# External Supplier Control Obligation

# Seguridad de la información y ciberseguridad (ICS)

Versión 11.0 con fecha de octubre de 2021

| Título / Área de control | Descripción del control | Por qué es importante |
|---|---|---|
| 1. Marco y gobernanza en materia de seguridad de la información o ciberseguridad | El proveedor deberá contar un marco estándar de la industria establecido y coherentes para la gobernanza en materia de seguridad de la información y ciberseguridad de conformidad con los procedimientos recomendados del sector (entre los programas recomendados del sector actuales se incluyen NIST, ISO/IEC 27001, ITIL, COBIT), así como cualquier requisito del sector aplicable. Esto permitirá al proveedor garantizar la existencia de salvaguardas o contramedidas de su proceso, tecnología y entorno físico. El programa de gobernanza de la información bien estructurado y aplicable al conjunto de la empresa debe garantizar que los conceptos básicos de disponibilidad, integridad y confidencialidad estén respaldados por unos controles adecuados diseñados para mitigar o reducir los riesgos de pérdida, disrupción o corrupción de la información, y el proveedor deberá garantizar la existencia de los controles exigidos por Barclays, así como su funcionamiento eficaz, con el fin de proteger el servicio o servicios de Barclays.<br><br>El marco de gobernanza de la seguridad debe desarrollarse, documentarse, aprobarse y aplicarse, lo que incluye medidas administrativas, organizativas técnicas y físicas para proteger los activos y los datos de la pérdida, uso indebido, acceso, revelación, alteración y destrucción no autorizados.<br><br>El programa de seguridad debe incluir, entre otras cosas, las siguientes áreas:<br>• Una política, procedimientos y un programa de estándares que cree, aplique y mida de manera continuada y efectiva la efectividad de la aplicación de los estándares y políticas de seguridad de la información y ciberseguridad.<br>• Un programa de seguridad completo con una estructura de liderazgo clara, mecanismos de apelación y supervisión ejecutiva para crear una cultura de la responsabilidad y conocimiento en materia de seguridad.<br>• Políticas, procedimientos y procesos aprobados y comunicados en toda la organización.<br>• Garantizar que las políticas y procedimientos/estándares de seguridad de la información y ciberseguridad se revisen de manera rutinaria (como mínimo cada año o cuando se produzcan cambios sustanciales) y que se adapten en función de las prácticas de ciberseguridad actuales y de la evolución de las amenazas. | De no aplicarse este principio, Barclays o sus proveedores podrían no disponer de (y no ser capaces de demostrar) una supervisión adecuada de la seguridad de la información o la ciberseguridad. Un marco de gobernanza de la seguridad fuerte establece el tono de seguridad para toda la organización. |

| | | |
|---|---|---|
| | • El proveedor garantizará que exista una responsabilidad individual relativa a los sistemas de seguridad y la información procurando que haya la responsabilidad apropiada de los entornos empresariales críticos, la información y los sistemas de seguridad, y que se asigne a personas capacitadas.<br>• El proveedor coordinará y alineará las funciones y responsabilidades del personal, aplicando, gestionando y supervisando la efectividad de la estrategia y el marco de seguridad con socios internos y externos.<br>• El proveedor deberá implementar un marco de control e infraestructuras seguro para proteger la organización frente a cualquier amenaza (incluyendo la ciberseguridad).<br>• Deben llevarse a cabo evaluaciones y revisiones expertas independientes como mínimo cada año para garantizar que la organización aborde las no conformidades de las políticas, estándares, procedimientos y obligaciones de cumplimiento establecidos.<br>**El proveedor garantizará que Barclays sea notificado (por escrito) en cuanto se pueda hacer legalmente si es objeto de una fusión, adquisición o cualquier otro cambio de propiedad.** | |
| 2. Gestión de los riesgos relacionados con la seguridad | El proveedor establecerá un programa de gestión de riesgos de seguridad que evalúe, mitigue y controle de manera efectiva la evolución de los riesgos de seguridad en todo el entorno controlado del proveedor.<br>El programa de gestión de riesgos debe incluir, entre otras cosas, las siguientes áreas:<br>• El proveedor debe contar con un marco de gestión de riesgos de seguridad aprobado por la autoridad competente correspondiente (por ejemplo, el Consejo o uno de sus comités). Este debería incorporarse a la estrategia de negocio general y el marco de gestión de riesgos.<br>• Deben llevarse a cabo evaluaciones de riesgos formales alineadas con el marco de riesgos como mínimo anualmente o a intervalos planificados, o activarse cuando se produzcan determinados acontecimientos, por ejemplo, como respuesta a un incidente o las lecciones aprendidas asociadas (y junto con cualquier cambio en los sistemas de información) para determinar la probabilidad y el impacto de todos los riesgos identificados empleando métodos cualitativos y cuantitativos. La probabilidad y el impacto asociados a los riesgos inherentes y residuales se determinarán de forma independiente, | Si este control no se implementa, es posible que los proveedores no puedan demostrar la implementación de medidas apropiadas para gestionar los riesgos de seguridad. |

| | | |
|---|---|---|
| | teniendo en cuenta todas las categorías de riesgo (por ejemplo, resultados de auditoría, análisis de amenazas y vulnerabilidades y cumplimiento normativo).<br>• Selección de opciones apropiadas de tratamiento de los riesgos de seguridad que tengan en cuenta los resultados de las evaluaciones de riesgos.<br>• Formulación de un plan de tratamiento de los riesgos de seguridad y los criterios de aceptación de riesgos a través de personas debidamente cualificadas y responsables. Estos criterios deberían incluir, por ejemplo, la sensibilidad de estos datos y su nivel de criticidad para la empresa.<br>• El proveedor garantizará que los riesgos identificados se minimicen o eliminen en el entorno a través de la priorización del riesgo y la aplicación de medidas de protección.<br>• Los riesgos deben mitigarse a un nivel aceptable. Deben establecerse y documentarse niveles de aceptación basados en criterios de riesgos de acuerdo con marcos temporales de resolución aceptables y con la aprobación de las partes interesadas.<br>• Las evaluaciones de riesgos asociadas a los requisitos de gobernanza de los datos deben tener en cuenta los siguientes elementos:<br>o Clasificación de datos y protección frente a uso no autorizado, revelación, acceso, pérdida, destrucción, alteración y falsificación.<br>o Conocimiento de los lugares en los que se almacenan y transmiten datos sensibles entre aplicaciones, bases de datos, servidores e infraestructuras de redes.<br>o Cumplimiento de los períodos de retención definidos y requisitos de eliminación al final de la vida útil.<br>• El proveedor llevará a cabo como mínimo anualmente una evaluación de los riesgos de seguridad en relación con la seguridad y, en función de los entornos específicos, con una frecuencia mayor.<br>**El proveedor debe hacer un registro y notificar a Barclays si no es capaz de remediar o reducir cualesquiera áreas de riesgo sustanciales que podrían afectar datos de Barclays y/o al servicio que presta a Barclays.** | |
| 3. Funciones y responsabilidades | El proveedor es responsable de garantizar que todas las personas implicadas en la prestación del servicio a Barclays estén informadas de los requisitos de control de Barclays recogidos en este documento y de que los cumplan. Por lo que respecta a los requisitos de control de Barclays, el proveedor garantizará la existencia de un equipo de especialistas apropiado y/o personas con las competencias necesarias, con funciones y | Una definición clara de las funciones y las responsabilidades contribuye a la implantación del SCO de seguridad de la información y ciberseguridad. |

| | | |
|---|---|---|
| | responsabilidades definidas para gestionar los requisitos de control de Barclays, así como su eficaz funcionamiento para proteger el servicio o los servicios de Barclays.<br><br>El proveedor definirá y comunicará las funciones y las responsabilidades en relación con todos los dominios de seguridad cubiertos por el requisito de control. Estas se revisarán periódicamente (y, en cualquier caso, al menos una vez cada 12 meses) y después de que se introduzca algún cambio importante en la actividad o el modelo operativo del proveedor. Las funciones principales incluirán a un alto ejecutivo que será responsable de la seguridad de la información y la ciberseguridad.<br><br>El proveedor será responsable de garantizar que sus empleados/personal estén familiarizados y cumplan con los requisitos de control de este estándar, así como de las políticas y estándares asociados. El proveedor deberá nombrar un punto de contacto para cualquier apelación, que será el enlace con Barclays. | |
| 4. Uso autorizado | El proveedor elaborará y publicará un documento con los requisitos de uso aceptable, en el que informará a todo su personal (incluyendo contratistas y usuarios terceros de los sistemas de la organización) de sus responsabilidades.<br><br>Deberán considerarse los siguientes temas:<br><br>• el uso de internet;<br>• el uso basado en software como servicio (SaaS);<br>• el uso de depósitos de códigos públicos;<br>• el uso plugins basados en navegadores y freeware/shareware;<br>• el uso de las redes sociales;<br>• el uso del correo electrónico corporativo;<br>• el uso de la mensajería instantánea;<br>• el uso de equipos informáticos facilitados por el proveedor;<br>• el uso de equipos informáticos no facilitados por el proveedor (por ejemplo, el uso de dispositivos propios para trabajar);<br>• el uso de dispositivos de almacenamiento portátiles o extraíbles;<br>• las responsabilidades relativas al tratamiento, la preservación y el almacenamiento de los activos de información de Barclays;<br>• la salida de canales de filtración de datos; y<br>• 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. | Los requisitos en cuanto a uso aceptable contribuyen a respaldar el entorno de control que protege los activos de información. |

