# Obrigações de controlo de fornecedores externos

# Segurança física (controlos técnicos)

Versão 13.0 de setembro de 2023

| Designação do controlo | Descrição do controlo | Por que é importante |
|---|---|---|
| 1. Controlo de acesso (TC 5.1) | As regras de controlo de acesso devem ser definidas para todas as áreas seguras, apoiadas por procedimentos formais aprovados e responsabilidades definidas.<br><br>As áreas seguras devem ser protegidas por controlos de entrada e pontos de acesso adequados, utilizando um controlo de acesso eletrónico, mecânico ou digital.<br><br>O acesso lógico e administrativo aos sistemas de controlo de acesso eletrónico deve ser limitado ao pessoal autorizado e o acesso a chaves físicas e combinações deve ser estritamente gerido e controlado. Deve ser mantido um registo de auditoria de titulares de credenciais/chaves/combinações, abrangendo a concessão, alteração e revogação de permissões de acesso.<br><br>Todas as credenciais de acesso devem ser geridas de forma eficaz a fim de reduzir o risco de um acesso não autorizado. As credenciais de acesso devem ser geridas em linha com os procedimentos de controlo de acesso do fornecedor. As credenciais de acesso único podem ser emitidas apenas mediante a receção da aprovação adequada. Todas as credenciais de acesso a áreas restritas deve ser novamente certificado em intervalos de tempo adequados. Quando o acesso a instalações ou a áreas restritas já não for necessário, as credenciais de acesso têm de ser desativadas pela função responsável pela administração das credenciais de acesso no prazo de 24 horas após a receção da notificação da unidade de negócio ou função relevante a aconselhar sobre a alteração dos requisitos para o funcionário em questão (por ex., mudança de função ou responsabilidades, cessação ou emprego). | A manutenção de um sistema de controlo de acesso e de processos e procedimentos de gestão de acesso eficazes é um componente vital dentro da combinação em camadas de controlos necessários para proteger as instalações contra acesso não autorizado e garantir a segurança dos ativos. Se não estiverem em vigor medidas de controlo de acesso eficazes, existe o risco de pessoas não autorizadas entrarem nos locais ou áreas restritas dentro dos locais do fornecedor. Tal pode aumentar o risco de perda ou danos para os ativos do Barclays, provocando perdas financeiras e danos para a reputação associados e/ou censura ou coimas relacionadas com regulamentos. |

| | | |
|---|---|---|
| 2. Segurança de perímetros, edifícios e espaço (TC 5.2) | Devem ser definidos e implementados perímetros de segurança para proteger áreas que contenham informações e outros ativos associados, proporcionais ao ambiente de risco e ameaça identificado e antecipado. Deve ser concebida e implementada segurança física para escritórios, salas e instalações (incluindo sistemas de controlo de acesso, câmaras de segurança, sistemas de deteção de intrusos e outros controlos técnicos adequados) a partir de uma abordagem baseada no risco atendendo aos níveis de ameaça atuais e previstos e proporcionais aos processos empresariais empreendidos e ao valor da informação e dos ativos.<br><br>Devem ser concebidos e implementados processos de segurança para trabalhar em áreas seguras. É necessário definir e aplicar de forma adequada regras claras relativas a secretárias no que respeita a papéis e suportes de armazenamento amovíveis, bem como regras claras relativas a ecrãs para instalações de processamento de informações.<br><br>Todos os centros de dados, fornecedores na nuvem, salas de dados e instalações de comunicação independentes colocalizados e de terceiros (incluindo salas de servidores e armários de comunicação independentes) têm de ser eficazmente protegidos para evitar o acesso não autorizado e roubo ou danos aos ativos ou dados do Barclays. Quando as instalações estiverem em locais partilhados, devem ser implementados controlos de segurança eficazes para obter uma segregação e monitorização discretas. | Para proteger os ativos ou dados do Barclays retidos nos centros de dados, salas de dados e instalações do fornecedor (mantidos pelo fornecedor e terceiros) contra o risco de perda, danos ou furto resultantes de um acesso não autorizado a espaços restritos. |
| 3. Proteção contra ameaças físicas à infraestrutura e aos ativos (TC 5.3) | A proteção contra ameaças físicas à infraestrutura e aos ativos deve ser concebida e implementada através da colocação de câmaras de segurança, sistemas de deteção de intrusos e/ou outros controlos de segurança em vários níveis adequados ao ambiente de ameaça existente e previsto. As instalações devem ser permanentemente monitorizadas quanto a acesso físico não autorizado. | A implementação e operação de controlos de segurança física proporcionais às ameaças atuais e previstas limitará ou impedirá o impacto de acesso não autorizado, roubo ou danos intencionais nas instalações e nos ativos. |

| | | |
|---|---|---|
| | O equipamento tem de estar instalado de forma segura e protegido. Os cabos que transportam energia, dados ou serviços de informação de suporte devem estar protegidos de interceção física, interferência ou danos. Os equipamentos e instalações de segurança devem ser instalados e mantidos de acordo com os requisitos do fabricante e monitorizados para garantir a disponibilidade, integridade e confidencialidade das informações.<br><br>Os ativos do Barclays detidos fora do local têm de ser protegidos em depósito e em trânsito.<br><br>Os equipamentos devem ser instalados e mantidos corretamente e de acordo com as normas da indústria em vigor para garantir a disponibilidade, integridade e confidencialidade das informações. A instalação e o funcionamento de todos os sistemas de segurança têm de estar em conformidade com os requisitos legais e regulamentares vigentes.<br><br>Quando existentes, as áreas de entrega e carregamento devem ser devidamente controladas e isoladas das instalações operacionais para evitar o acesso não autorizado e a potencial ameaça de entregas não verificadas. | |

Esta norma deve ser lida em conjunto com a seguinte norma, devendo ser aplicados os controlos de gestão identificados como se enquadrando nesse âmbito:

**Obrigação de controlo de fornecedores de serviços terceiros (TPSPCO), Requisitos de controlos de gestão - Informações, segurança física e cibernética, tecnologia, planeamento de recuperação, privacidade de dados, gestão de dados, PCI DSS e EUDA.**