Obblighi di controllo dei Fornitori esterni

Sicurezza fisica

Versione 10.0 ottobre 2020

Titolo di controllo	Descrizione del controllo	Perché è importante?
1. Valutazione dei rischi sotto il profilo della sicurezza	I fornitori devono aver cura di eseguire le Valutazioni dei Rischi concernenti la Sicurezza al fine di controllare le misure e le procedure riguardanti la sicurezza fisica. Le valutazioni devono essere eseguite da una persona adeguatamente esperta o qualificata, e devono considerare l'adeguatezza e l'efficacia dei controlli fisici di sicurezza per ridurre sia l'attuale profilo di rischio dell'edificio che eventuali problemi emergenti che possono avere un impatto sul sito. La frequenza dell'attività di valutazione del rischio deve essere in linea con lo scopo e la criticità del luogo. Si prevede che i siti critici per il funzionamento dei processi Barclays (compresi i Data Center) saranno valutati almeno annualmente. I risultati della Valutazione dei rischi per la sicurezza devono essere documentati, devono essere sviluppati gli opportuni piani d'azione e i problemi/rischi identificati devono essere assegnati a un responsabile e tracciati fino alla loro risoluzione. Barclays deve essere informata di tutti i risultati significativi entro 10 giorni lavorativi dalla scoperta.	Le valutazioni dei rischi per la sicurezza sono un requisito fondamentale per fornire una valutazione accurata dell'ambiente, dei controlli e dei processi relativi alla sicurezza fisica del Fornitore e della loro reale efficacia. Ciò consente di individuare i punti deboli e le carenze nei controlli esistenti o nuovi, nonché di ridurre il rischio di perdita o danneggiamento dei beni Barclays e di danni correlati alla reputazione e/o sanzioni o richiami ufficiali.
2. Controllo degli accessi	Il controllo degli accessi elettronici, meccanici o digitali deve essere implementato e gestito in tutte le sedi in cui si svolgono attività relative ai contratti Barclays. Tutti i sistemi di sicurezza devono essere installati, gestiti e mantenuti conformemente ai requisiti legali e normativi. L'accesso al sistema deve essere limitato al personale autorizzato e l'accesso alle chiavi e alle combinazioni deve essere rigorosamente gestito e controllato.	Un controllo efficace degli accessi fa parte dei controlli a più livelli necessari per proteggere i locali da accessi non autorizzati e per garantire la sicurezza dei beni. A meno che non siano in atto efficaci misure di controllo dell'accesso, esiste il rischio che personale non autorizzato possa entrare nei siti del Fornitore o nelle aree riservate all'interno dei suoi siti. Ciò può incrementare il rischio di perdite o danneggiamento dei beni di Barclays, generando perdite finanziarie e danni correlati alla reputazione e/o sanzioni o richiami ufficiali.