| | | |
|---|---|---|
| | El proveedor emprenderá las acciones necesarias para garantizar el cumplimiento de estos requisitos. | |
| 5. Educación y conocimiento | El proveedor contará con un programa de formación de conocimiento y educación en seguridad para todos sus empleados, contratistas y usuarios terceros de los sistemas de la organización y dará instrucciones cuando proceda. Todas las personas con acceso a datos/información de Barclays deberán recibir formación de conocimiento y educación apropiada y actualizaciones regulares en procedimientos, procesos y políticas técnicos y organizativos correspondientes a su función profesional en lo que atañe a la organización. Los niveles de educación, formación y conocimiento deben ser acordes a las funciones desarrolladas y consignarse en una plataforma de gestión del aprendizaje adecuada.<br><br>El proveedor garantizará que todo el personal bajo su control siga la formación en seguridad de la información obligatoria (constantemente actualizada para reflejar las nuevas amenazas que surjan y riesgos específicos de la industria), incluyendo los procedimientos recomendados de la industria y la protección de datos de Barclays, en el plazo de un mes desde que pasen a formar parte de la organización y reciclarse luego como mínimo anualmente. Deben incluirse los siguientes elementos cuando proceda:<br><br>Los grupos de alto riesgo, como las personas con acceso privilegiado o en funciones sensibles (incluyendo usuarios privilegiados, altos ejecutivos, personal de seguridad de la información y ciberseguridad y terceras partes interesadas) deben recibir formación reforzada de conocimiento de la situación de la seguridad de la información y ciberseguridad de acuerdo con sus funciones y responsabilidades. Esta formación deberá ser impartida por expertos externos cuando proceda. | En la educación y el conocimiento se basan todos los demás controles de este anexo.<br><br>De no aplicarse este principio, los empleados pertinentes no conocerán los ciberriesgos ni los vectores de ataque y serán incapaces de detectar o evitar ataques. |
| 6. Gestión de incidentes de ciberseguridad | El proveedor establecerá un marco de gestión de incidentes de seguridad que valide, remita, contenga y repare efectivamente los incidentes de seguridad del entorno del proveedor.<br><br>El proveedor garantizará que existan planes escritos de respuesta a los incidentes adaptados para cada categoría de incidente/riesgo de seguridad conocido que definan las funciones del personal, los mecanismos de apelación, así como las fases de gestión/tratamiento de incidentes:<br><br>• Validación de incidentes - Establecer un proceso de validación de incidentes que potencie distintas fuentes de datos y esté integrado en la empresa para | Un proceso de respuesta y gestión en caso de incidentes contribuye a garantizar que estos se contengan rápidamente y a evitar tener que remitirlos a instancias superiores. |

| | | |
|---|---|---|
| | validar de manera efectiva los incidentes de seguridad (esto depende de que el proveedor disponga de los mecanismos de supervisión y detección oportunos establecidos en su entorno de TI).<br>• Clasificación de incidentes - Establecer un proceso de clasificación de incidentes que clasifique de manera efectiva y rápida los incidentes validados para todos los tipos de eventos.<br>• Apelación de incidentes - Establecer mecanismos apropiados para remitir el incidente (en función de la clasificación) a las partes interesadas oportunas, personas responsables y, cuando proceda, a especialistas externos, y que permitan una respuesta rápida a los incidentes.<br>• Contención de incidentes - Utilizar a las personas, procesos y capacidades tecnológicas para identificar de forma rápida y eficaz el vector de ataque y, por consiguiente, contener los incidentes de seguridad en el entorno.<br>• Reparación - Potenciar al personal, los procesos y las capacidades tecnológicas para reparar de manera efectiva las amenazas de seguridad y/o sus componentes en el entorno. Una reparación eficaz evitará ataques de naturaleza similar en el futuro.<br><br>El proveedor procurará determinar que las actividades de respuesta a incidentes se mejoren en la medida de lo posible incorporando las lecciones aprendidas de las actividades de detección/respuesta actuales y anteriores.<br><br>El proveedor se asegurará de que se efectúen pruebas, como mínimo de carácter anual, de los procesos y equipos de respuesta a incidentes para garantizar que puede responder a los incidentes de ciberseguridad identificados.<br><br>• Las simulaciones y pruebas deben demostrar que Barclays será informado de un incidente de seguridad que le afecte; esto se pondrá de manifiesto por la capacidad del proveedor de contactar con las personas apropiadas en caso de que se produzca tal incidente.<br>• Comunicación – El proveedor deberá nombrar un punto de contacto para los incidentes de seguridad que será el enlace con Barclays en caso de producirse algún incidente. El proveedor notificará a Barclays los datos de contacto de dicha persona y cualquier cambio en los mismos, incluido el horario de contacto y los números de teléfono.<br><br>Dichos datos deben incluir: Nombre, responsabilidades dentro de la organización, función, correo electrónico y teléfono | |

| | | |
|---|---|---|
| | El proveedor informará (y, cuando proceda, se asegurará de que cualquiera de sus subcontratistas informe) a Barclays, dentro de unos plazos razonables, tras tener conocimiento de cualquier incidente que afecte o se sospeche que podría afectar al servicio prestado a Barclays o la información/datos de Barclays no más tarde de **dos (2) horas** después del momento en el que el proveedor tenga conocimiento del incidente de seguridad.<br><br>En caso de una violación de la seguridad de los datos sospechada o constatada (incluyendo una violación de la seguridad que dé lugar a la destrucción, pérdida, alteración, divulgación no autorizada o acceso a datos personales de forma accidental o ilícita), el proveedor informará a Barclays de tales incidentes en un plazo razonable desde que haya tenido constancia de ellos y en cualquier caso en el plazo máximo de **dos (2) horas** desde el momento en el que el proveedor tenga conocimiento los mismos.<br><br>Además de la notificación inicial anteriormente detallada, el proveedor entregará a Barclays un informe en el plazo de **veinticuatro (24) horas** desde que tenga conocimiento de cualquier incidente que afecte al servicio prestado a Barclays o la información/datos de Barclays. Dicho informe deberá incluir la siguiente información:<br><br>• Fecha y hora en las que el proveedor tuvo conocimiento del incidente de seguridad<br>• Jurisdicciones supuestamente afectadas<br>• Tipo y resumen breve del incidente de seguridad<br>• Impacto y consecuencias probables para los servicios prestados a Barclays y/o para la información/datos de Barclays (y, si procede, interesados afectados).<br>• Estado del incidente de seguridad (por ejemplo, se ha incorporado a expertos forenses, se ha notificado a las autoridades competentes, se ha conocido el vector de ataque, se ha realizado un seguimiento mejorado, se ha efectuado una contención)<br>• Actuación emprendida o planificada para reparar el incidente de seguridad<br>• Detalles de cualquier dato comprometido<br><br>Esos incidentes, así como todas las informaciones más recientes relativas a los esfuerzos de reparación y notificaciones a los interesados, deben comunicarse al responsable de proveedores de Barclays y al centro de operaciones conjuntas de Barclays dentro del **Centro de Operaciones Conjuntas (JOC) de la Dirección General de Seguridad de Barclays (CSO) - gcsojoc@barclays.com.** | |

| | | |
|---|---|---|
| | Por favor, incluya en el asunto del mensaje de correo electrónico: "[Insertar nombre del proveedor] – Incidente de seguridad – Se requiere atención urgente". Si el incidente es muy urgente y debe ser marcado de inmediato, se puede contactar con el JOC en su línea de atención telefónica 24/7:<br>• Reino Unido: +44 330 041 5586<br>• Estados Unidos: +1 201 499 1900<br>• India: +91 788 781 9890 | |
| 7. Clasificación y protección de la información | El proveedor contará con un marco/plan apropiado y establecido de clasificación, tratamiento y almacenamiento de la información (alineado con los procedimientos recomendados del sector y/o los requisitos de Barclays) que incluya, entre otros, los siguientes elementos:<br>• Revisar de forma constante la información/datos de Barclays existentes y nuevos<br>• Asignar a la información/los datos de Barclays el plan de etiquetado de la información correcto.<br>• Gestionar y almacenar la información/los datos de Barclays de forma segura y apropiada, en línea con su nivel de clasificación asignado.<br>• Garantizar que todo el personal conozca los requisitos de etiquetado, almacenamiento y tratamiento del proveedor/Barclays y cómo aplicar la clasificación de la información correcta.<br>El proveedor deberá remitirse al Plan del etiquetado de la información y los requisitos de tratamiento (Apéndice B, Tabla B1 y B2) de Barclays, o un plan alternativo para garantizar que protege la información de Barclays que mantiene y/o trata. Este requisito se aplica a todos los activos de información que se mantengan o traten en nombre de Barclays. | Si estos requisitos no se aplican, se podrían poner en peligro datos de Barclays, dejándolos expuestos a modificaciones no autorizadas, filtraciones, accesos no autorizados, daños, pérdidas o destrucción, lo que podría conllevar daños en el marco jurídico o para la reputación. |
| 8. Gestión de activos informáticos (hardware y software) | El proveedor garantizará que se establezca un programa de gestión de activos efectivo durante todo el ciclo de vida de los activos. La gestión de activos debe gobernar el ciclo de vida de los activos desde su adquisición hasta su retirada, aportando visibilidad y seguridad a todas las clases de activos en el entorno.<br>El proveedor mantendrá un inventario exacto y preciso de activos críticos para la empresa ubicados en todos los centros y/o ubicaciones geográficas que presten servicio a Barclays, incluyendo los equipos de Barclays alojados en instalaciones del proveedor y/o un subcontratista suministrado por Barclays, y garantizará que se | Resulta esencial disponer de un inventario completo y exacto de activos de información para garantizar la implantación de los controles pertinentes.<br>Si no se aplica este principio, los activos de Barclays o los activos utilizados por proveedores para |

