad - equipo ECAM, externalcyberassurance@barclayscorp.com) para acceder a estos datos desde ubicaciones no autorizadas/desde fuera de la oficina/desde casa. • El acceso de inicio de sesión remoto a la red del proveedor debe encriptarse durante el tránsito de los datos y utilizar autenticación multifactor. • El proveedor mantendrá registros de las personas que han estado trabajando de forma remota y la justificación de este acceso remoto. • El proveedor realizará la reconciliación de todos los usuarios remotos trimestralmente • El proveedor desactivará las credenciales de autenticación una vez que el acceso ya no sea necesario (por ejemplo, despido de empleados, reasignación de proyectos, etc.) en el plazo de veinticuatro (24) horas. • El proveedor garantizará que el extremo empleado para conectar a distancia datos de Barclays se configura de manera segura (por ejemplo, nivel de los parches, estado de las soluciones contra el software malintencionado, etc.). • No se debe permitir que dispositivos personales/BYOD accedan a los 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).	

<table>
<tr>
<td>5. Gestión de registros de seguridad</td>
<td>El proveedor debe contar con un marco de gestión de registros y auditoría administrado, aprobado, asentado y de carácter complementario. El marco debe incluir sistemas de TI esenciales, lo que engloba aplicaciones, equipos de red, dispositivos de seguridad y servidores configurados para registrar eventos clave. El proveedor debe asegurarse de que los registros están centralizados y protegidos adecuadamente contra la manipulación o eliminación, y ha de conservarlos durante un período mínimo de 12 meses o según disponga la normativa, lo que sea mayor.
<table>
<tr><th>Categoría</th><th>Sistemas/servicio de bajo impacto</th><th>Sistemas/servicio de impacto medio</th><th>Sistemas/servicio de alto impacto</th></tr>
<tr><td>Conservación de registros</td><td>3 meses</td><td>6 meses</td><td>12 meses</td></tr>
</table>
El marco de gestión de registros de seguridad debe incluir las siguientes áreas:

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 supervisar, 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.
Los registros de eventos de muestra podrían incluir:

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 en los que se debe habilitar el registro apropiado y conforme a los procedimientos recomendados del sector, incluidos aquellos que se hayan externalizado o estén ‘en la nube’.
</td>
<td>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.</td>
</tr>
</table>

	• 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, MFA, 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 corresponda 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. • Los incidentes clave registrados incluirán aquellos que puedan afectar a la confidencialidad, la integridad y la disponibilidad de los servicios prestados a Barclays y que pueden ayudar a identificar o investigar incidentes importantes y/o vulneraciones de los derechos de acceso que se hayan producido en relación con los sistemas del proveedor. • Compruebe periódicamente que el marco sigue cumpliendo los requisitos anteriores. **Orientación para el cliente de servicios en la nube (proveedor) utilizados para prestar servicio(s) a Barclays** El cliente de servicios en la nube (CSC) debe asegurarse de que se implementan los controles de gestión de registros de seguridad adecuados para proteger el servicio de Barclays. • El cliente de servicios en la nube debe definir y documentar sus requisitos para el registro de eventos y verificar que el servicio en la nube cumple esos requisitos. • Si se delega una operación con privilegios al cliente de servicios en la nube, se debe registrar el funcionamiento y el rendimiento de dicha operación. El cliente de servicios en la nube debe determinar si las capacidades de registro proporcionadas por el proveedor de servicios en la nube son adecuadas o si debe implementar capacidades de registro adicionales por su cuenta. • El cliente de servicios en la nube debe solicitar información sobre la sincronización de relojes utilizada en los sistemas del proveedor de servicios en la nube.	

	• El cliente de servicios en la nube debe solicitar al proveedor de servicios en la nube información sobre las capacidades de supervisión de servicios disponibles para cada servicio en la nube.	
6. Defensas contra malware	De conformidad con los procedimientos recomendados del sector, el proveedor debe disponer de políticas y procedimientos establecidos, además de implementar procesos empresariales y medidas técnicas que los respalden, para impedir la ejecución de malware en todo el entorno informático. 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. La protección contra malware debe incluir, entre otras cosas, lo siguiente: • Soluciones contra el software malintencionado gestionado centralmente para controlar y defender continuamente el entorno informático de la organización. • Comprobaciones de que el software antimalware de la empresa actualiza su motor de análisis • Actualizaciones regulares de la base de datos de firmas • 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 debe implementar los controles adecuados para protegerse contra el malware y los ataques a los dispositivos móviles utilizados para los servicios de Barclays. 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.	Las soluciones contra el software malintencionado resultan esenciales para proteger los activos de información de Barclays contra el código malintencionado.
7. Estándares de configuración segura	El proveedor contará con un marco establecido para garantizar que todos los sistemas/equipos de red configurables se configuran de forma segura de acuerdo con los procedimientos recomendados del sector (como NIST, SANS, CIS). El proceso estándar de configuración debe cubrir, entre otras cosas, las siguientes áreas: • Establece políticas, procedimientos/medidas organizativas y herramientas que permiten la implementación de las normas de configuración de seguridad conforme	Los controles sobre revisiones de versiones estándar ayudan a proteger los activos de información contra accesos no autorizados. El cumplimiento respecto de los controles y las normas

	a los procedimientos recomendados del sector para todos los dispositivos de red y sistemas operativos autorizados, aplicaciones y servidores. • Realiza comprobaciones de cumplimiento regulares (anuales como mínimo) para garantizar que los incumplimientos de los estándares de seguridad básicos se rectifiquen inmediatamente. Se establecen comprobaciones y seguimientos apropiados para garantizar que se mantenga la integridad de los equipos/dispositivos. • Los sistemas y dispositivos de red están configurados para funcionar de acuerdo con principios de seguridad (por ejemplo, concepto de controles de limitación de puertos, protocolos y servicios, software no autorizado, eliminación y desactivación de cuentas de usuario innecesarias, cambio de contraseñas por defecto de las cuentas, eliminación de software innecesario, etc.). • Realiza auditorías periódicas de la configuración al menos una vez al año para garantizar que el entorno de producción real no tenga ninguna configuración no autorizada. • Garantiza que la gestión de la configuración rija los estándares de configuración segura y detecte, alerte y responda de manera efectiva a los cambios en la configuración o las desviaciones. **Orientación para el cliente de servicios en la nube (proveedor) utilizados para prestar servicio(s) a Barclays** El cliente de servicios en la nube (CSC) debe asegurarse de que se implementan los controles de configuración segura adecuados para proteger el servicio de Barclays. • Al configurar máquinas virtuales, los clientes de servicios en la nube deben asegurarse de que se han reforzado los aspectos adecuados (por ejemplo, solo los puertos, protocolos y servicios necesarios) y de que se han adoptado las medidas técnicas apropiadas (por ejemplo, antimalware, registro) para cada máquina virtual utilizada.	sobre revisiones de versiones que garanticen que los cambios se autoricen contribuye a asegurar la protección de los activos de información de Barclays.
8. Seguridad en los extremos	El proveedor debe adoptar un enfoque de gestión unificada de extremos para garantizar que los extremos empleados para acceder a la red de Barclays o a los datos o activos de información de Barclays (o para tratar estos) se refuerzan para protegerse frente a cualquier ataque malicioso. Los procedimientos recomendados del sector deberán estar establecidos y la seguridad de los dispositivos de acceso debe incluir, entre otras cosas:	De no aplicarse este control, la red de Barclays y la red del proveedor, así como sus extremos podrían ser vulnerables a los ciberataques.

