Obligaciones de control de proveedores externos

Seguridad física (controles técnicos o TC)

Versión 13.0 Final Septiembre de 2023

Título del control	Descripción del control	Por qué es importante
1. Control de acceso (TC 5.1)	Se deben definir reglas de control de acceso para todas las áreas seguras, con procedimientos aprobados formales y responsabilidades definidas. Las áreas seguras deben estar protegidas con controles de entrada y puntos de acceso adecuados mediante control de acceso electrónico, mecánico o digital. El acceso lógico y administrativo a los sistemas de control de acceso electrónico debe limitarse al personal autorizado y el acceso a las claves físicas y las combinaciones debe gestionarse y controlarse estrictamente. Se debe mantener un registro de auditoría de titulares de credenciales/claves/combinaciones que cubra la concesión, modificación y revocación de permisos de acceso. Todas las credenciales de acceso deben gestionarse de manera efectiva para reducir el riesgo de accesos no autorizados. Las credenciales de acceso deberán gestionarse de conformidad con los procedimientos de control de acceso del proveedor. Las credenciales de acceso únicas se expiden tras recibir la autorización correspondiente. Todas las credenciales de acceso a áreas restringidas deben recertificarse a intervalos razonables. Cuando ya no sea necesario acceder a un local o a un área restringida, la función responsable de la administración de las credenciales de acceso debe desactivarlas en un plazo de 24 horas a partir de la recepción de la notificación de la unidad de negocio o función pertinente que informa del cambio en los requisitos para el empleado en cuestión (por ejemplo, cambio de función o responsabilidades, o despido o cese de empleo).	El mantenimiento de un sistema de control de acceso eficaz y de los procesos y procedimientos de gestión de acceso es un componente vital dentro de la combinación de niveles de controles necesarios para proteger las instalaciones del acceso no autorizado y garantizar la seguridad de los activos. Salvo que se cuente con medidas de control de acceso efectivas, existe el riesgo de que personal no autorizado entre en las instalaciones o las áreas restringidas del proveedor dentro de sus sedes. Esto podría aumentar el riesgo de pérdida o deterioro de los activos de Barclays, lo que provocaría pérdidas económicas y daños asociados para la reputación y/o sanciones por incumplimiento de normativa o censura.

2. Seguridad de perímetros, edificios y espacios (TC 5,2)	Se deben definir y establecer perímetros de seguridad para proteger las áreas que contienen información y otros activos asociados, en proporción al entorno de riesgo y amenazas identificadas y previstas. Se debe definir y establecer la seguridad física de oficinas, salas e instalaciones (incluidos sistemas de control de acceso, cámaras de seguridad, sistemas de detección de intrusos y otros controles técnicos adecuados) de acuerdo con un enfoque basado en el riesgo con arreglo a los niveles de amenaza actuales y previstos, y ser proporcionales a los procesos empresariales realizados y al valor de la información y los activos. Se deben diseñar y adoptar procesos de seguridad para trabajar en áreas seguras. Se deben definir y aplicar adecuadamente unas normas claras para los papeles y medios de almacenamiento extraíbles, así como para las pantallas de ordenadores, en las instalaciones de procesamiento de información. Todos los centros de datos, proveedores de nube, salas de datos e instalaciones de comunicación independientes, en ubicaciones conjuntas y de terceros (lo que incluye las salas de servidores y los gabinetes de comunicación independientes) deben estar protegidos de forma eficaz para evitar el acceso no autorizado, el robo o los daños a los activos o datos de Barclays. Cuando las instalaciones se encuentren en ubicaciones compartidas, se deben establecer controles de seguridad eficaces para permitir una segregación discreta y el control.	Para proteger los activos o datos de Barclays que se mantienen en los centros de datos, salas de datos e instalaciones de los proveedores (mantenidas por ellos o por terceros) frente a la pérdida, robo o daños derivados de los accesos no autorizados a áreas restringidas.
3. Protección contra amenazas físicas a infraestructuras y activos (TC 5.3)	La protección contra amenazas físicas a infraestructuras y activos deben diseñarse e implementarse mediante el despliegue de cámaras de seguridad, sistemas de detección de intrusos u otros controles de seguridad por capas adecuados para el entorno de amenazas existente y previsto. Se deben supervisar de manera continua las instalaciones para detectar accesos físicos no autorizados.	El establecimiento y el funcionamiento de controles de seguridad físicos acordes con las amenazas actuales y previstas limitarán o evitarán el impacto del acceso no autorizado, el robo o los daños intencionados a las instalaciones y los activos.

	Los equipos deben ubicarse en sitios seguros y protegidos. Los cables de electricidad, datos o servicios informáticos de apoyo deben estar protegidos contra intercepciones físicas, interferencias o daños. Los equipos e instalaciones de seguridad deben instalarse y mantenerse siguiendo las instrucciones del fabricante, y supervisarse para garantizar la disponibilidad, integridad y confidencialidad de la información. Los activos de Barclays mantenidos fuera de las instalaciones deben protegerse cuando estén en tránsito y estáticos. Los equipos deben instalarse y mantenerse correctamente y de acuerdo con los estándares del sector para garantizar la disponibilidad, integridad y confidencialidad de la información. La instalación y el funcionamiento de todos los sistemas de seguridad deben cumplir los requisitos legales y normativos vigentes. Cuando estén presentes, las zonas de entrega y carga deben estar debidamente controladas y aisladas de las instalaciones operativas para evitar el acceso no autorizado y la posible amenaza de entregas no verificadas.	

Este estándar debe leerse junto con el siguiente, cuyos controles de gestión aplicables deberán considerarse:

Obligación de control del proveedor de servicios de terceros (TPSPCO), requisitos de control de gestión: información, seguridad física y cibernética, tecnología, planificación de recuperación, privacidad y gestión de datos, PCI DSS y EUDA.