| | | |
|---|---|---|
| | efectúe como mínimo una prueba anual para validar que el inventario está actualizado, está completo y es correcto.<br><br>Todo el proceso de gestión de activos debe incluir como mínimo las siguientes áreas:<br><br>• Rastreo/actualización constante de todos los activos e infraestructuras de información<br>• Activos e infraestructuras de información protegidos en función de su clasificación, criticidad y valor empresarial.<br>• El proveedor implantará controles para garantizar el registro y mantenimiento continuado de los datos de los activos de hardware durante todo su ciclo de vida.<br>• El proveedor debe mantener un inventario de activos actualizado<br>• **Los proveedores con una configuración de Nivel 1, 2 y 3 deben mantener inventarios de activos actualizados, completos y precisos (incluyendo dispositivos de acceso, equipos de red, tokens RSA y cualquier activo suministrado por Barclays).**<br>• **El proveedor reconciliará todos los activos de Barclays (hardware y software) con una periodicidad anual y lo certificará a Barclays (Dirección General de Seguridad - equipo ECAM).**<br>• Garantizar que los activos no autorizados se retiren de la red o se pongan en cuarentena y que el inventario se actualice de manera regular.<br>• Mantener una lista actualizada de todo el software autorizado que sea necesario para prestar servicio a Barclays.<br>• Garantizar que solo se añadan al inventario de software autorizado de la organización aplicaciones de software y sistemas operativos compatibles en la actualidad y que sean objeto de actualizaciones. El software no compatible debe etiquetarse como no compatible en el sistema de inventario. El software que se aproxime al final de su vida útil también debe etiquetarse como tal en el sistema de inventario.<br><br>El proveedor debe garantizar que se apliquen procesos eficientes y efectivos de manera oportuna para mitigar las tecnologías no compatibles y el final de la vida útil, retirada y destrucción de activos y datos para eliminar el riesgo de comprometer los datos. | prestar servicio a Barclays podrían estar en peligro, lo que podría generar pérdidas económicas, pérdida de datos, daños a la reputación y sanciones reglamentarias. |
| 9. Eliminación/destrucción de activos físicos | Cuando se destruyan o eliminen activos de información de Barclays que se guarden en formato físico o electrónico, dicha destrucción o eliminación se efectuará de una | La destrucción segura de los activos de información ayuda a garantizar que los activos de |

| | | |
|---|---|---|
| y remanencia de datos de la información electrónica | manera segura y adecuada al riesgo asociado, garantizando que los datos de Barclays no puedan recuperarse.<br><br>El proveedor deberá disponer de políticas y procedimientos eficaces establecidos para valorar constantemente y determinar cuándo resulta apropiado y necesario destruir o eliminar activos de información de Barclays almacenados en formato físico o electrónico, de conformidad con el contrato o por motivos de seguridad de la información, legales o reglamentarios. Barclays también puede pedir la destrucción de activos de información de Barclays mediante una solicitud escrita.<br><br>El proveedor debe establecer procedimientos con procesos empresariales que los respalden además de implementar medidas técnicas para la retirada segura y la eliminación completa de datos de Barclays (incluyendo copias de seguridad) de cualquier medio de almacenamiento, garantizando que los datos no puedan recuperarse por ningún medio forense informático.<br><br>Los datos de Barclays almacenados en medios de almacenamiento deben ser borrados hasta un nivel suficiente como para que no sean recuperables, preferiblemente utilizando técnicas de borrado de datos apropiadas como borrado seguro, purga, eliminación o destrucción de datos o métodos basados en software para sobrescribir los datos o utilizar el marco estándar de la industria para la eliminación de datos (NIST). Todo el equipo debe ser eliminado al final de su vida operativa (defectuoso, retirado debido al servicio, retirado o ya no necesario, utilizado en una prueba o ensayo de concepto, etc.). Para el equipo que vaya a ser reutilizado, se pueden utilizar servicios de borrado de datos.<br><br>Los requisitos de eliminación resultan de aplicación a las agencias subcontratadas/cuartas partes del proveedor utilizadas para prestar el servicio a Barclays.<br><br>La eliminación de información impresa deberá ser triturada hasta el mínimo de la norma P4 DIN66399 utilizando una trituradora de corte transversal (esto incluye información de tarjetas de pago) o bien se podrá incinerar de conformidad con BS EN15713:2009.<br><br>Para Barclays, la evidencia de la eliminación de los datos debe mantenerse, proporcionando un registro de auditoría, evidencia y seguimiento, y debe incluir lo siguiente:<br><br>• La prueba de la destrucción y/o eliminación (incluyendo la fecha en que se realizó el y método utilizado). | información de Barclays no puedan recuperarse mediante una vulneración de la seguridad de los datos o de actividades malintencionadas. |

| | | |
|---|---|---|
| | • Registros de auditoría del sistema para la eliminación.<br>• Certificados de eliminación de datos.<br>• Quién se encargó de la eliminación (incluyendo cualquier socio de eliminación, terceras partes o contratistas).<br>• Se debe generar un informe de destrucción y verificación para confirmar el éxito o fracaso de cualquier proceso de destrucción/eliminación (es decir, un proceso de sobrescritura debe proporcionar un informe que detalle los sectores que no se pudieron borrar).<br><br>Durante la salida, el proveedor debe asegurarse de que los datos de Barclays se hayan destruido de forma segura tras la notificación y autorización de Barclays. | |
| 10. Seguridad de la red y límites | **El proveedor se asegurará de que todos los sistemas informáticos que utilice él o sus subcontratistas y que se empleen para los servicios prestados a Barclays se protejan contra las amenazas entrantes y salientes de la red del proveedor (y de cualquier subcontratista pertinente).** El proveedor supervisará, detectará, evitará y en caso necesario corregirá el flujo de información que se transfiere entre redes con distintos niveles de confianza centrándose especialmente en las violaciones de seguridad de los datos.<br><br>Los mecanismos de integridad de la red deben incluir, entre otras cosas, las siguientes áreas:<br><br>• Mantener un inventario actualizado de todos los límites de la red de la organización (a través de una arquitectura/diagrama de red).<br>• El diseño y la implementación de la red, así como potenciales vulnerabilidades y la necesidad de retirar y renovar su infraestructura, deben revisarse como mínimo anualmente o si surge un requisito motivado por un acontecimiento que provoque cambios.<br>• Las conexiones externas a la red del proveedor deben documentarse, enrutarse a través de un firewall, ser comprobadas y aprobadas antes de establecerse, a fin de evitar infracciones de seguridad.<br>• 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.).<br>• El proveedor deberá contar con tecnologías que eviten las intrusiones en la red para detectar y evitar la entrada de tráfico malicioso en la red. | 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. |

| | | |
|---|---|---|
| | • El uso de capacidades de firewall de red fuertes que ofrezcan una capa de defensa perimetral frente a los ataques maliciosos contra las redes.<br>• El tráfico de la red de Internet debe pasar a través de un proxy que esté configurado para filtrar conexiones no autorizadas.<br>• Garantizar que el registro y el seguimiento deben estar activados.<br>• Los dispositivos de red deben endurecerse de forma segura para evitar los ataques maliciosos.<br>• Separación lógica de los puertos/las interfaces de gestión de dispositivos del tráfico de usuarios; controles de autenticación apropiados.<br>• 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.<br>• Denegar la comunicación o el tráfico de aplicaciones sobre puertos TCP o UDP no autorizados para garantizar que solo se permita cruzar el límite de la red a protocolos autorizados en cada uno de los límites de la red de la organización.<br>• Realizar lecturas regulares desde fuera de cada límite de red de confianza para detectar las conexiones no autorizadas accesibles a través del límite.<br>• Comunicaciones seguras entre dispositivos y estaciones/consolas de gestión.<br>• Configurar sistemas de seguimiento para registrar los paquetes de red que pasen a través del límite en cada uno de los límites de la red de la organización.<br>• 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.<br>• El proveedor debe revisar las reglas del firewall (externo e interno) cada año.<br>• Todo acceso inalámbrico a la red se somete a protocolos de autorización, autenticación, segmentación y cifrado para evitar infracciones de seguridad<br>• El proveedor se asegurará de que se lleve un control del acceso a la red interna y de que solo se permitan dispositivos autorizados, por medio de controles de acceso a la red pertinentes.<br>• El acceso de inicio de sesión remoto a la red del proveedor debe utilizar autenticación multifactor.<br>• El proveedor debe tener una red segregada para el servicio o los servicios de Barclays. | |