	• Cifrado completo del disco duro. • 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 predeterminado, la partición de sistemas y los servicios por defecto, antivirus, etc. • No usar unidades USB para copiar información/datos de Barclays en 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 • El acceso a las impresoras debe estar deshabilitado de forma predeterminada. • El proveedor debe asegurarse de evitar la exfiltración de datos de Barclays a redes sociales, servicios de correo web y sitios que puedan almacenar información, como, entre otros, Google Drive, Dropbox o iCloud. • La compartición/transmisión de datos de Barclays debe estar deshabilitada utilizando herramientas/software de mensajería instantánea. • Detectar, detener y corregir la presencia o el uso de software no autorizado, lo que incluye el software malicioso. NOTA: Los soportes extraíbles/dispositivos portátiles deben estar deshabilitados por defecto o habilitarse solamente por razones empresariales legítimas. 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 configurarse mediante imágenes o plantillas aprobadas. Cuando se permita el acceso de extremos (ordenadores de sobremesa/portátiles) a la red de Barclays a través de la aplicación Citrix de Barclays por Internet, el proveedor instalará la herramienta de análisis del extremo (EPA) proporcionada por Barclays para validar la seguridad del extremo y la conformidad del sistema operativo. Solo los dispositivos que superen las comprobaciones del EPA podrán acceder de forma remota a la red de Barclays a través de la aplicación Citrix de Barclays. Si el proveedor no puede instalar o utilizar la herramienta EPA, deberá consultar al responsable de proveedores de Barclays. Dispositivos móviles empleados para los servicios de Barclays.	

	• El proveedor garantizará que implementa capacidades de gestión unificada de extremos (UEM) o gestión de dispositivos móviles (MDM) para controlar y gestionar de forma segura durante todo el ciclo de vida los dispositivos móviles que tengan acceso o contengan información de Barclays clasificada, reduciendo el riesgo de comprometer los datos. • El proveedor garantizará la disposición y el uso de capacidades de bloqueo y borrado a distancia para los dispositivos móviles que protejan la información en caso de que un dispositivo se robe, se pierda o se vea comprometido. • Cifrar los datos de Barclays almacenados o tratados en dispositivos móviles	

9. Prevención de las filtraciones de datos	El proveedor debe utilizar un marco efectivo aprobado por la administración para proteger los datos de Barclays contra fugas/exfiltración e incluir, entre otros, canales de filtración de datos: -
	• transferencia no autorizada de información fuera de la red interna o la red del proveedor
	  o Correo electrónico
	  o pasarela web/de internet (incluyendo almacenamiento online y webmail)
	  o DNS
	• 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 de información con terceros sin el grado adecuado de seguridad (subcontratistas, subencargados del tratamiento).
	• impresión o copia inadecuadas de información.
		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).
		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.

10. Seguridad de los datos	El proveedor debe proteger los datos de Barclays que se conserven o traten mediante una combinación de técnicas de cifrado, protección de integridad y prevención de pérdida de datos. El acceso a los datos de Barclays debe limitarse únicamente a sus empleados autorizados y protegerse frente a la contaminación, los ataques de agregación, los ataques de inferencia y las amenazas de almacenamiento, incluidas, entre otras, las amenazas procedentes de entornos de computación en la nube. Los controles de seguridad de datos deben incluir, entre otras cosas, las siguientes áreas: 1. El proveedor está obligado en todo momento a cumplir todas y cada una de las leyes de protección de datos aplicables.	

	2. Debe establecer políticas, procesos y procedimientos, apoyando los procesos empresariales y las medidas técnicas. Debe documentar y mantener los flujos de datos de la información contenida en la ubicación geográfica del servicio (física y virtual). Debe abarcar detalles relacionados con las aplicaciones y los componentes de los sistemas que forman parte del flujo de datos. 3. Debe mantener un diagrama de flujo de los datos de Barclays contenidos en ubicaciones geográficas (físicas y virtuales) en aplicaciones y componentes del sistema. 4. Debe mantener un inventario de toda la información sensible/confidencial de Barclays almacenada, tratada o transmitida por el proveedor. 5. Debe garantizar que todos los datos de Barclays estén clasificados y marcados de acuerdo con el estándar de clasificación y protección de datos aprobado por la administración. 6. Protección de datos en reposo; a. Cifrar los datos en reposo para evitar la exposición de los activos de información de Barclays. 7. Supervisión de la actividad de las bases de datos; a. Supervisar y registrar el acceso y la actividad de las bases de datos para identificar de manera rápida y efectiva la actividad maliciosa. 8. Protección de datos en uso; a. Garantizar el control de la capacidad de gestión de acceso al tratamiento de información confidencial para protegerla contra su potencial explotación. b. Uso de tecnologías de enmascaramiento y ofuscación de datos para proteger de manera efectiva los datos sensibles en uso de las revelaciones accidentales y/o la explotación maliciosa. 9. Protección de datos en tránsito; 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 cifrado de transporte o carga (mensaje o campo selectivo). Los mecanismos de encriptado de transporte incluyen, entre otros: 10. Seguridad de la capa de transporte (TLS) (de acuerdo con los procedimientos recomendados del sector para la criptografía moderna, incluyendo el uso/rechazo de protocolos y cifrados) 11. Tunelización segura (IPsec) 12. Secure Shell (SSH)	