	Tutte le credenziali di accesso devono essere gestite in modo efficace per 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 vengono rilasciate al ricevimento dell'apposita approvazione. Tutti gli accessi alle aree riservate devono essere ricertificati ad intervalli adeguati. Se l'accesso a un locale o a un'area riservata non è più necessario, le credenziali di accesso devono essere disattivate entro 24 ore dalla notifica.	
3. Sistemi di rilevamento delle intrusioni e telecamere di sicurezza	Devono essere installati e utilizzati sistemi di rilevamento degli intrusi (Intruder Detection Systems - IDS) e telecamere di sicurezza per scoraggiare, rilevare, monitorare e identificare accessi impropri o attività illegali. Le apparecchiature devono essere impiegate in modo proporzionato alle minacce fisiche prevalenti per la sicurezza identificate durante l'attività di valutazione dei rischi per la sicurezza di ogni località. Tutti i sistemi di videosorveglianza e IDS devono essere installati, gestiti e mantenuti conformemente agli standard di settore accettati. L'accesso al sistema deve essere limitato al personale autorizzato.	I sistemi IDS e le telecamere di sicurezza fanno parte dei controlli a più livelli per proteggere i locali da accessi non autorizzati e per garantire la sicurezza dei beni. A meno che questi sistemi non siano installati, gestiti e sottoposti a manutenzione in modo efficace, esiste il rischio di accesso non autorizzato ai siti e agli edifici contenenti beni e dati Barclays e che tale accesso non autorizzato non sia rilevato tempestivamente.
4. Personale addetto alla sicurezza	Il personale addetto alla sicurezza deve essere impiegato in modo proporzionato alle minacce fisiche prevalenti di ciascuna località. Tutto il personale addetto alla sicurezza (sia esso impiegato dal fornitore, dal proprietario dell'immobile o da un fornitore esterno) deve essere assunto o contrattualizzato tramite un fornitore di servizi accreditato e autorizzato conformemente alla legislazione locale. Il personale deve ricevere una formazione in materia di sicurezza commisurata al proprio ruolo e alle proprie responsabilità. Tutta la formazione erogata deve essere documentata e deve essere tenuto un	Il personale addetto alla sicurezza rientra nei controlli a più livelli per proteggere i locali da accessi non autorizzati e per garantire la sicurezza dei beni. A meno che il personale addetto alla sicurezza non sia impiegato in linea con la minaccia alla sicurezza prevalente e adeguatamente addestrato, potrebbe verificarsi, o potrebbe non essere rilevato in modo tempestivo, l'accesso non autorizzato a siti contenenti risorse e dati di Barclays. Ciò può incrementare il rischio di perdite o danneggiamento dei beni di Barclays, generando perdite finanziarie e danni correlati alla reputazione e/o sanzioni o richiami ufficiali.

	registro della formazione per tutto il personale addetto alla sicurezza.	
5. Gestione degli incidenti relativi alla sicurezza e livelli di risposta	I fornitori devono implementare procedure di gestione degli incidenti relativi alla sicurezza e svolgere le dovute indagini se necessario. In caso di impatto sui beni di Barclays, l'incidente deve essere segnalato a Barclays entro 48 ore e le relazioni ufficiali e i dettagli delle indagini devono essere condivisi il prima possibile, ma non oltre 10 giorni lavorativi dopo l'incidente. Sono inclusi i dati di controllo degli accessi e le immagini delle telecamere di sicurezza, ove opportuno e in linea con le leggi e i regolamenti locali.	In caso di mancato adempimento, è possibile che Barclays non possa avere la certezza che il Fornitore abbia adottato procedure documentate adeguate per gestire gli incidenti relativi alla sicurezza. Ciò può condurre ad adottare misure non appropriate in caso di incidenti, aumentando il rischio di perdite o danneggiamento dei beni o dei dati Barclays, danneggiamento correlato della reputazione e/o sanzioni o richiami ufficiali.
6. Trasporto	I Fornitori devono accertarsi che tutti i beni e i dati di Barclays siano trasportati in modo sicuro con controlli proporzionati al valore dei beni e dei dati movimentati (sia dal punto di vista finanziario che del danno alla reputazione) e al contesto di rischio in cui vengono trasportati.	Per proteggere i beni e i dati di Barclays in transito tra il sito del Fornitore e/o il sito di Barclays, riducendo il rischio di perdite, furti e danni, danneggiamento correlato della reputazione e/o sanzioni o richiami ufficiali.
7. Data Center e sale	Tutti i data center, i fornitori di cloud e le sale dati indipendenti, co-locati e di terze parti sono efficacemente protetti per prevenire l'accesso non autorizzato e il furto o il danneggiamento di beni o dati di Barclays. Tutti i data center devono essere dotati di controlli tecnici, fisici e presidiati a più livelli e di procedure specifiche del sito per proteggere efficacemente il perimetro, l'edificio e l'integrità delle sale dati. I controlli includono, a titolo esemplificativo, telecamere di sicurezza, sistemi di rilevamento delle intrusioni e controllo degli accessi.	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.