| | | |
|---|---|---|
| | El proveedor debe garantizar que ningún servidor empleado para prestar servicio a Barclays se despliegue en redes que no sean de confianza (redes fuera de su perímetro de seguridad, que escapen a su control administrativo, por ejemplo, con acceso a Internet) sin controles de seguridad apropiados.<br><br>El proveedor que aloje información de Barclays (incluyendo subcontratistas) en un centro de datos o la nube debe contar con un certificado de procedimientos recomendados del sector para la gestión de la seguridad.<br><br>Redes T2 y T3 -<br><br>• 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.<br>• 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<br>• 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;<br>o Garantizar que el registro y el seguimiento deben estar activados.<br><br>*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.* | |
| 11. 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).<br><br>El proveedor se asegurará de que los canales externos o conectados a internet que se empleen para prestar servicios a Barclays cuenten con una adecuada protección contra ataques de denegación de servicio, a fin de garantizar la disponibilidad.<br><br>Si el proveedor aloja una aplicación que está conectada a Internet y tiene datos restringidos o respalda un servicio de categoría de resistencia 0 o 1, debe protegerse hasta una capa 7 utilizando tecnologías apropiadas que deben ser aprobadas por Barclays. | De no aplicarse este principio, Barclays y sus proveedores podrían no ser capaces de evitar que un ataque por denegación de servicio alcance su objetivo. |

| | | |
|---|---|---|
| 12. Trabajo en remoto (acceso remoto) | Por lo que respecta al acceso remoto a la red de Barclays a través de aplicaciones Citrix de Barclays y/o a datos de Barclays alojados/almacenados en redes/entornos administrados por el proveedor, si el proveedor o cualquiera de sus subcontratistas permite que datos de Barclays o datos personales de Barclays o cualquier dato sensible facilitado al proveedor por necesidad de conocimiento, tanto en formato físico como electrónico, sean consultados, compartidos o tratados de forma remota, en particular cuando su personal pueda estar en régimen de teletrabajo, el proveedor obtendrá la correspondiente aprobación previa de Barclays (Dirección General de Seguridad - equipo ECAM).<br><br>El proveedor se asegurará de que los siguientes componentes estén establecidos, como mínimo, para el acceso remoto:<br><br>• El acceso de inicio de sesión remoto a la red del proveedor debe encriptarse durante los datos en tránsito y utilizar siempre autenticación multifactor.<br>• 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<br>• El proveedor mantendrá un inventario de todos los tokens RSA (hard y soft) suministrados por Barclays y un proceso de gestión que incluya la revisión y el seguimiento de la asignación, el uso y la devolución de los tokens (hard).<br>• El proveedor mantendrá registros de las personas que han pedido trabajar a distancia y la justificación de dicha solicitud<br>• **El proveedor reconciliará todos los usuarios remotos de forma trimestral y lo certificará a Barclays (Dirección General de Seguridad - equipo ECAM).**<br>• Barclays desactivará inmediatamente las credenciales de autenticación si no se han utilizado durante cierto tiempo (dicho período no deberá superar un mes).<br>• El proveedor garantizará que el extremo empleado para conectar a distancia sistemas de información de Barclays debe configurarse de manera segura y de conformidad con los procedimientos recomendados del sector (por ejemplo, nivel de los parches, estado de las soluciones contra el software malintencionado, solución EDR de detección y respuesta del extremo, inicio de sesión, etc.).<br>• 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. | 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. |

<table>
<tr>
<td></td>
<td>
<ul>
<li>No se debe permitir que dispositivos personales/BYOD accedan al entorno de Barclays y/o a datos de Barclays que residan/estén almacenados en el entorno gestionado del proveedor (incluido, entre otros, el personal del proveedor, consultores, trabajadores temporales, contratistas y socios de servicios gestionados (MPS)).</li>
</ul>
Cuando se permita el acceso de extremos (ordenadores de sobremesa/portátiles) a la red de Barclays a través de aplicaciones 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.<br><br>
NOTA: 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.
</td>
<td></td>
</tr>
<tr>
<td>13. Gestión de registros de seguridad</td>
<td>
El proveedor garantizará que exista una auditoría y un marco de gestión de registros establecido que confirme que los sistemas y procesos informáticos clave, incluyendo aplicaciones, equipos de red, bases de datos, extremos, dispositivos de seguridad, infraestructuras y servidores, estén configurados para producir los registros necesarios, de conformidad con las directrices y los procedimientos recomendados del sector. Dichos registros deben estar debidamente asegurados, guardados de manera centralizada y conservados por el proveedor durante un período mínimo de 12 meses o sobre la base de las categorías siguientes con la correspondiente justificación.
<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 proceso de gestión de registros de seguridad debe incluir como mínimo las siguientes áreas:
<ul>
<li>El proveedor debe establecer políticas y procedimientos para la gestión de registros.</li>
</ul>
</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>

| | | |
|---|---|---|
| | • El proveedor debe crear y mantener una infraestructura de gestión de registros.<br>• El proveedor debe definir las funciones y responsabilidades de las personas y equipos que se espera que participen en la gestión de registros.<br>• Recopilar, gestionar y analizar los registros de auditoría de eventos que puedan ayudar a supervisar, detectar, comprender y recuperarse de los ataques.<br>• 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.<br>• Los registros de eventos de muestra podrían incluir:<br>o IDS/IPS, router, firewall, proxy web, software de acceso remoto (VPN), servidores de autenticación, aplicaciones, registros de bases de datos.<br>o Accesos exitosos, intentos de registro fallidos (por ejemplo, ID de usuario o contraseña incorrectos), creación, modificación y eliminación a/de cuentas de usuario<br>o Registros de cambio de configuración.<br>• 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'.<br>• Análisis de registros de eventos vinculados a la seguridad (incluida la normalización, agregación y correlación).<br>• Sincronización de marcas horarias en registros de eventos con un origen común y de confianza<br>• Protección de registros de eventos vinculados a la seguridad (por ejemplo, mediante encriptado, MFA, control del acceso y copias de seguridad).<br>• Realización de acciones necesarias para remediar los problemas identificados y responder a los incidentes de ciberseguridad de manera rápida y efectiva.<br>• Despliegue de herramientas analíticas de registro o gestión de eventos e información de seguridad (SIEM) para la correlación y análisis de los registros.<br>• 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. | |
| 14. 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.<br><br>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.<br><br>La protección contra malware debe tener o incluir, entre otras cosas, lo siguiente:<br>• Soluciones contra el software malintencionado gestionado centralmente para controlar y defender continuamente el entorno informático de la organización.<br>• Garantizar que las soluciones contra el software malintencionado de la organización actualizan su motor de lectura y base de datos de firmas de manera regular y de conformidad con los procedimientos recomendados del sector.<br>• 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.<br>• El proveedor aplicará controles apropiados para proteger frente al malware y los ataques los dispositivos móviles que se conecten a las redes de Barclays o del proveedor y que accedan a los datos de Barclays.<br>• Deberán existir procesos para la celebración de reuniones/foros periódicos (por ejemplo, mensualmente) con el fin de tratar posibles vulnerabilidades o mejoras necesarias. Las medidas de reparación se deberán emprender de forma priorizada y oportuna. Se deberán conservar registros de los informes, foros y medidas de reparación emprendidas.<br><br>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. |

| | | |
|---|---|---|
| 15. 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).<br><br>El proceso estándar de configuración debe cubrir, entre otras cosas, las siguientes áreas:<br><br>• Establece políticas, procedimientos/medidas organizativas y herramientas que permiten la implementación de las normas de configuración de seguridad conforme a los procedimientos recomendados del sector para todos los dispositivos de red y sistemas operativos autorizados, aplicaciones y servidores.<br>• Realiza comprobaciones de cumplimiento regulares (anuales) para garantizar que los incumplimientos de los estándares de seguridad básicos se rectifiquen inmediatamente. Existen comprobaciones y seguimientos apropiados para garantizar que se mantenga la integridad de los equipos/dispositivos.<br>• 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.).<br><br>Garantizar que la gestión de la configuración rija los estándares de configuración segura y detecte, alerte y responda de manera efectiva a los cambios en la configuración o las desviaciones. | Los controles sobre revisiones de versiones estándar ayudan a proteger los activos de información contra accesos no autorizados.<br><br>El cumplimiento respecto de los controles y las normas sobre revisiones de versiones que garanticen que los cambios se autoricen contribuye a asegurar la protección de los activos de información de Barclays. |
| 16. Seguridad en los extremos | El proveedor reforzará los dispositivos utilizados para acceder a la red de Barclays o procesar/acceder a activos de información/datos de Barclays, a fin de protegerlos contra los ataques maliciosos.<br><br>Los procedimientos recomendados del sector deberán estar establecidos y la seguridad de los dispositivos de acceso debe incluir, entre otras cosas:<br><br>• Encriptado de disco.<br>• Deshabilitar todo el software/servicios/puertos innecesarios.<br>• Deshabilitar el acceso con derechos de administración para el usuario local. | De no aplicarse este control, la red de Barclays y la red del proveedor, así como sus extremos podrían ser vulnerables a los ciberataques. |