	a. 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. 13. Copia de seguridad de los datos. a. Se aplicarán las disposiciones necesarias para garantizar que se haga una copia de seguridad de la información y que esta pueda recuperarse (en un plazo de tiempo razonable) 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. d. Si el proveedor de servicios en la nube proporciona la capacidad de copia de seguridad como parte del servicio en la nube, el cliente de servicios en la nube debe solicitar las especificaciones de esta capacidad de copia de seguridad al referido proveedor de servicios en la nube. El cliente de servicios en la nube también debe verificar que se cumplen sus requisitos de copia de seguridad. El cliente de servicios en la nube deberá encargarse de implementar capacidades de copia de seguridad cuando el proveedor de servicios en la nube no las proporcione.	
11. Seguridad del software de aplicaciones	El proveedor desarrollará aplicaciones utilizando procedimientos de programación seguros y en entornos seguros. Cuando el proveedor desarrolle aplicaciones para uso de Barclays, o bien que se utilicen para dar soporte al servicio de Barclays, deberá establecer un marco de desarrollo de software seguro para integrar la seguridad en el ciclo de vida del desarrollo de software. El proveedor debe probar y corregir las vulnerabilidades del software antes de entregarlo a Barclays. La seguridad del software de aplicaciones debe incluir, entre otras cosas, las siguientes áreas:	Los controles que protegen el desarrollo de aplicaciones contribuyen a garantizar que se mantiene la seguridad de estas durante su despliegue.

	• Establecer y adoptar estándares de codificación seguros aprobados por la administración y conforme a los procedimientos recomendados del sector para evitar vulnerabilidades e interrupciones del servicio. • 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 sector para el 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 procedimientos recomendados del sector (como OWASP para aplicaciones web). • Prohibir el uso de depósitos de códigos públicos El proveedor debe proteger las aplicaciones web desarrollando firewalls de aplicaciones web (WAF) que inspeccionen todo el tráfico a dichas aplicaciones para evitar ataques actuales y 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.	
12. Gestión de accesos lógicos (LAM)	Se restringirá el acceso a la información, teniendo debidamente en cuenta los principios relativos a su divulgación solo cuando sea necesario conocerla, al privilegio mínimo y a la separación de funciones. El responsable de activos de información se encarga de decidir el acceso que necesita cada persona.	Los controles de LAM pertinentes ayudan a garantizar la protección de los

	• 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 Estados Unidos. • 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. El proveedor debe garantizar que el acceso a los datos personales se gestiona de forma apropiada y se limita a aquellas personas que necesitan acceder para prestar el servicio. Se definirán procesos de gestión del acceso de acuerdo con los procedimientos recomendados del sector, que incluirán lo siguiente: • El proveedor debe asegurarse de que los procesos y decisiones 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. • Implementar la gestión del ciclo de vida de los derechos de acceso, incluida la identificación, la autenticación y la autorización. La gestión de los derechos de acceso debe incluir una autorización para garantizar que el proceso de concesión, modificación y retirada del acceso incluya 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.	activos de información contra un uso inadecuado. Los controles de gestión de acceso contribuyen a garantizar que solo puedan acceder a los activos de información los usuarios autorizados.

	• 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 con privilegios se deben revisar al menos cada seis (6) meses. La gestión de privilegios debe ser compatible con la gestión de acceso privilegiado (PAM) efectiva. • Las credenciales no personales (es decir, contraseñas y secretos) deben incorporarse a una herramienta adecuada que se ajuste a los mejores estándares del sector y que garantice la confidencialidad, integridad y disponibilidad (CIA) de las credenciales y las capacidades de acceso de emergencia. Cuando esto no sea posible, las credenciales deben estar protegidas para que ningún ser humano pueda utilizarlas. Cuando se requiere el uso humano de la cuenta, el acceso debe ser temporal y limitado, y las credenciales deben restablecerse después; esto se suele denominar «acceso de emergencia». El acceso de emergencia (o «break-glass») dentro de la informática es un término utilizado para describir el acto de extraer una contraseña de cuenta del sistema para que la utilice un humano. Generalmente se utiliza para cuentas de sistema de nivel superior, como root para Unix o SYS/SA para bases de datos. Estas cuentas gozan de privilegios de alto nivel y no están individualizadas en sí mismas para un usuario específico, por lo que el acceso de emergencia se limita por la duración de la contraseña, con el objetivo de controlar y reducir el uso de la cuenta a lo que es necesario. • Controles de empleados que cambian de puesto - Se debe revocar el acceso para asegurarse de que no esté disponible a partir del cierre/fin de movimiento/día de transferencia. • Controles de empleados que dejan la empresa - Se ha de revocar todo acceso lógico utilizado para acceder a los recursos de información de Barclays o prestar servicios a Barclays desde la fecha de salida/el último día laborable con el proveedor.	

	• Autenticación - Deben aplicarse controles de la longitud y complejidad apropiados de las contraseñas, historial de 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 (y se mantendrán los correspondientes registros). • 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 contraseñas de 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 o un número máximo más bajo si así lo dictan los procedimientos recomendados del sector. **Orientación para el cliente de servicios en la nube (proveedor) utilizados para prestar servicio(s) a Barclays** El cliente de servicios en la nube (CSC) debe asegurarse de que se implementan los controles de gestión de acceso lógico adecuados para proteger el servicio de Barclays. • El cliente de servicios en la nube debe utilizar suficientes técnicas de autenticación (por ejemplo, autenticación multifactor) para identificar a los administradores del servicio en la nube contratado y sus capacidades administrativas del servicio en la nube según los riesgos identificados. • El cliente de servicios en la nube debe asegurarse de que el acceso a la información en el servicio en la nube se puede restringir de acuerdo con su política de control de acceso y de que se aplican dichas restricciones. Esto incluye la restricción del acceso a los servicios en la nube, las funciones del servicio en la nube y los datos de los clientes del servicio en la nube que se mantienen en este. • Cuando se permita el uso de programas de utilidad, el cliente de servicios en la nube debe identificar estos programas que se utilizarán en su entorno de computación en la nube y asegurarse de que no interfieren con los controles del servicio en la nube.	
13. Gestión de las vulnerabilidades	El proveedor debe poner en marcha un programa eficaz de gestión de vulnerabilidades mediante políticas y procedimientos establecidos, procesos/medidas organizativas que los respalden, y medidas técnicas implementadas para la supervisión efectiva, la detección puntual y la reparación de las vulnerabilidades dentro de aplicaciones gestionadas o	De no aplicarse este control, los atacantes podrían aprovechar las vulnerabilidades de los

<table>
<tr>
<td></td>
<td>
propiedad del proveedor, redes de infraestructuras y componentes de sistema para garantizar la eficiencia de los controles de seguridad implementados.

