Obligaciones de control de proveedores externos

Seguridad física (controles técnicos o TC)

Versión 12.0 Octubre de 2022

Título del control	Descripción del control	Por qué es importante
1. Control de acceso (TC 5.1)	Se debe aplicar y gestionar un control electrónico, mecánico o digital de los accesos en todas las instalaciones que lleven a cabo determinadas actividades relativas a los contratos de Barclays. Todos los sistemas de seguridad deben instalarse, operarse y mantenerse de acuerdo con requisitos legales y normativos. 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 únicamente se expiden tras recibir la autorización correspondiente. Todos los accesos 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). Si es necesario trabajar en remoto cuando el proveedor o sus subcontratistas vayan a acceder, almacenar o tratar datos de Barclays de naturaleza restringida en formato físico o	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.

	electrónico (incluyendo datos personales o cualquier información sensible facilitada al proveedor por necesidad de conocimiento), el proveedor debe aprobar estas disposiciones con Barclays antes de permitir el acceso a estos datos.	
2. Sistemas de detección de intrusos y cámaras de seguridad (TC 5.2)	Deben instalarse sistemas de detección de intrusos (IDS) y cámaras de seguridad para disuadir, detectar, controlar e identificar los accesos inapropiados o las actividades delictivas. Deben instalarse equipos proporcionales a las amenazas de seguridad física existentes identificadas durante la actividad de evaluación de los riesgos de seguridad de cada instalación. Todos los sistemas de cámaras e IDS deben instalarse, utilizarse y mantenerse de acuerdo con los estándares actuales del sector (por ejemplo, la Organización Internacional de Normalización [ISO], el Control de sistemas y organizaciones [SOC], los requisitos legales y normativos vigentes, y las especificaciones actuales del fabricante). Deben establecerse procedimientos para garantizar que las alarmas de IDS y de las cámaras de seguridad se supervisen y gestionen de forma eficaz. El acceso al sistema de seguridad debe limitarse al personal autorizado.	Los IDS y sistemas de cámaras de seguridad forman parte de los controles estratificados para proteger las instalaciones de los accesos no autorizados y garantizar la seguridad de los activos. Salvo que dichos sistemas se instalen, operen y mantengan de forma efectiva, existe el riesgo de que se produzcan accesos no autorizados a las sedes y edificios que contengan activos y datos de Barclays, y que los intentos de acceso no autorizado no se detecten a tiempo.
3. Centros y salas de datos, e instalaciones de comunicaciones (TC 5.3)	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. Todos los centros de datos deben contar con controles técnicos, físicos y humanos estratificados así como con procedimientos específicos de la propia sede para proteger el	Para proteger los activos o datos de Barclays que se mantienen en los centros de datos, salas de datos y otros emplazamientos críticos similares frente a la pérdida, robo o daños derivados de los accesos no autorizados a áreas restringidas.

	perímetro, el edificio y la integridad de las salas de datos y de todas las demás áreas críticas. Estos controles incluyen, entre otros, cámaras de seguridad, sistemas de detección de intrusos, controles de los accesos y delegados de seguridad. Cuando las instalaciones se encuentran en ubicaciones compartidas, se debe implementar una seguridad eficaz en torno a su separación discreta.	

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.