| | | |
|---|---|---|
| | • El personal del proveedor no podrá realizar cambios en la configuración básica, como el pack de servicios, la partición de sistemas y los servicios por defecto, etc.<br>• El puerto USB debe estar deshabilitado para prohibir las copias de datos de Barclays a soportes externos<br>• Actualización con las últimas firmas antivirus y parches de seguridad.<br>• Prevención de la pérdida de datos limitada a no cortar-copiar-pegar e imprimir pantalla de los datos de Barclays<br>• Por defecto, el acceso a las impresoras debe estar deshabilitado.<br>• 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.<br>• La compartición/transmisión de activos de información/datos de Barclays debe estar deshabilitada cuando se utilizan herramientas/software de mensajería instantánea.<br>• Capacidad y procesos para detectar el software no autorizado identificado como malicioso y evitar la instalación de software no autorizado.<br><br>NOTA: Los soportes extraíbles/dispositivos portátiles deben estar deshablitados por defecto o habilitarse solamente por razones empresariales legítimas.<br><br>El proveedor debe mantener imágenes o plantillas seguras para todos los sistemas de la empresa basados en los estándares de configuración aprobados por la organización. Cualquier despliegue de un nuevo sistema o de sistemas existentes que se hayan visto comprometidos debe representarse empleando una de esas imágenes o plantillas.<br><br>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.<br><br>Dispositivos móviles empleados para los servicios de Barclays -<br><br>1. El proveedor garantizará que implementa capacidades de gestión de dispositivos móviles (MDM) para controlar y gestionar de forma segura los | |

| | | |
|---|---|---|
| | dispositivos móviles que tengan acceso y/o contengan información de Barclays clasificada, reduciendo el riesgo de comprometer los datos.<br>2. El proveedor garantizará la implementación de capacidades de bloqueo y borrado a distancia para los dispositivos móviles que protejan la información en caso de que un dispositivo se robe, pierda o vea comprometido.<br>3. Encriptado de datos en dispositivos móviles (datos de Barclays). | |
| 17. Prevención de las filtraciones de datos | El proveedor contará con un marco establecido para garantizar que exista protección frente a las fugas de datos inapropiadas que garantice la protección, incluidos los siguientes canales de fugas de información (entre otros):<br>• transferencia no autorizada de información fuera de la red interna o la red del proveedor<br>  o Correo electrónico<br>  o pasarela web/de internet (incluyendo almacenamiento online y webmail)<br>  o DNS<br>• 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).<br>• transferencia no autorizada de información a soportes portátiles.<br>• intercambio no seguro de información con terceros (cuartas partes o subcontratistas).<br>• 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).<br>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. |
| 18. Seguridad de los datos | El proveedor garantizará que los activos de información/datos de Barclays bajo su custodia/su red estén debidamente protegidos a través de una combinación de técnicas de encriptado, medios seguros para el acceso a los datos, protección de la integridad y técnicas de prevención de la pérdida de datos. Es importante extremar el cuidado para limitar el acceso a los activos de información/datos de Barclays, incluyendo datos personales, y para que ese acceso resulte seguro.<br><br>Los controles de seguridad de datos deben incluir, entre otras cosas, las siguientes áreas:<br>1. El proveedor está obligado en todo momento a cumplir todas y cada una de las leyes de protección de datos aplicables. | |

| | | |
|---|---|---|
| | 2. Deben establecerse políticas y procedimientos, así como procesos empresariales/medidas organizativas que los respalden y medidas técnicas aplicadas, con el fin de inventariar, documentar y mantener los flujos de datos que residan (temporal o permanentemente) en las aplicaciones distribuidas geográficamente (física y virtualmente) dentro del servicio y la red de infraestructuras y los componentes de los sistemas y/o que se compartan con otros terceros.<br>3. Mantener un inventario de toda la información sensible/confidencial (activos de información/datos de Barclays) almacenada, tratada o transmitida por el proveedor.<br>4. Establecer un estándar de clasificación de los datos para garantizar que la información sensible (activos de información/datos de Barclays) se clasifique y proteja apropiadamente.<br>5. Garantizar que todos los datos de Barclays estén clasificados y marcados de acuerdo con el estándar de clasificación y protección de datos.<br>6. Protección de los datos en reposo;<br>a. Como mínimo, encriptar los datos en reposo para evitar que se explote información sensible a través de accesos no autorizados.<br>7. Supervisión de la actividad de las bases de datos;<br>a. Supervisar y registrar el acceso y la actividad de las bases de datos para identificar de manera rápida y efectiva la actividad maliciosa.<br>8. Protección de los datos en uso;<br>a. Garantizar que la visualización y uso de la información sensible se controle a través de capacidades de gestión de acceso para proteger de la explotación de la información sensible.<br>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.<br>9. Protección de los datos en tránsito;<br>a. Aprovechamiento de capacidades de encriptado fuerte para garantizar la protección de los datos en tránsito.<br>b. El encriptado de los datos en tránsito suele lograrse a través del encriptado de transporte o carga (mensaje o campo selectivo). Los mecanismos de encriptado de transporte incluyen, entre otros:<br>• 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) | |

| | | |
|---|---|---|
| | • Tunelización segura (IPsec)<br>• Secure Shell (SSH)<br>c. Deben configurarse protocolos de seguridad de transporte para evitar la negociación de algoritmos más débiles y/o longitudes de clave más cortas cuando ambos extremos admitan la opción más fuerte.<br>10. Copia de seguridad de los datos –<br>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.<br>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.<br>c. Garantizar que se realicen copias de seguridad con regularidad de todos los datos de Barclays. | |
| 19. Seguridad del software de aplicaciones | El proveedor desarrollará aplicaciones utilizando procedimientos de programación seguros y en entornos seguros. Si el proveedor desarrolla aplicaciones para que Barclays las utilice, o que se utilicen para respaldar el servicio prestado a Barclays, deberá establecer un marco de desarrollo seguro para prevenir las infracciones de seguridad e identificar y corregir las vulnerabilidades en el código durante el proceso de desarrollo.<br>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. |

| | | |
|---|---|---|
| | • Deben establecerse y adoptarse estándares de codificación seguros en línea con los procedimientos recomendados del sector para evitar vulnerabilidades e interrupciones del servicio y que al mismo tiempo defiendan frente a posibles vulnerabilidades ya conocidas.<br>• Establecer prácticas de codificación seguras apropiadas al lenguaje de programación.<br>• Todo el desarrollo debe llevarse a cabo en un entorno no productivo.<br>• Mantener entornos separados para los sistemas productivos y no productivos. Los desarrolladores no deben acceder sin control a los entornos productivos.<br>• Separación de tareas para los sistemas productivos y no productivos.<br>• Sistemas desarrollados en línea con los procedimientos recomendados del sector para el desarrollo seguro (como OWASP).<br>• El código debe almacenarse de manera segura y someterse a controles de calidad.<br>• El código debe protegerse adecuadamente de las modificaciones no autorizadas una vez que las pruebas se hayan validado y se haya entregado a producción.<br>• Utilizar solo componentes de terceros actualizados y de confianza para el software desarrollado por el proveedor.<br>• Aplicar herramientas analíticas estáticas y dinámicas para comprobar que se cumplen las prácticas de codificación seguras.<br>• El proveedor debe asegurarse de que los datos activos (incluyendo datos personales) no se utilizarán en entornos que no sean de producción.<br>• 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).<br><br>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. | |
| 20. 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 | Los controles de LAM pertinentes ayudan a garantizar la protección |

| | | |
|---|---|---|
| | mínimo y a la separación de funciones. El responsable de activos de información se encarga de decidir el acceso que necesita cada persona.<br><br>• El principio de divulgación de información solo cuando sea necesario conocerla se basa en que solo se debería tener acceso a ella cuando se necesite conocerla para desempeñar las obligaciones para las que nos hayan autorizado. Por ejemplo, si un empleado trata en exclusiva con clientes que tengan su sede en Reino Unido, no «necesitará conocer» información que pertenezca a clientes con sede en Reino Unido.<br>• 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.<br>• 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.<br><br>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.<br><br>Se definirán procesos de gestión del acceso de acuerdo con los procedimientos recomendados del sector que incluirán lo siguiente:<br><br>• 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.<br>• Deben existir controles para la autorización, para asegurarse de que el proceso de concesión, modificación y retirada del acceso incluye un nivel de autorización que se ajuste al nivel de privilegios otorgados.<br>• Deben existir controles que garanticen que los procesos de gestión de acceso incluyen los mecanismos apropiados para la verificación de identidades. | de los activos de información contra un uso inadecuado.<br><br>Los controles de gestión de acceso contribuyen a garantizar que solo puedan acceder a los activos de información los usuarios autorizados. |

| | | |
|---|---|---|
| | • Cada cuenta debería estar asociada a una sola persona, que responderá de toda actividad que se lleve a cabo usando la cuenta.<br>• 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.<br>• Todos los permisos de acceso privilegiado deben revisarse al menos cada (6) meses y deben implantarse los controles adecuados para los requisitos del acceso privilegiado.<br>• Controles del personal que cambia de puesto - Modificación del acceso en el plazo 24 horas desde la fecha de traslado (y mantenimiento de los correspondientes registros);<br>• Controles del personal que abandona la empresa - Todo acceso lógico utilizado para prestar servicios a Barclays se eliminará en un plazo de 24 horas desde la fecha de cese (y se mantendrán los correspondientes registros);<br>• Acceso remoto - Los controles de acceso remoto solo se permitirán a través de mecanismos acordados por Barclays (Dirección General de Seguridad - equipo ECAM) y el acceso remoto debe usar autenticación multifactor.<br>• Autenticación - Deben seguirse controles de la longitud y complejidad apropiada de las contraseñas, frecuencia del cambio de estas, autenticación multifactor, gestión segura de las credenciales de las contraseñas, entre otros, de acuerdo con los procedimientos recomendados del sector.<br>• Cuentas inactivas - Las cuentas inactivas que no se usen durante 60 días consecutivos o más deben suspenderse/desactivarse (y se mantendrán los correspondientes registros).<br>• 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.<br>• Las cuentas privilegiadas deben modificarse después de cada uso y cada 90 días como mínimo.<br>• 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. | |
| 21. Gestión de las vulnerabilidades | El proveedor debe contar con 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 propiedad del proveedor, redes de | De no aplicarse este control, los atacantes podrían aprovechar las vulnerabilidades de los sistemas para realizar ciberataques, lo que |

