Obblighi di controllo dei Fornitori esterni

Sicurezza fisica (controlli tecnici)

Versione 12.0, ottobre 2022

Titolo del controllo	Descrizione del controllo	Perché è importante
1. Controllo degli accessi (TC 5.1)	Il controllo degli accessi elettronici, meccanici o digitali deve essere implementato e gestito in tutte le sedi in cui si svolgono attività associate ai contratti Barclays. Tutti i sistemi di sicurezza devono essere installati, gestiti e mantenuti conformemente ai requisiti legali e normativi. L'accesso logico e amministrativo ai sistemi di controllo degli accessi elettronici deve essere limitato al personale autorizzato, gestendo e controllando rigorosamente l'accesso alle chiavi e alle combinazioni fisiche. È necessario mantenere una traccia di audit dei possessori di credenziali, chiavi e combinazioni, che copra la concessione, la modifica e la revoca delle autorizzazioni di accesso. Tutte le credenziali di accesso devono essere gestite in modo efficace al fine di ridurre il rischio di accesso non autorizzato. Le credenziali di accesso devono essere gestite in linea con le procedure di controllo degli accessi del Fornitore. Le credenziali di accesso possono essere rilasciate solo al ricevimento dell'approvazione corrispondente. Tutti gli accessi alle aree riservate devono essere ricertificati a intervalli adeguati. Laddove non sia più necessario l'accesso a un locale o a un'area limitata, le credenziali di accesso devono essere disattivate dalla funzione responsabile dell'amministrazione delle credenziali di accesso entro 24 ore dalla ricezione della notifica da parte della business unit o della funzione che comunica il cambiamento dei requisiti per il dipendente in questione (ad esempio, cambio di ruolo o responsabilità, licenziamento o assunzione). Se è necessario utilizzare modalità di lavoro remoto per le attività in cui il Fornitore o i suoi subappaltatori memorizzano, elaborano o accedono alle informazioni	Il mantenimento di un sistema di controllo degli accessi efficace, oltre che di processi e procedure appropriati per la gestione degli accessi, svolge un ruolo essenziale nell'ambito della combinazione dei controlli multilivello necessari per proteggere i locali dall'accesso non autorizzato e per garantire la sicurezza degli asset. Se non vengono adottate efficaci misure di controllo dell'accesso, esiste il rischio di accesso non autorizzato alle sedi del Fornitore o alle aree riservate all'interno di tali sedi. Ciò può incrementare il rischio di perdita o danneggiamento degli asset di Barclays, generando potenziali perdite economiche, danni reputazionali e/o sanzioni amministrative o richiami ufficiali.

	riservate di Barclays, in forma fisica o virtuale (compresi i dati personali o qualsiasi informazione sensibile che viene trasmessa al Fornitore sulla base della necessità di conoscere), il Fornitore deve approvare le disposizioni con Barclays prima di consentire l'accesso a tali dati.	
2. Sistemi di rilevamento delle intrusioni e telecamere di sicurezza (TC 5.2)	Devono essere installati e utilizzati sistemi di rilevamento delle intrusioni (IDS, Intruder Detection System) e telecamere di sicurezza al fine di scoraggiare, rilevare, monitorare e identificare gli accessi inappropriati o le attività illegali. È necessario utilizzare apparecchiature commisurate alle minacce fisiche prevalenti per la sicurezza identificate durante la valutazione dei rischi per la sicurezza di ogni sede. Tutti i sistemi di telecamere e IDS devono essere installati, utilizzati e sottoposti a manutenzione conformemente agli attuali standard di settore, ad esempio ISO (International Organization for Standardization), SOC (System and Organisation Control), requisiti legali e normativi prevalenti e specifiche correnti del produttore. Devono essere adottate procedure con lo scopo garantire che gli allarmi IDS e le telecamere di sicurezza siano monitorati e gestiti in modo efficace. L'accesso al sistema di sicurezza deve essere limitato al personale autorizzato.	I sistemi IDS e le telecamere di sicurezza fanno parte dei controlli multilivello utilizzati per proteggere i locali dall'accesso non autorizzato e per garantire la sicurezza degli asset. Se questi sistemi non sono correttamente installati, gestiti, monitorati e sottoposti a manutenzione, esiste il rischio di accesso non autorizzato alle sedi e agli edifici che ospitano gli asset e i dati di Barclays, e tale accesso non autorizzato potrebbe non essere rilevato tempestivamente.
3. Data center, sale e sistemi di comunicazione (TC 5.3)	Tutti i data center indipendenti, in co-location e di terze parti, i provider di servizi cloud, le sale dati e i sistemi di comunicazione (incluse le sale server e gli armadietti di comunicazione standalone) devono essere protetti in modo efficace per evitare l'accesso non autorizzato, così come furti o danni agli asset o ai dati di Barclays. Tutti i data center devono essere dotati di controlli multilivello di tipo tecnico, fisico e presidiato, oltre che di procedure specifiche della sede con lo scopo di proteggere efficacemente il perimetro, l'edificio e l'integrità delle sale dati e di	Per proteggere i beni e i dati di Barclays conservati all'interno di data center, sale dati e luoghi critici simili dal rischio di perdita, danneggiamento o furto derivante dall'accesso non autorizzato a spazi riservati.

	tutte le altre aree critiche. I controlli includono, a titolo esemplificativo, telecamere di sicurezza, sistemi di rilevamento delle intrusioni, controllo degli accessi e addetti alla sicurezza. Se le installazioni si trovano in aree condivise, è necessario implementare una protezione efficace intorno alla relativa separazione discreta.	

Il presente Standard deve essere letto unitamente allo Standard indicato di seguito, che prevede l'applicazione dei controlli di gestione identificati come inclusi nell'ambito:

Obblighi di controllo per provider di servizi esterni (TPSPCO), Requisiti di controllo della gestione - Informazioni, Sicurezza informatica e fisica, Tecnologia, Pianificazione del ripristino, Riservatezza dei dati, Gestione dei dati, PCI DSS ed EUDA.