La gestión de vulnerabilidades debe incluir, entre otras cosas, las siguientes áreas:

Funciones, responsabilidades y obligaciones definidas para la supervisión, presentación de información, apelación y reparación.
Herramientas e infraestructura apropiadas para el análisis de vulnerabilidades.
El proveedor de servicios llevará a cabo análisis de vulnerabilidades de manera rutinaria (con la frecuencia que dicten los procedimientos recomendados del sector) 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.
Garantizar que las vulnerabilidades se resuelven de manera efectiva a través de actividades de reparación y gestión de parches robustas para reducir el riesgo de explotación de vulnerabilidad (la reparación se producirá de forma oportuna y de conformidad con los procedimientos recomendados del sector o el programa de gestión de parches).
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.
Comparar regularmente los resultados de análisis consecutivos de vulnerabilidades para comprobar que estas se han remediado de forma puntual.

Para los servicios del proveedor relacionados con la infraestructura de alojamiento/las aplicaciones web en nombre de Barclays (incluidos los terceros de alto riesgo comunicados)

El proveedor debe notificar a Barclays de inmediato si se identifica alguna vulnerabilidad crítica/alta.
El proveedor debe reparar las vulnerabilidades de conformidad con la tabla siguiente o tal y como acuerde con Barclays (Dirección General de Seguridad - equipo ECAM).

<table>
<tr><th>Prioridad</th><th>Calificación</th><th>Días de cierre (máximo)</th></tr>
<tr><td>P1</td><td>Crítico</td><td>15</td></tr>
<tr><td>P2</td><td>Alto</td><td>30</td></tr>
</table>
</td>
<td>sistemas para realizar ciberataques, lo que podría provocar daños en el marco jurídico o para la reputación.</td>
</tr>
</table>

	<table><tr><td>P3</td><td>Medio</td><td>60</td></tr><tr><td>P4</td><td>Bajo</td><td>180</td></tr><tr><td>P5</td><td>Informativo</td><td>360</td></tr></table> Todos los problemas y las vulnerabilidades de seguridad que pudieran afectar de forma importante a la infraestructura de alojamiento/las 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, externalcyberassurance@barclayscorp.com). **Orientación para el cliente de servicios en la nube (proveedor) utilizados para prestar servicio(s) a Barclays** El cliente de servicios en la nube (CSC) debe asegurarse de que se implementan los controles de gestión de vulnerabilidades adecuados para proteger el servicio de Barclays. • El cliente de servicios en la nube debe solicitar al proveedor de servicios en la nube información sobre la gestión de vulnerabilidades técnicas que puedan afectar a los servicios en la nube que se prestan. El cliente de servicios en la nube debe identificar las vulnerabilidades técnicas que deberá gestionar, definiendo claramente un proceso para su gestión.	
14. Gestión de revisiones	El proveedor debe disponer de un programa de gestión de parches respaldado por políticas y procedimientos establecidos, procesos empresariales/medidas organizativas que los respalden, y medidas técnicas implementadas para supervisar/controlar la necesidad de parches e implementar parches de seguridad para gestionar todo el entorno/estado del proveedor. El proveedor debe asegurarse de que los servidores, los dispositivos de red, las aplicaciones y los dispositivos de extremos se mantienen actualizados con los parches de seguridad más recientes y de acuerdo con los procedimientos recomendados del sector, asegurándose de que: • El proveedor se cerciorará de 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	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.

<table>
<tr>
<td></td>
<td>del servicio con el parche se comprueba después de la actividad de parcheado. Si un sistema no puede parchearse, desplegar contramedidas 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 respaldar los futuros requisitos de auditoría, investigación, solución de problemas y análisis.
• El proveedor se asegurará de que los parches se reflejen en entornos de producción y recuperación de desastres (DR).</td>
<td></td>
</tr>
<tr>
<td>15. Simulación de amenazas/ Pruebas de penetración/ Evaluación de la seguridad informática</td>
<td>El proveedor contratará a un proveedor de seguridad cualificado e independiente para realizar una simulación de amenazas o una evaluación de la seguridad 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.

Este proceso 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.

Para los servicios del proveedor relacionados con la infraestructura de alojamiento/las aplicaciones web en nombre de Barclays (incluidos los terceros comunicados de alto riesgo)
• 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.
• Todos los problemas cuyo riesgo se haya decidido aceptar se comunicarán a Barclays para acordarlos con el banco (Dirección General de Seguridad - equipo ECAM).
• El proveedor deberá compartir anualmente el informe de evaluación de la seguridad más reciente con Barclays (Dirección General de Seguridad - equipo ECAM, externalcyberassurance@barclayscorp.com).
• El proveedor debe notificar a Barclays de inmediato si se identifica alguna vulnerabilidad crítica/alta.
• El proveedor debe reparar las vulnerabilidades de conformidad con la tabla siguiente o tal y como acuerde con Barclays (Dirección General de Seguridad - equipo ECAM).

<table>
<tr><th>Prioridad</th><th>Calificación</th><th>Días de cierre (máximo)</th></tr>
</table>
</td>
<td>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.

Podría revelarse información de Barclays o producirse una pérdida de servicio. Esto tendría como consecuencia daños en el marco jurídico o para la reputación.</td>
</tr>
</table>

<table>
<tr><td></td><td></td><td><table>
<tr><td>P1</td><td>Crítico</td><td>15</td></tr>
<tr><td>P2</td><td>Alto</td><td>30</td></tr>
<tr><td>P3</td><td>Medio</td><td>60</td></tr>
<tr><td>P4</td><td>Bajo</td><td>180</td></tr>
<tr><td>P5</td><td>Informativo</td><td>360</td></tr>
</table></td><td></td><td></td></tr>
<tr><td>16. Criptografía</td><td colspan="3">
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. El proveedor debe retirar sus claves una vez finalizado el período de servicio o establecer un programa de rotación de claves obligatorio.
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 pseudoaletorios criptográficamente seguro (CSPRNG) en forma de software.