<table>
<tr>
<td></td>
<td>infraestructuras y componentes de sistema para garantizar la eficiencia de los controles de seguridad implementados.<br><br>La gestión de vulnerabilidades debe incluir, entre otras cosas, las siguientes áreas:<br><br>• Funciones, responsabilidades y obligaciones definidas para la supervisión, presentación de información, apelación y reparación.<br>• Herramientas e infraestructura apropiadas para el análisis de vulnerabilidades.<br>• Desarrollar 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.<br>• Utilizar un proceso de evaluación del riesgo para priorizar la remediación de las vulnerabilidades descubiertas.<br>• 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.<br>• 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).<br>• Comparar regularmente los resultados de análisis consecutivos de vulnerabilidades para comprobar que estas se han remediado de forma puntual.<br><br>En el caso de los servicios de proveedor relacionados con la infraestructura de alojamiento/aplicaciones en nombre de Barclays,<br><br>• El proveedor debe notificar a Barclays de inmediato si se identifica alguna vulnerabilidad crítica/alta.<br>• 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>
</table>
</td>
<td>podría provocar daños en el marco jurídico o para la reputación.</td>
</tr>
</table>

| | | |
|---|---|---|
| | <table><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><br>Todos los problemas y vulnerabilidades de seguridad que pudieran afectar de forma importante a la infraestructura de alojamiento/aplicaciones web de Barclays suministradas por el proveedor y cuyo riesgo el proveedor haya decidido aceptar se comunicarán de inmediato a Barclays y se acordarán por escrito con Barclays (Dirección General de Seguridad - equipo ECAM). | |
| 22. Gestión de revisiones | El proveedor debe contar con 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.<br><br>El proveedor garantizará que se apliquen a los sistemas/activos/redes/aplicaciones los últimos parches de seguridad de manera oportuna, y de conformidad con los procedimientos recomendados del sector, de forma que se garantice que:<br><br>• El proveedor probará que todos los parches en los sistemas representan de manera precisa la configuración de los sistemas de producción objetivo antes de desplegar el parche en los sistemas de producción y que el correcto funcionamiento del servicio con el parche se comprueba después de la actividad de parcheado. Si un sistema no puede parchearse, desplegar contramedidas apropiadas.<br>• Todos los cambios informáticos importantes deben ser registrados, probados y autorizados antes de la implementación mediante un proceso sólido y aprobado de gestión de cambios, a fin de evitar interrupciones del servicio o infracciones de seguridad.<br>• El proveedor se asegurará de que los parches se reflejen en entornos de producción y recuperación de desastres (DR). | 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>23. 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 informática de la infraestructura informática que incluya el centro de recuperación tras desastres y las aplicaciones web en relación con los servicios que preste a Barclays.<br><br>
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.<br><br>
En el caso de los servicios de proveedor relacionados con la infraestructura de alojamiento/aplicaciones en nombre de Barclays,
<ul>
<li>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.</li>
<li>Todos los problemas cuyo riesgo se haya decidido aceptar se comunicarán a Barclays para acordarlos con el banco (Dirección General de Seguridad - equipo ECAM).</li>
<li>El proveedor deberá compartir el informe de evaluación de la seguridad más reciente con Barclays (Dirección General de Seguridad - equipo ECAM).</li>
<li>El proveedor debe notificar a Barclays de inmediato si se identifica alguna vulnerabilidad crítica/alta.</li>
<li>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).</li>
</ul>
<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>
<tr><td>P3</td><td>Medio</td><td>60</td></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.<br><br>
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>

| | | | | | |
|---|---|---|---|---|---|
| | | P4 | Bajo | 180 | |
| | | P5 | Informativo | 360 | |
| 24. Criptografía | • 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.<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>o El proveedor deberá garantizar que todas las claves se sometan a una vida de criptoperiodo definida y limitada tras el cual se sustituyan o desactiven. Esto también debe ser acorde a los requisitos del National Institute of Standards and Technology (NIST) y a los procedimientos recomendados del sector aplicables<br>• Protección del almacenamiento de claves - El proveedor deberá garantizar que solo existan claves criptográficas secretas/privadas en las siguientes formas:<br>o En el límite criptográfico de un dispositivo/módulo con hardware certificado. | | | | Los algoritmos y la protección del cifrado pertinentes y actualizados garantizan una protección continua para los activos de información de Barclays. |

| | | |
|---|---|---|
| | o En forma encriptada bajo otra clave establecida o derivada de una contraseña.<br>o En partes de componentes divididos entre grupos de custodia diferentes.<br>o No encriptadas en la memoria host durante el período de operación criptográfica, salvo que se precise en la protección de HSM.<br>• 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:<br>o Claves para servicios regulados donde los HSM sean obligatorios.<br>o Certificados que representen a Barclays de CA públicos.<br>o Certificados raíz, de emisión, OCSP y RA (autoridad de registro) empleados para emitir certificados que protejan los servicios de Barclays.<br>o Claves que protejan depósitos agregados almacenados de claves, credenciales de acreditación o datos PII.<br>• 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.<br>• 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:<br>o Equipo de soporte informático<br>o Activos relacionados<br>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.<br>• 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.<br>• 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.<br>• 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.<br>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.<br>• 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.**<br>• 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. | |
| 25. Computación en la nube | El proveedor 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 proteger los conceptos básicos 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.<br>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 | 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. |

| | | |
|---|---|---|
| | unos controles apropiados equivalentes a la versión más reciente de la Matriz de Controles de Seguridad en la Nube (CCM) de la Cloud Security Alliance.<br><br>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 servicio 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.<br><br>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):<br><br>• Mecanismos de gobernanza y rendición de cuentas<br>• Identidad y gestión de acceso<br>• Seguridad de la red (incluyendo conectividad)<br>• Seguridad de datos (en tránsito/reposo/almacenados)<br>• Criptografía, encriptado y gestión de claves - CEK<br>• Registro y monitorización<br>• Virtualización<br>• Segregación de servicios<br><br>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).<br><br>Cuando un proveedor del servicio en la nube vaya a mantener datos sensibles (personales y restringidos), el proveedor debe facilitar a Barclays las ubicaciones, zonas de datos y zonas de datos de conmutación por error donde se guardarán esos datos. | |

| | | |
|---|---|---|
| 26. 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).<br><br>Los diferentes tipos de EDB son:<br><br>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.<br><br>Nivel 2 (clase empresarial) - Toda la infraestructura informática es gestionada por el **proveedor** y se conecta a las pasarelas de Extranet de **Barclays** - dispositivos LAN, WAN y Desktop - es propiedad y está gestionada por el proveedor.<br><br>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. |
| 26.1 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. | |
| 26.2 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.<br>• 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.<br>• Una tarjeta electrónica de acceso autorizado para acceder a las áreas EDB de las instalaciones.<br>• 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.<br>• 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).<br>• 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<br>• Deben activarse controles automáticos seguros para el acceso al EDB, como:<br>Para el personal autorizado:<br>o Tarjeta de identificación con foto siempre visible<br>o Implementación de lectores de tarjeta por proximidad<br>o Habilitación de un mecanismo antirretorno | |

| | |
|---|---|
| | • El proveedor contará con procesos y procedimientos para controlar y monitorizar a las personas externas, incluyendo terceros con acceso físico a las áreas EDB para realizar tareas de mantenimiento y limpieza. |
| 26.3 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.<br>• Todos los puntos de entrada y salida de las EDB deben contar con videovigilancia.<br>• 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.<br>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. |
| 26.4 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<br>• El proveedor mantendrá registros de las personas que han pedido tokens de autenticación de Barclays y realizará una reconciliación trimestral.<br>• 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.<br>• Barclays desactivará inmediatamente las credenciales de autenticación si no se han utilizado durante cierto tiempo (dicho período no deberá superar un mes).<br>• 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.<br>Consultar control - 12. Trabajo en remoto (acceso remoto) |
| 26.5 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). |
| 26.6 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).<br>• El diseño e implementación de la red debe revisarse como mínimo anualmente.<br>• 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.<br>• 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;<br>o Garantizar que el registro y el seguimiento deben estar activados.<br>• La red EDB debe ser monitorizada y solo deben permitirse dispositivos autorizados por medio de controles de acceso a la red pertinentes.<br><br>Consultar control - 10. Seguridad de la red y límites |
| 26.7 EDB - Red inalámbrica | Las redes inalámbricas deben estar deshabilitadas para el segmento de la red de Barclays que preste servicios al banco. |
| 26.8 EDB - Seguridad de los extremos | Deben configurarse equipos de escritorio seguros según los procedimientos recomendados del sector para los ordenadores de la red EDB.<br><br>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:<br><br>• Encriptado de disco;<br>• Deshabilitación de todo el software/servicios/puertos innecesarios.<br>• Deshabilitación del acceso con derechos de administración para el usuario local.<br>• El personal del proveedor no podrá realizar cambios en la configuración básica, como el pack de servicios y los servicios por defecto, etc.<br>• El puerto USB debe estar deshabilitado para prohibir las copias de datos de Barclays a soportes externos;<br>• Actualización con las últimas firmas antivirus y parches de seguridad;<br>• 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<br>• Por defecto, el acceso a las impresoras debe estar deshabilitado;<br>• La compartición/transmisión de datos de Barclays debe estar deshabilitada utilizando herramientas/software de mensajería instantánea;<br>• Capacidad y procesos para detectar el software no autorizado identificado como malicioso y evitar la instalación de software no autorizado;<br><br>Consultar control - 16. Seguridad en los extremos |
| 26.9 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.<br>• 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.<br>• La transmisión no autorizada de datos de Barclays fuera de la red EDB debe protegerse de las fugas de datos: |

