# Obligaciones de control de proveedores externos

## Seguridad física

Versión 10.0 con fecha de octubre de 2020

| Título del control | Descripción del control | Por qué es importante |
|---|---|---|
| 1. Evaluación de los riesgos relacionados con la seguridad | Los proveedores se asegurarán de realizar evaluaciones de riesgos de seguridad para revisar las medidas y procesos de seguridad física. Las evaluaciones deben correr por cuenta de una persona con la experiencia o cualificación adecuada y tener en cuenta si los controles de seguridad física resultan apropiados y efectivos para mitigar tanto el perfil de amenazas actual como las cuestiones emergentes que puedan afectar a las instalaciones. La frecuencia de la actividad de evaluación de riesgos debe ser acorde a la finalidad y criticidad de la ubicación. Se espera que las instalaciones críticas para el funcionamiento de los procesos de Barclays (incluyendo los centros de datos) se evalúen como mínimo anualmente.<br><br>Las conclusiones de las evaluaciones de riesgos de seguridad deben documentarse, desarrollar planes de actuación y los problemas/riesgos identificados deben asignarse a un responsable, además de ser objeto de seguimiento hasta su conclusión.<br><br>Barclays deberá ser informado de todas las conclusiones relevantes en el plazo de 10 días hábiles desde su descubrimiento. | Las evaluaciones de riesgos de seguridad son un requisito clave para garantizar una evaluación precisa del entorno de seguridad física del proveedor, sus controles, sus procesos y su efectividad actual. Identificarán vulnerabilidades nuevas o ya existentes y lagunas de control para poder reducir el riesgo de pérdida o deterioro de los activos de Barclays y los daños para la reputación asociados y/o sanciones por incumplimiento de normativa o censura. |
| 2. Control de acceso | 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 al sistema debe restringirse al | El control de los accesos efectivo forma parte de los controles estratificados necesarios para proteger las instalaciones de los accesos no autorizados 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 |

| | | |
|---|---|---|
| | personal autorizado y el acceso a las claves y combinaciones debe gestionarse y controlarse de forma estricta.<br><br>Todas las credenciales de acceso deben gestionarse de manera efectiva para reducir el riesgo de accesos no autorizados. Todas las credenciales de acceso deberán gestionarse de conformidad con los procedimientos de control de acceso del proveedor. Las credenciales de acceso se expiden tras recibir la autorización correspondiente. Todos los accesos a áreas restringidas deben recertificarse a intervalos razonables. Si el acceso a las instalaciones o áreas restringidas ya no es necesario, las credenciales de acceso deben desactivarse en el plazo de 24 horas desde la notificación. | reputación y/o sanciones por incumplimiento de normativa o censura. |
| 3. Sistemas de detección de intrusos y cámaras de seguridad | 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 proporcionados 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, operarse y mantenerse de acuerdo con estándares industriales aceptados. El acceso al sistema 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. |
| 4. Personal de seguridad | Debe desplegarse personal de seguridad proporcionado a las amenazas de seguridad física existentes identificadas en cada instalación.<br><br>Todo el personal de seguridad (tanto si lo emplea el proveedor como el arrendador o un proveedor externo) debe emplearse o contratarse a través de un proveedor de servicios acreditado y con licencia de acuerdo con la legislación local. El personal debe recibir formación en seguridad proporcional a su función y responsabilidades. Toda la formación impartida debe documentarse y es preciso | El personal de seguridad forma parte de los controles estratificados para proteger las instalaciones de los accesos no autorizados y garantizar la seguridad de los activos. Salvo que se despliegue personal de seguridad de acuerdo con la amenaza de seguridad existente y que este reciba una formación adecuada, existe el riesgo de que se produzcan accesos no autorizados a las sedes que contengan activos y datos de Barclays, o de que estos no se detecten a tiempo. Esto podría aumentar el riesgo de pérdida o deterioro de los activos de Barclays, lo que provocaría pérdidas económicas y daños |

| | | |
|---|---|---|
| | mantener un registro de formación para todo el personal de seguridad. | asociados para la reputación y/o sanciones por incumplimiento de normativa o censura. |
| 5. Gestión de los incidentes de seguridad y niveles de respuesta | Los proveedores deberán contar con procedimientos para gestionar e investigar los incidentes relacionados con la seguridad cuando proceda. Si se ven afectados activos de Barclays, el incidente deberá declararse al banco en el plazo de 48 horas y los detalles de la investigación deberán compartirse en cuento resulte posible, pero siempre antes de que hayan transcurrido 10 días hábiles con respecto a la fecha del incidente. Esto debe incluir los datos de control de los accesos y las imágenes de las cámaras de seguridad, si procede, y en cumplimiento de las leyes y normativas locales. | Si este requisito no se implementa, Barclays no tendrá la seguridad de que el proveedor ha documentado y comprobado los procedimientos para gestionar los incidentes de seguridad. Esto podría llevar a tomar medidas inadecuadas a raíz de un incidente, lo cual aumentaría el riesgo de pérdida o deterioro de los activos o datos de Barclays, o daños a la reputación y/o sanciones por incumplimiento de normativa o censura. |
| 6. Transporte | Los proveedores deberán garantizar que todos los activos y los datos de Barclays se transportan de manera segura con controles proporcionales acordes al valor de los activos y datos en cuestión (tanto desde una perspectiva de daños económicos como para la reputación) y el entorno de amenazas en el que se esté produciendo el transporte. | Proteger los activos o datos de Barclays que deben ser transportados entre las sedes del proveedor y/o las del banco, a fin de reducir el riesgo de pérdidas, robo o deterioro, o daños a la reputación y/o sanciones por incumplimiento de normativa o censura. |
| 7. Centros y salas de datos | Todos los centros de datos independientes, localizados en un mismo lugar y de terceros, proveedores de servicios en la nube y salas de datos deben protegerse de forma segura para evitar los accesos no autorizados o daños en 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 perímetro, el edificio y la integridad de las salas de datos. Estos controles incluyen, entre otros, cámaras de | 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. |

| | | |
|---|---|---|
| | seguridad, sistemas de detección de intrusos y controles de los accesos. | |