El proveedor deberá garantizar que todas las claves se sometan a una vida de criptoperiodo definida y limitada tras la cual se sustituyan o desactiven. Esto también debe ser acorde a los requisitos del National Institute of Standards and Technology (NIST) y a los procedimientos recomendados del sector aplicables

</td><td>Los algoritmos y la protección del cifrado pertinentes y actualizados garantizan una protección continua para los activos de información de Barclays.</td></tr>
</table>

	• Protección del almacenamiento de claves - El proveedor deberá garantizar que solo existan claves criptográficas secretas/privadas en las siguientes formas: o En el límite criptográfico de un dispositivo/módulo con hardware certificado. o En forma encriptada bajo otra clave establecida o derivada de una contraseña. o En partes de componentes divididos entre grupos de custodia diferentes. o 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: o Claves para servicios regulados donde los HSM sean obligatorios. o Certificados que representen a Barclays de CA públicos. o Certificados raíz, de emisión, OCSP y RA (autoridad de registro) empleados para emitir certificados que protejan los servicios de Barclays. o Claves que protejan depósitos agregados almacenados de claves, credenciales de acreditación o datos PII. • 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: o Equipo de soporte informático o Activos relacionados o 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. o 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 los procedimientos recomendados del sector.	
17. Computación en la nube	El proveedor (cliente de servicios en la nube o CSC) debe asegurarse de que el servicio en la nube utilizado para la prestación del servicio o los servicios a Barclays cuente con un marco de controles de seguridad bien definido para cumplir los objetivos de disponibilidad, integridad y confidencialidad, y garantizar la existencia de controles de seguridad, así como su funcionamiento eficaz, con el fin de proteger el servicio o servicios de Barclays. El proveedor debe contar con la certificación ISO/IEC 27017 o 27001 o SOC 2 o un marco de seguridad en la nube similar o conforme a los procedimientos recomendados del sector, así como implementar medidas para garantizar que todo uso de tecnología en la nube resulte seguro. El proveedor debe asegurarse de que el proveedor del servicio en la nube cuente con una certificación conforme a los procedimientos recomendados del sector, incluyendo unos	Si este control de la nube no se implementa, la seguridad de los datos de Barclays podría verse afectada. Esto tendría como consecuencia daños en el marco jurídico o para la reputación.

	controles apropiados equivalentes a la versión más reciente de la Matriz de Controles de Seguridad en la Nube (CCM) de la Cloud Security Alliance. El proveedor debe solicitar pruebas documentadas de que la implementación de controles y directrices de seguridad de la información para el servicio en la nube concuerda con cualquier reivindicación realizada por el proveedor de servicios en la nube. El proveedor es responsable de garantizar los controles de seguridad de los datos relacionados con los activos de información/datos de Barclays, incluyendo los datos personales en la nube, y el proveedor del servicio en la nube es responsable de la seguridad del entorno de computación en la nube. El proveedor sigue siendo responsable de la configuración y supervisión de los controles de seguridad implementados para ofrecer protección frente a incidentes de seguridad, incluyendo violaciones de la seguridad de los datos. El proveedor debe implementar medidas de seguridad en todos los aspectos del servicio que se va a prestar, incluyendo el modelo de responsabilidad compartida en la nube, de forma que se proteja la confidencialidad, integridad, disponibilidad y accesibilidad, minimizando la oportunidad de que personas no autorizadas logren acceder a información de Barclays y a los servicios utilizados por Barclays. Los controles de seguridad en la nube deben incluir, entre otros, los siguientes dominios para modelos de despliegue (IaaS/PaaS/SaaS): • Mecanismos de gobernanza y rendición de cuentas • Identidad y gestión de acceso • Seguridad de la red (incluyendo conectividad) • Seguridad de datos (en tránsito/reposo/almacenados) • Eliminación/depuración de datos segura • Criptografía, encriptado y gestión de claves - CEK • Registro y monitorización • Virtualización • Segregación de servicios Los activos de información/datos, incluyendo datos personales de Barclays almacenados en la nube como parte del servicio prestado a Barclays deben ser aprobados por Barclays (Dirección General de Seguridad - equipo ECAM). El proveedor proporcionará a Barclays las ubicaciones de las zonas de datos normales y de conmutación automática en las que se almacenarán o conservarán los datos de Barclays.	

	El proveedor debe confirmar las funciones y responsabilidades de seguridad de la información relacionadas con el servicio en la nube, según se describe en el acuerdo de servicio. Estas pueden incluir los siguientes procesos: • Protección contra malware; • Copia de seguridad; • Controles criptográficos; • Gestión de las vulnerabilidades; • Gestión de incidentes; • Pruebas de seguridad; • Auditorías; • Recopilación, mantenimiento y protección de pruebas, incluidos registros y registros de auditoría; • Protección de la información tras la finalización del contrato de servicio; • Identidad y gestión de acceso.	
18. Espacio dedicado al banco (EDB)	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). Los diferentes tipos de EDB son: 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. Nivel 2 (clase empresarial) - Toda la infraestructura informática es gestionada por el **proveedor** y se conecta a las pasarelas de extranet de **Barclays** - los dispositivos de LAN, WAN y Desktop son propiedad y están gestionados por el proveedor. 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.	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/incidentes de seguridad.
18.1 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.	
18.2 EDB - Control del acceso físico	• 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 (y se mantendrán los correspondientes registros). • 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: Para un empleado autorizado: o Tarjeta de identificación con foto siempre visible o Implementación de lectores de tarjeta por proximidad o Habilitación y supervisión de un mecanismo antirretorno • El proveedor contará con procesos y procedimientos para controlar y monitorizar a las personas externas, incluyendo subcontratistas y subencargados con acceso físico a las áreas EDB para realizar tareas de mantenimiento y limpieza.
18.3 EDB - Videovigilancia	• 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. 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.
18.4 EDB - Acceso a la red de Barclays y tokens de autenticación de Barclays	• 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, 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).

	• 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. Consultar control - 4. Trabajo en remoto (acceso remoto)
18.5 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).
18.6 EDB - Seguridad de la red	• 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; o Garantizar que el registro y la monitorización estén habilitados. • La red EDB debe ser monitorizada y solo deben permitirse dispositivos autorizados por medio de controles de acceso a la red pertinentes. Consultar control - 2. Seguridad de la red y límites
18.7 EDB - Red inalámbrica	Debe desactivarse la red inalámbrica para la provisión de red EDB para los servicios de Barclays.
18.8 EDB - Seguridad de los extremos	Deben configurarse equipos de escritorio seguros según los procedimientos recomendados del sector para los ordenadores de la red EDB. Los procedimientos recomendados del sector deberán estar establecidos y la seguridad de los dispositivos de acceso de la red EDB debe incluir, entre otras cosas: • Cifrado completo del disco duro. • 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. • No usar unidades USB para copiar información/datos de Barclays en soportes externos. • Actualización con las últimas firmas antimalware 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 • El acceso a las impresoras debe estar deshabilitado de forma predeterminada. • La compartición/transmisión de datos de Barclays debe estar deshabilitada utilizando herramientas/software de mensajería instantánea; • Detectar, detener y corregir la presencia o el uso de software no autorizado, lo que incluye el software malicioso. Consultar control - 8. Seguridad en los extremos	

18.9 EDB - Correo electrónico e Internet	• La conexión de red debe configurarse de forma segura para restringir el correo electrónico y la actividad de Internet en la red del EDB.
	• 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:
	  • 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.	