| | | |
|---|---|---|
| | • Correo electrónico<br>• pasarela web/de internet (incluyendo almacenamiento online y webmail)<br>• 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<br>• bloquear todos los adjuntos y/o función de carga en sitios web<br>• Garantizar que solo se permiten navegadores web y clientes de correo electrónico totalmente compatibles. | |
| 26.10 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 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.<br><br>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.<br><br>El proveedor debe prestar a Barclays toda la asistencia que solicite en términos de razón en relación con cualquier inspección y documentación presentada durante una inspección que deba completarse y devolverse a Barclays. | Si no aceptan, los proveedores no podrán garantizar plenamente que se cumplen estas obligaciones de seguridad. |

## Apéndice A. Glosario

| Definiciones | |
|---|---|
| Cuenta | Un conjunto de credenciales (por ejemplo, el ID de un usuario y la contraseña) mediante el cual se gestiona el acceso a un sistema informático usando controles de acceso lógico. |
| Copia de seguridad, copia de seguridad | Una copia de seguridad o el proceso de copia de seguridad se refiere a la realización de copias de datos para poder recuperar el original tras un incidente de pérdida de datos. |
| Espacio dedicado al banco | Espacio dedicado al banco significa cualquier instalación propiedad de un miembro del grupo del proveedor o de cualquier subcontratista, o bajo su control, que se dedique exclusivamente a Barclays y desde la que se presten o realicen los servicios. |
| 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.<br>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<br>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). |
| Datos personales | 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 mantenimiento del sistema, administración de la seguridad o cambios de configuración de un sistema informático.<br><br>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:<br>• Los intentos (fallidos o exitosos) de obtener acceso no autorizado a un sistema o sus datos.<br>• Perturbaciones no deseadas o denegaciones de servicio.<br>• Uso no autorizado de un sistema para procesar o almacenar datos.<br>• Cambios en las características de hardware, firmware o software del sistema sin el conocimiento, dirección o consentimiento del propietario.<br>• Vulnerabilidades de una aplicación que dan lugar a un acceso no autorizado a datos. |

## Apéndice B. Plan del etiquetado de la información de Barclays

### Tabla B1: Plan del etiquetado de la información de Barclays

| Etiqueta | Definición | Ejemplos |
|---|---|---|
| **Secreta** | 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).<br><br>Esta información está restringida a un público específico y no debe distribuirse sin el permiso de la persona de la que se haya obtenido. El público puede incluir destinatarios externos con autorización explícita del responsable de información. | • Información sobre posibles fusiones o adquisiciones.<br>• Información de planificación estratégica: empresarial y organizativa.<br>• Determinada configuración de la seguridad de la información.<br>• Determinados resultados de auditorías e informes.<br>• Actas del Comité Ejecutivo.<br>• Datos de autenticación o identificación y verificación: cliente y empleado.<br>• Volúmenes generales de información de los titulares de tarjetas.<br>• Pronósticos de beneficios o resultados financieros anuales (antes de hacerse públicos).<br>• Cualquier elemento cubierto por un Acuerdo de confidencialidad formal (NDA). |
| **Restringida – Interna** | La información deberá clasificarse como **Restringida – Interna** si los destinatarios previstos son solo empleados de Barclays autenticados y Proveedores de servicios gestionados de Barclays con un contrato en vigor y restringida a un público específico.<br><br>La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero).<br><br>Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla. | • Estrategias y presupuestos<br>• Evaluaciones del personal<br>• Remuneración y datos personales de los empleados<br>• Evaluaciones de la vulnerabilidad |
| **Restringida- Externa** | La información deberá clasificarse como **Restringida – Externa** si los destinatarios previstos son empleados autenticados de Barclays y Proveedores de servicios gestionados de Barclays con un contrato en vigor y que esté restringida a un público específico o partes externas autorizadas por el responsable de la información.<br><br>La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero). | • Planes de nuevos productos<br>• Contratos de clientes<br>• Contratos legales<br>• Información de clientes individuales o de escaso volumen que deba enviarse externamente.<br>• Comunicaciones de clientes.<br>• Materiales de oferta de nuevas emisiones (por ejemplo, folleto, nota sobre la oferta).<br>• Documento de investigación definitivo. |

| | | |
|---|---|---|
| | Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla. | • Información no pública de carácter material no perteneciente a Barclays (MNPI).<br>• Todos los informes de investigación.<br>• Determinados materiales de marketing<br>• Comentario de marketing<br>• Resultados de auditorías e informes |
| Sin restricción | La información debe clasificarse como Sin restricción si está destinada a su distribución general o que no causaría ninguna repercusión en la organización si se distribuyera. | • Material de marketing<br>• Publicaciones<br>• Anuncios públicos<br>• Anuncios de ofertas de trabajo<br>• Información sin impacto para Barclays. |

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

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

| Fase del ciclo de vida | Secreta | Restringida – Interna | Restringida – Externa |
|---|---|---|---|
| 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 lugares donde personas no autorizadas puedan verlos o acceder a ellos.<br>• 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.<br>• 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. | • 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).<br>• 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.<br>• Los activos almacenados en formato electrónico se protegerán mediante cifrado, o con controles de compensación apropiados, si hubiera un riesgo importante de que personal no autorizado pudiera acceder a ellos. |

| | | | |
|---|---|---|---|
| Acceso y uso | • 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).<br>• Para la impresión de activos se usarán herramientas de impresión segura.<br>• Los activos en formato electrónico se protegerán mediante controles de gestión de acceso lógico apropiados. | • Los activos (físicos o electrónicos) no se dejarán en zonas públicas fuera de las instalaciones.<br>• Los activos (físicos o electrónicos) no se dejarán en zonas públicas de las instalaciones a las que puedan acceder visitantes sin supervisión.<br>• 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).<br>• Los activos que se envíen a imprimir se recogerán inmediatamente de la impresora. Si no fuera posible, se usarán herramientas para la impresión segura.<br>• Los activos en formato electrónico se protegerán mediante controles de gestión de acceso lógico apropiados. |
| Uso compartido | • Los activos en papel llevarán una etiqueta de información visible en cada página.<br>• 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.<br>• 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.<br>• Los activos solo se distribuirán usando sistemas, métodos o proveedores aprobados por la organización. | • Los activos en papel llevarán una etiqueta de información visible. La etiqueta irá como mínimo en la página que lleve el título.<br>• Los activos electrónicos llevarán una etiqueta informativa clara.<br>• Los activos solo se distribuirán usando sistemas, métodos o proveedores aprobados por la organización.<br>• Los activos solo se distribuirán a personas empleadas por la organización (o con una obligación contractual apropiada) o como parte de una necesidad comercial claramente reconocida, como una negociación de contrato. | • Los activos en papel llevarán una etiqueta de información visible. La etiqueta irá como mínimo en la página que lleve el título.<br>• Los sobres que contengan activos en papel llevarán una etiqueta de información visible en la parte delantera.<br>• 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.<br>• Los activos solo se distribuirán usando sistemas, métodos o proveedores aprobados por la organización.<br>• 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 empleadas por la organización (o con una obligación contractual apropiada) o como parte de una necesidad comercial claramente reconocida, como una negociación de contrato.<br>• Los activos solo se distribuirán a personas específicamente autorizadas por el propietario del activo de información.<br>• Los activos no se enviarán por fax.<br>• Los activos electrónicos se cifrarán utilizando un mecanismo de protección criptográfico cuando transiten fuera de la red interna.<br>• Se mantendrá la cadena de custodia de los activos electrónicos. | | • Los activos solo se distribuirán a personas que necesiten recibirlos por razones del negocio.<br>• Los activos no se enviarán por fax a no ser que el remitente haya confirmado que los destinatarios están listos para recibirlos.<br>• Los activos electrónicos se cifrarán utilizando un mecanismo de protección criptográfico cuando transiten fuera de la red interna. |
| Archivo y eliminación | • Los activos en papel se eliminarán utilizando un servicio de gestión de residuos confidencial.<br>• Las copias de los activos electrónicos también se eliminarán de las «papeleras de reciclaje» del sistema de manera oportuna.<br>• Los soportes en los que se hayan almacenado activos electrónicos «secretos» se limpiarán adecuadamente antes o durante la eliminación. | • Los activos en papel se eliminarán utilizando un servicio de gestión de residuos confidencial.<br>• 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.<br>• Las copias de los activos electrónicos también se eliminarán de las «papeleras de reciclaje» del sistema de manera oportuna. |

