External Supplier Control Obligations

Segurança física

Versão 11.0 Datada de outubro de 2021

Designação do controlo	Descrição do controlo	Por que é importante
1. Avaliações de risco de segurança	Os fornecedores garantirão a realização de Avaliações de Segurança visando a identificação, avaliação e implementação de controlos, medidas e processos de segurança física. As avaliações têm de ser realizadas por uma pessoa devidamente experiente ou qualificada e terão de ter em conta a adequação e eficiência dos controlos de segurança física a fim de mitigar o atual perfil de ameaça do edifício e quaisquer outras questões emergentes que posam afetar o local. A frequência da atividade de avaliação do risco deve estar em linha com a finalidade e criticidade do local. Espera-se que os locais críticos para a execução dos processos do Barclays (incluindo Centros de dados) sejam avaliados, pelo menos, anualmente. As conclusões da Avaliação do risco de segurança têm de ser documentadas, os planos de ação têm de ser elaborados e os problemas/riscos identificados têm de ser atribuídos a um responsável e rastreados até à respetiva conclusão. O Barclays será informado de todas as conclusões significativas num prazo de 10 dias úteis após a respetiva descoberta.	As Avaliações do risco de segurança são um requisito crucial para garantir uma avaliação rigorosa do ambiente de segurança física, controlos e processos do fornecedor e respetiva eficácia atual. As avaliações identificarão vulnerabilidades e lacunas de controlo novas ou existentes e reduzirão o risco de perdas ou danos para os ativos do Barclays, danos para a reputação associados e/ou coimas relacionadas com regulamentos ou censura.
2. Controlo do acesso	Serão implementados e geridos controlos eletrónicos, mecânicos ou digitais em todas as instalações que realizam atividades no âmbito de contratos celebrados com o Barclays. Todos os sistemas de segurança devem ser instalados, operados e mantidos em conformidade com os requisitos legais e regulamentares. O acesso ao sistema tem	Um controlo de acessos eficaz faz parte integral da camada de controlos necessários para proteger as instalações contra acessos não autorizados 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

	de ser limitado ao pessoal autorizado e o acesso às chaves e códigos deve ser gerido e controlado de forma rigorosa. 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 são emitidas mediante a receção da aprovação adequada. Todo o acesso a áreas restritas deve ser novamente certificado em intervalos de tempo adequados. Sempre que o acesso a instalações ou áreas restritas já não seja necessário, deve proceder-se à desativação das credenciais de acesso num prazo de 24 horas após a notificação. Caso seja exigido trabalho remoto em que o fornecedor ou os seus subcontratantes acederão, armazenarão ou processarão informação Barclays, na forma física ou virtual que, por natureza, é restrita (incluindo dados pessoais ou qualquer informação sensível disponibilizada ao fornecedor em função da necessidade de tomar conhecimento), o Fornecedor tem de aprovar estas disposições com o Barclays antes de permitir o acesso a estes dados.	danos para os ativos ou dados do Barclays associados a danos para a reputação e/ou coimas relacionadas com regulamentos/censura.
3. Sistemas de deteção de intrusos e câmaras de segurança	Devem ser instalados Sistemas de deteção de intrusos (SDI) e câmaras de segurança para dissuadir, detetar, monitorizar e identificar quaisquer acessos indevidos ou atividades criminosas. O equipamento deve ser instalado de forma proporcional às ameaças correntes à segurança física identificadas durante a atividade de Avaliação do risco de segurança para cada local. Todos os sistemas de câmaras e SDI devem ser instalados, operados e mantidos em conformidade com os padrões do setor aceites. O acesso ao sistema tem de ser limitado ao pessoal autorizado.	Os SDI e sistemas de câmaras de segurança fazem parte integral da camada de controlos para proteger as instalações contra acessos não autorizados e garantir a segurança dos ativos. Se estes sistemas não forem devidamente instalados, operados e mantidos, existe risco de acesso não autorizado a locais e edifícios que contenham ativos e dados do Barclays e de que os acessos não autorizados não sejam detetados atempadamente.

4. Pessoal de segurança	O pessoal de segurança é destacado de forma proporcional às ameaças correntes à segurança física para cada local. Todo o pessoal de segurança (contratado pelo fornecedor, por um senhorio ou por um fornecedor externo) tem de ser contratado através de um prestador de serviços acreditado e licenciado, nos termos da legislação local. O pessoal tem de receber formação sobre segurança proporcional às suas funções e responsabilidades. Toda a formação prestada tem de ser documentada, devendo manter-se um registo da formação relativo a todo o pessoal de segurança.	O pessoal de segurança faz parte integral da camada de controlos para proteger as instalações contra acessos não autorizados e garantir a segurança dos ativos. Se não for destacado pessoal de segurança em linha com as ameaças correntes à segurança e se este pessoal não receber formação adequada, poderá ocorrer acesso não autorizado a locais que contenham ativos e dados do Barclays ou os acessos não autorizados poderão não ser detetados atempadamente. Tal pode aumentar o risco de perda ou danos para os ativos ou dados do Barclays associados a danos para a reputação e/ou coimas relacionadas com regulamentos/censura.
5. Gestão de incidentes de segurança e níveis de resposta	Os fornecedores devem implementar procedimentos de gestão de incidentes de segurança e levar a cabo investigações sempre que necessário. Sempre que os ativos do Barclays forem afetados, o incidente deve ser reportado ao Barclays num prazo de 48 horas e os relatórios formais e detalhes da investigação devem ser partilhados o mais rapidamente possível, mas nunca depois de mais de 10 dias úteis após o incidente. Tal deve incluir dados de controlo de acesso e imagens do sistema de câmaras de segurança sempre que adequado e em conformidade com as leis e regulamentos locais.	Se esta exigência não for cumprida, o Barclays poderá não conseguir certificar-se de que o fornecedor dispõe de procedimentos adequadamente robustos e documentados para a gestão dos incidentes de segurança. Tal pode levar à adoção de medidas inadequadas no seguimento de um incidente, aumentando o risco de perda ou danos para os ativos ou dados do Barclays associados a danos para a reputação e/ou coimas relacionadas com regulamentos/censura.
6. Transporte	Os fornecedores garantirão que todos os ativos e Dados do Barclays são transportados de forma segura, com a implementação de controlos proporcionais ao valor dos ativos e dos bens transportados (numa perspetiva que abranja os danos financeiros e danos para a reputação), e tendo em conta o ambiente de ameaça nos quais são transportados.	Para proteger os ativos ou dados do Barclays em trânsito entre instalações do fornecedor e/ou do Barclays, reduzindo o risco de perda, furto ou danos e danos para a reputação associados e/ou coimas relacionadas com regulamentos/censura.
7. Centros e salas de dados	Todos os centros de dados, fornecedores de serviços de nuvem e salas de dados independentes, de utilização partilhada e de terceiros são eficazmente protegidos a fim de prevenir um acesso não autorizado e furtos ou danos a ativos	Para proteger os ativos ou dados do Barclays retidos nos centros de dados, salas de dados e locais críticos semelhantes contra o risco de perda, danos ou furto resultantes de um acesso não autorizado a espaços restritos.

	ou dados do Barclays. Todos os centros de dados possuem controlos técnicos, físicos e humanos por camadas e procedimentos específicos para os locais para proteger de forma eficaz os perímetros, edifícios e integridade das salas de dados e todas as demais áreas críticas. Os controlos incluem, entre outros, câmaras de segurança, sistemas de deteção de intrusos, controlo de acesso e responsáveis pela segurança.	