18.10 EDB - BYOD/Dispositivo personal	Los dispositivos personales/ BYOD no deben tener permitido el acceso al entorno y/o los datos de Barclays	
Derecho de inspección	El proveedor debe permitir que Barclays, previa notificación por escrito con una antelación mínima de diez (10) días hábiles, pueda llevar a cabo una revisión de seguridad de cualquier instalación o tecnología utilizada por el proveedor o sus subcontratistas 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.	Si no aceptan, los proveedores no podrán garantizar plenamente que se cumplen estas obligaciones de seguridad.

	Todo incumplimiento de controles identificado por Barclays durante una inspección debe someterse a una evaluación de riesgos por parte de Barclays y este especificará un plazo para que se corrija. El proveedor se encargará entonces de implantar cualquier medida correctiva que sea necesaria en el plazo establecido. El proveedor debe prestar a Barclays toda la asistencia que solicite en términos razonables en relación con cualquier inspección y documentación presentada durante una inspección que deba completarse y devolverse a Barclays.	

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	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 (EDB) significa cualquier instalación propiedad de un miembro del grupo del proveedor o de cualquier subcontratista o subencargado, o bajo su control, que se dedique exclusivamente a Barclays y desde la que se presten o realicen los servicios.
Procedimientos recomendados del sector	Utilizar las mejores y más actuales prácticas, procesos, estándares y certificaciones del mercado y aplicar el grado de competencia y cuidado que cabría razonablemente esperar de una organización altamente cualificada, experimentada y líder del mercado dedicada a la prestación de servicios iguales o similares a los servicios prestados a Barclays.
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.
Ciberseguridad	La aplicación de tecnologías, procesos, controles y medidas organizativas para proteger sistemas informáticos, redes, programas, dispositivos y datos frente a ataques digitales que pueden implicar, por ejemplo, revelaciones no autorizadas, destrucción, pérdida, alteración, robo o daños de hardware, software o datos.
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 (MFA)	Autenticación que requiere 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).
Información personal	Cualquier información relacionada con una persona física identificada o identificable («el interesado»); una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en concreto por referencia a un identificador como el nombre, un número de identificación, datos de localización, un identificador online o conforme a uno o más factores específicos de la identidad física, psicológica, genética, mental, económica, cultural o social de dicha persona física.
Acceso privilegiado	Asignación de accesos, permisos o capacidades especiales a un usuario, proceso u ordenador (por encima del estándar).
Cuenta privilegiada	Una cuenta que ofrece un mayor nivel de control sobre un sistema informático concreto. Estas cuentas se suelen utilizar para el 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.
Acceso remoto	Tecnología y técnicas utilizadas para permitir a usuarios autorizados el acceso a las redes y los sistemas de una organización desde una ubicación remota.
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.
Incidente de seguridad	Los incidentes de seguridad se definen como eventos que incluyen, entre otras cosas: • 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.
Máquina virtual:	Entorno completo que admite la ejecución de software invitado. NOTA: Una máquina virtual es un encapsulamiento completo del hardware virtual, los discos virtuales y los metadatos asociados. Las máquinas virtuales permiten la multiplexación de la máquina física subyacente a través de una capa de software denominada hipervisor.

Secreto bancario

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

Título / Área de control	Descripción del control	Por qué es importante
1. Funciones y responsabilidades	El proveedor definirá y comunicará las funciones y las responsabilidades en relación con el tratamiento de datos que identifiquen a los clientes (en adelante CID). El proveedor revisará los documentos en los que se señalen las funciones y responsabilidades en relación con los CID cuando se introduzca algún cambio importante en la actividad o el modelo operativo (o el negocio) del proveedor, o al menos una vez al año, y los distribuirá en la jurisdicción con secreto bancario pertinente. Las funciones principales incluirán a un alto ejecutivo que será responsable de proteger y supervisar todas las actividades relacionadas con los CID (consúltese la definición de CID en el Apéndice A) El número de empleados con acceso a los CID debe mantenerse a un nivel mínimo basado en el principio de la necesidad de conocer.	Una definición clara de las funciones y las responsabilidades contribuye a la implantación del Anexo sobre las obligaciones de control de proveedores externos.

2. Notificación de violaciones de la seguridad de los CID	Existirán controles, procesos y procedimientos documentados que garanticen la notificación y la gestión de cualquier violación de la seguridad que repercuta en los CID. El proveedor responderá a toda vulneración de los requisitos de gestión (definidos en la tabla B2) y se comunicará a la 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, y someter a pruebas periódicas, los incidentes que afecten a los CID. El proveedor se asegurará de contar con un plan de reparación (acción, persona responsable y fecha de entrega) donde se incluyan las medidas correctivas a emprender en caso de que se produzca un incidente. Este plan se pondrá en conocimiento de la jurisdicción con secreto bancario correspondiente para su aprobación. El proveedor deberá emprender medidas de reparación de forma oportuna. 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.	Un proceso de respuesta en caso de incidentes contribuye a garantizar que estos se contengan rápidamente y a evitar tener que remitirlos a instancias superiores. Toda vulneración de la seguridad que repercuta en los CID podría causar importantes daños a la reputación de Barclays y podría derivar en la imposición de multas y en la pérdida de la licencia bancaria en Suiza y Mónaco.