# 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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>El proveedor se asegurará de que todos sus empleados nuevos (que tengan acceso a los CID o los gestionen), en un plazo razonable (aproximadamente tres meses) realicen un curso de formación que garantice que entienden sus responsabilidades con respecto a los CID.<br><br>El proveedor llevará un seguimiento de los empleados que han realizado el curso de formación.<br><br>* las jurisdicciones con secreto bancario ofrecerán información sobre el contenido previsto para los cursos de formación. | En la educación y el conocimiento se basan todos los demás controles de este anexo. |
| 4. Plan de etiquetado de la información | *Cuando proceda**, el proveedor deberá aplicar el Plan del etiquetado de la información de Barclays (Tabla 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.<br><br>Los requisitos de gestión de los CID se incluyen en la Tabla E2 del Apéndice E.<br><br>* «*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 C: Glosario

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

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

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

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

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

| Clasificación de la información | Secreto bancario | | Restringida – Interna |
|---|---|---|---|
| **Clasificación** | **CID directos (CIDD)** | **CID directos (CIDI)** | |
| | | **Indirectos (N1)** | **Posiblemente indirectos (N2)** | **Identificador impersonal (N3)** |
| Tipo de información | Nombre del cliente | Número de contenedor / ID de contenedor | 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

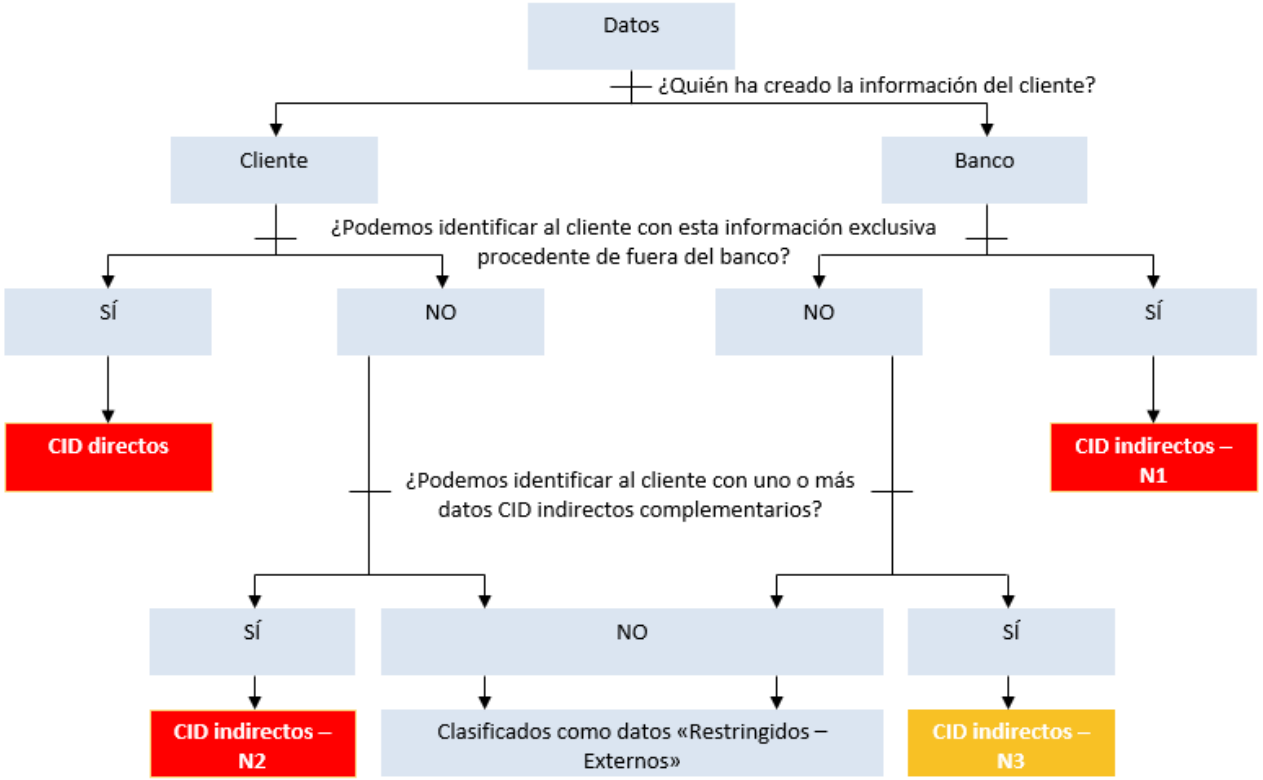
   (DIDD) = Vulneración del secreto bancario

2. ID de contenedor

   (N1CIDI) = Vulneración del secreto bancario

3. Situación patrimonial + Nacionalidad

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


Datos
¿Quién ha creado la información del cliente?
Cliente
Banco
¿Podemos identificar al cliente con esta información exclusiva procedente de fuera del banco?
SÍ
NO
NO
SÍ
CID directos
CID indirectos – N1
¿Podemos identificar al cliente con uno o más datos CID indirectos complementarios?
SÍ
NO
SÍ
CID indirectos – N2
Clasificados como datos «Restringidos – Externos»
CID indirectos – N3

## Apéndice E: Plan del etiquetado de la información de Barclays

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

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

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

| | | |
|---|---|---|
| | empresariales (ERMF) como «crítico» (financiero o no financiero).<br><br>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.<br>• Determinados resultados de auditorías e informes.<br>• Actas del Comité Ejecutivo.<br>• Datos de autenticación o identificación y verificación: cliente y compañero.<br>• Volúmenes generales de información de los titulares de tarjetas.<br>• Pronósticos de beneficios o resultados financieros anuales (antes de hacerse públicos).<br>• 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.<br><br>La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero).<br><br>Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla. | • Estrategias y presupuestos.<br>• Evaluaciones del personal.<br>• Remuneración y datos personales de los empleados.<br>• Evaluaciones de la vulnerabilidad.<br>• 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.<br>• Contratos de clientes.<br>• Contratos legales.<br>• Información de clientes individuales o de escaso volumen que deba enviarse externamente.<br>• Comunicaciones de clientes.<br>• Materiales de oferta de nuevas emisiones (por ejemplo, folleto, nota sobre la oferta).<br>• Documento de investigación definitivo. |

| | | |
|---|---|---|
| | La divulgación no autorizada causaría un perjuicio a Barclays, valorado de acuerdo con el ERMF como «importante» o «limitado» (financiero o no financiero).<br><br>Esta información no está destinada a la distribución general aunque sus destinatarios pueden reenviarla o compartirla con quienes necesiten conocerla. | • Información no pública de carácter material no perteneciente a Barclays (MNPI).<br>• Todos los informes de investigación.<br>• Determinados materiales de marketing.<br>• 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.<br>• Publicaciones.<br>• Anuncios públicos.<br>• Anuncios de ofertas de trabajo.<br>• Información sin impacto para Barclays. |

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

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

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

| | |
|---|---|
| Almacenamiento | De acuerdo con «Restringida-Externa» y:<br>• Los activos se guardarán exclusivamente en soportes extraíbles durante el tiempo exigido explícitamente por una necesidad empresarial concreta, reguladores o auditores externos.<br>• 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).<br>• 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.<br>• 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).<br>• 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.<br>• 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:<br>• 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).<br>• 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).<br>• 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:<br>• 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.<br>• La transferencia ocasional de activos en soportes extraíbles requiere la aprobación del responsable del activo de información y del CIS.<br>• Se cifrarán las comunicaciones electrónicas en tránsito.<br>• Los activos (en papel) enviados por correo deberán entregarse utilizando un servicio que exija un acuse de recibo.<br>• 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).<br>• 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.<br>• 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.<br>• 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.<br>• Los activos (físicos o electrónicos) no se dejarán en zonas públicas de las instalaciones a las que puedan acceder visitantes sin supervisión.<br>• 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).<br>• Los activos que se envíen a imprimir se recogerán inmediatamente de la impresora. Si no fuera posible, se usarán herramientas para la impresión segura.<br>• 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).<br>• Para la impresión de activos se usarán herramientas de impresión segura.<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>• Los activos solo se distribuirán usando sistemas, métodos o proveedores aprobados por la organización.<br>• 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.<br>• Los activos solo se distribuirán a personas que necesiten recibirlos por razones del negocio.<br>• Los activos no se enviarán por fax a no ser que el remitente haya confirmado que los destinatarios están listos para recibirlos.<br>• 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.<br>• 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.<br>• Los activos solo se distribuirán usando sistemas, métodos o proveedores aprobados por la organización.<br>• 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.<br>• Los activos solo se distribuirán a personas específicamente autorizadas por el propietario del activo de información.<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>• Las copias de los activos electrónicos también se eliminarán de las «papeleras de reciclaje» del sistema de manera oportuna.<br>• Los soportes en los que se hayan almacenado activos electrónicos «secretos» se limpiarán adecuadamente antes o durante la eliminación. |