Obblighi di controllo dei Fornitori esterni

Sicurezza fisica (controlli tecnici)

Versione 14.0, ottobre 2024

Titolo del controllo	Descrizione del controllo	Perché è importante
1. Controllo degli accessi (TC 5.1)	Le regole inerenti al controllo degli accessi devono essere definite per tutte le aree sicure, nonché supportate da procedure formali approvate, con le relative responsabilità ben evidenziate. Le aree sicure devono essere protette per mezzo di efficaci controlli degli ingressi e mediante adeguati punti di accesso, ricorrendo all'utilizzo di dispositivi elettronici, meccanici o digitali. 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 univoche possono essere rilasciate solo al ricevimento dell'approvazione corrispondente. Tutte le credenziali utilizzate per l'accesso alle aree riservate devono essere ricertificate 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	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.

	esempio, cambio di ruolo o responsabilità, licenziamento o assunzione).	
2. Sicurezza di perimetri, edifici e spazi (TC 5.2)	Per proteggere le aree che custodiscono informazioni e altri asset associati, devono essere definiti e implementati appositi perimetri di sicurezza, in modo commisurato al contesto di rischio e minaccia identificato e previsto. La sicurezza fisica relativamente a uffici, locali e strutture (compresi i sistemi di controllo degli accessi, le telecamere di sicurezza, i sistemi di rilevamento delle intrusioni e altri controlli tecnici appropriati) deve essere progettata e implementata adottando un approccio basato sul rischio esistente e correlato agli effettivi livelli di pericolosità attuali e previsti, e deve essere inoltre commisurata ai processi aziendali intrapresi e al valore delle informazioni e degli asset. Devono essere progettati e implementati specifici processi di sicurezza per lo svolgimento delle attività lavorative nelle aree sicure. Devono essere inoltre definite e adeguatamente applicate chiare regole riguardo alle scrivanie, in relazione ai documenti e ai supporti di archiviazione rimovibili. Occorrono altresì regole ben definite relativamente agli schermi presenti nelle strutture adibite all'elaborazione delle informazioni. 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. Se le installazioni si trovano in aree condivise, è necessario implementare efficaci controlli di sicurezza atti a garantire una separazione e un monitoraggio improntati alla discrezione.	Per proteggere gli asset o i dati di Barclays custoditi nei data center, nelle sale dati e nelle sedi dei Fornitori (sia gestiti dal Fornitore stesso che riconducibili a terze parti) dal rischio di perdita, danneggiamento o furto derivante dall'accesso non autorizzato a spazi riservati.
3. Protezione dalle minacce fisiche all'infrastruttura e agli asset (TC 5.3)	La protezione dalle minacce fisiche all'infrastruttura e agli asset deve essere progettata e implementata attraverso l'installazione di telecamere di sicurezza, sistemi di rilevamento delle intrusioni e/o altri controlli di sicurezza	L'implementazione e l'utilizzo di appropriati controlli inerenti alla sicurezza fisica, commisurati agli effettivi livelli di pericolosità attuali e previsti, limiteranno o preverranno l'impatto esercitato da eventuali

	multilivello, che risultino appropriati in relazione all'ambiente in cui si possono manifestare le minacce prevalenti e previste. I locali devono essere costantemente monitorati per prevenire e individuare eventuali presenze dovute ad accessi fisici non autorizzati. Le apparecchiature devono essere posizionate in modo sicuro e protette. I cavi che trasportano l'alimentazione elettrica, i dati o i servizi informativi di supporto devono essere protetti da intercettazioni, interferenze o danni fisici. Le apparecchiature e i sistemi di sicurezza devono essere installati e sottoposti a manutenzione in conformità con i requisiti indicati dal produttore, e opportunamente monitorati per garantire la disponibilità, l'integrità e la riservatezza delle informazioni. Gli asset di Barclays conservati fuori sede devono essere protetti sia durante i periodi di inattività, sia durante il trasporto. Le apparecchiature devono essere installate e sottoposte a manutenzione in modo corretto e secondo gli standard di settore prevalenti, per garantire la disponibilità, l'integrità e la riservatezza delle informazioni. L'installazione e il funzionamento di tutti i sistemi di sicurezza devono risultare conformi ai requisiti legali e normativi prevalenti. Ove presenti, le aree di consegna e carico devono essere adeguatamente controllate e isolate dalle strutture operative per evitare accessi non autorizzati e potenziali minacce derivanti da consegne non verificate.	accessi non autorizzati, furti o danneggiamenti intenzionali a locali e asset.

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.