3. Educación y conocimiento	Los empleados del proveedor que tengan acceso a los CID o los gestionen deberán realizar un curso de formación* que incluya los requisitos de secreto bancario de los CID tras cualquier cambio en la normativa, o al menos una vez al año. El proveedor se asegurará de que todos sus empleados nuevos (que tengan acceso a los CID o los gestionen), en un plazo razonable (aproximadamente 3 meses) realicen un curso de formación que garantice que entienden sus responsabilidades con respecto a los CID. El proveedor llevará un seguimiento de los empleados que han realizado el curso de formación. * las jurisdicciones con secreto bancario ofrecerán información sobre el contenido previsto para los cursos de formación.	Todos los demás controles de este anexo se basan en la educación y el conocimiento.
4. Plan de etiquetado de la información	*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. Los requisitos de gestión de los CID se incluyen en la Tabla E2 del Apéndice E. * «*cuando proceda*» *se refiere a las ventajas del etiquetado frente a los riesgos asociados. Por ejemplo, sería inapropiado etiquetar un documento si ello infringe los requisitos normativos para evitar su manipulación.*	Resulta esencial disponer de un inventario completo y exacto de activos de información para garantizar la implantación de los controles pertinentes.
5. Almacenamiento externo/computación en la nube	Todo uso de computación en la nube o almacenamiento externo de CID (en servidores situados fuera de la jurisdicción con secreto bancario o fuera de la infraestructura del proveedor) que se realice como parte del servicio a dicha jurisdicción debe ser aprobado por los equipos locales pertinentes (incluida la Dirección General de Seguridad, Cumplimiento y Asesoría Jurídica); y se implantarán controles con arreglo a las leyes y reglamentos aplicables de la correspondiente jurisdicción con secreto bancario para proteger información de los CID con deficiencias con respecto al perfil de riesgo elevado que presentan.	Si este principio no se implementa correctamente, la seguridad de los datos de los clientes (CID) protegidos podría verse afectada. Esto tendría como consecuencia una sanción legal o normativa, o daños en la reputación.

Apéndice B: 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 C: DATOS QUE IDENTIFICAN AL CLIENTE - DEFINICIÓN

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/cliente potencial	Número de contenedor / ID de contenedor	Lugar 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	Título	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	
			Lugar 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

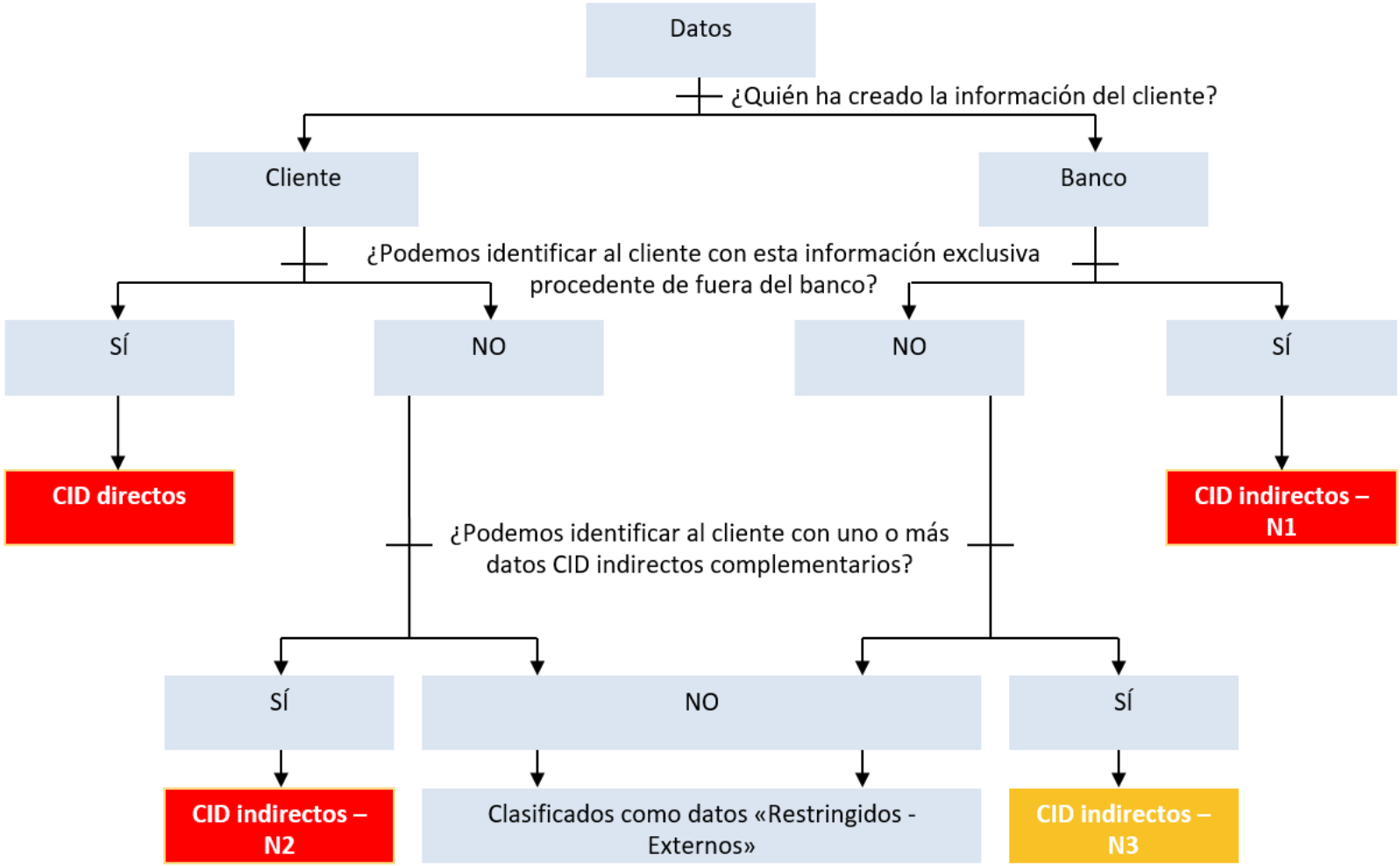
   (DIDD) = Vulneración del secreto bancario

2. ID de contenedor

   (N1CIDI) = Vulneración del secreto bancario

3. Situación patrimonial + Nacionalidad

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



Apéndice D: Plan del etiquetado de la información de Barclays

Tabla D1: Plan del etiquetado de la información de Barclays

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

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

Etiqueta	Definición	Ejemplos
Secreta	Se clasificará la información como «secreta» si su divulgación no autorizada causara un perjuicio a Barclays, valorado de acuerdo con el marco de gestión de riesgos empresariales (ERMF) como «crítico» (financiero o no financiero).	• Información sobre posibles fusiones o adquisiciones. • Información de planificación estratégica: empresarial y organizativa.

	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.	• Determinada configuración de la seguridad de la información. • Determinados resultados de auditorías e informes. • Actas del Comité Ejecutivo. • Datos de autenticación o identificación y verificación: cliente y compañero. • Volúmenes generales de información de los titulares de tarjetas. • Pronósticos de beneficios o resultados financieros anuales (antes de hacerse públicos). • Cualquier elemento cubierto por un Acuerdo de confidencialidad formal.
Restringida – Interna	La información deberá clasificarse como Restringida – Interna si los destinatarios previstos son solo empleados de Barclays autenticados y Proveedores de servicios gestionados de Barclays con un contrato en vigor y restringida a un público específico. La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero). Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla.	• Estrategias y presupuestos. • Evaluaciones del personal. • Remuneración de los empleados e información personal. • Evaluaciones de la vulnerabilidad. • Resultados de auditorías e informes.
Restringida – Externa	La información deberá clasificarse como Restringida – Externa si los destinatarios previstos son empleados autenticados de Barclays y Proveedores de servicios gestionados de Barclays con un contrato en vigor y que esté restringida a un público específico o partes externas autorizadas por el responsable de la información.	• Planes de nuevos productos. • Contratos de clientes. • Contratos legales. • Información de clientes individuales o de escaso volumen que deba enviarse externamente. • Comunicaciones de clientes.

	La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero). Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla.	• Materiales de oferta de nuevas emisiones (por ejemplo, folleto, nota sobre la oferta). • Documento de investigación definitivo. • Información no pública de carácter material no perteneciente a Barclays (MNPI). • Todos los informes de investigación. • Determinados materiales de marketing. • Comentario de marketing.
Sin restricción	Información destinada a su distribución general o que no causaría ninguna repercusión en la organización si se distribuyera.	• Material de marketing. • Publicaciones. • Anuncios públicos. • Anuncios de ofertas de trabajo. • Información sin impacto para Barclays.

Tabla D2: Plan del etiquetado de la información – Requisitos de tratamiento

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

Fase del ciclo de vida	Requisitos del secreto bancario
Creación y etiquetado	De acuerdo con «Restringida-Externa» y: • A los activos se les asignará un responsable de CID.

Almacenamiento	De acuerdo con «Restringida-Externa» y: • Los activos se guardarán exclusivamente en soportes extraíbles durante el tiempo exigido explícitamente por una necesidad empresarial concreta, reguladores o auditores externos. • No deben guardarse en dispositivos/soportes portátiles grandes volúmenes de activos de información de secreto bancario. Para obtener más información, póngase en contacto con el equipo de ciberseguridad y seguridad de la información (en adelante CIS). • Los activos (físicos o electrónicos) no se almacenarán en lugares donde personas no autorizadas puedan verlos o acceder a ellos, de acuerdo con el principio basado en la necesidad de conocerlos y la necesidad de tenerlos. • Se emplearán prácticas seguras en el lugar de trabajo, como el bloqueo de los equipos de sobremesa y la política de no dejar nada sobre la mesa de trabajo, a fin de proteger los activos (ya sean en formato electrónico o físico). • Los activos de información en soportes extraíbles solo se utilizarán para el almacenamiento durante el plazo exigido explícitamente y se guardarán y pondrán bajo llave cuando no se estén usando. • Las transferencias de datos ocasionales a soportes o dispositivos portátiles requieren la aprobación del responsable de los datos, el departamento de cumplimiento y el CIS.
Acceso y uso	De acuerdo con «Restringida-Externa» y: • No se eliminarán los activos ni se verán fuera de las instalaciones (de Barclays) sin una autorización formal del responsable del CID (o su delegado). • No se eliminarán los activos ni se verán fuera de la jurisdicción de reserva del cliente sin una autorización formal del responsable del CID (o su delegado) y del cliente (renuncia / Poder notarial limitado). • Se seguirán prácticas seguras de trabajo en emplazamientos remotos, para garantizar que nadie pueda espiar el trabajo por encima del hombro cuando se saquen de las instalaciones activos físicos.
	• Garantizar que las personas no autorizadas no puedan observar ni acceder a activos electrónicos que contengan CID utilizando un acceso restringido a aplicaciones empresariales.
Uso compartido	De acuerdo con «Restringida-Externa» y: • Los activos solo deben distribuirse de acuerdo con el «principio basado en la necesidad de conocerlos» Y dentro del personal y los sistemas de información de la jurisdicción con secreto bancario de origen. • La transferencia ocasional de activos en soportes extraíbles requiere la aprobación del responsable del activo de información y del CIS. • Se cifrarán las comunicaciones electrónicas en tránsito. • Los activos (en papel) enviados por correo deberán entregarse utilizando un servicio que exija un acuse de recibo. • Los activos solo deben distribuirse de acuerdo con el «principio basado en la necesidad de conocerlos».

Archivo y eliminación	De acuerdo con «Restringida-Externa»

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

Fase del ciclo de vida	Restringida – Interna	Restringida – Externa	Secreta
Creación e introducción	• A los activos se les asignará un responsable del activo de información.	• A los activos se les asignará un responsable del activo de información.	• A los activos se les asignará un responsable del activo de información.
Almacenamiento	• Los activos (físicos o electrónicos) no se almacenarán en áreas públicas (incluidas las áreas públicas de las instalaciones a las que puedan acceder visitantes sin supervisión). • No se dejará información en áreas públicas en las instalaciones a las que puedan acceder visitantes sin supervisión.	• Los activos (físicos o electrónicos) no se almacenarán en lugares donde personas no autorizadas puedan verlos o acceder a ellos. • Los activos almacenados en formato electrónico se protegerán mediante cifrado, o con controles de compensación apropiados, si hubiera un riesgo importante de que personal no autorizado pudiera acceder a ellos.	• Los activos (físicos o electrónicos) no se almacenarán en lugares donde personas no autorizadas puedan verlos o acceder a ellos. • Los activos almacenados en formato electrónico se protegerán mediante cifrado, o con controles de compensación apropiados, si hubiera un riesgo importante de que personal no autorizado pudiera acceder a ellos.

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

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

			• Los activos electrónicos se cifrarán utilizando un mecanismo de protección criptográfico cuando transiten fuera de la red interna. • Se mantendrá la cadena de custodia de los activos electrónicos.
Archivo y eliminación	• Los activos en papel se eliminarán utilizando un servicio de gestión de residuos confidencial. • Las copias de los activos electrónicos también se eliminarán de las «papeleras de reciclaje» del sistema de manera oportuna.	• Los activos en papel se eliminarán utilizando un servicio de gestión de residuos confidencial. • Las copias de los activos electrónicos también se eliminarán de las «papeleras de reciclaje» del sistema de manera oportuna.	• Los activos en papel se eliminarán utilizando un servicio de gestión de residuos confidencial. • Las copias de los activos electrónicos también se eliminarán de las «papeleras de reciclaje» del sistema de manera oportuna. • Los soportes en los que se hayan almacenado activos electrónicos «secretos» se limpiarán adecuadamente antes o durante la eliminación.