External Supplier Control Obligation

Sicurezza Informatica e Cibernetica (ICS)

Versione 11.0 ottobre 2021

Area di controllo / Titolo	Descrizione del controllo	Perché è importante?
1. Quadro di Governance per la Sicurezza Informatica / Cibernetica	Il Fornitore deve avere una struttura standard di settore consolidata e coerente per la governance della Sicurezza Informatica e Cibernetica conformemente alle Migliori Prassi del Settore (i migliori programmi di settore attuali includono NIST, ISO/IEC 27001, ITIL, COBIT) e a qualsiasi requisito di settore applicabile. Questo permetterà al Fornitore di garantire che sono in essere misure di salvaguardia o contromisure per i rispettivi processi, tecnologie e ambienti fisici. Un programma ben strutturato di governance delle informazioni a livello aziendale deve garantire che i concetti fondamentali di disponibilità, integrità e riservatezza siano supportati da controlli adeguati progettati per mitigare o ridurre i rischi di perdita, interruzione o corruzione delle informazioni e il Fornitore deve garantire che i controlli dei requisiti di Barclays siano in atto e funzionino efficacemente per proteggere i servizi di Barclays. Il Quadro di Governance per la Sicurezza deve essere sviluppato, documentato, approvato e implementato, utilizzando misure di sicurezza amministrative, organizzative, tecniche e fisiche per proteggere i beni e i dati da perdita, uso improprio, accesso, divulgazione, alterazione e distruzione non autorizzati. Il programma di sicurezza deve includere, a titolo esemplificativo, le seguenti aree: • Politica, procedure e programma standard finalizzati alla reale creazione, implementazione e costante misurazione dell'efficacia della politica per la Sicurezza Informatica e Cibernetica e dell'applicazione dei relativi standard. • Un programma di sicurezza completo con una chiara struttura di leadership, un meccanismo di escalation e una supervisione esecutiva per creare una cultura di responsabilità e consapevolezza per la sicurezza. • Politiche, procedure e processi che vengono approvati e comunicati in tutta l'organizzazione. • Accertarsi che le politiche e le procedure/gli standard in materia di Sicurezza Informatica e Cibernetica siano rivisti regolarmente (almeno una volta all'anno o in caso di modifiche sostanziali) e adattati secondo le attuali pratiche di Sicurezza Informatica e il mutevole panorama delle minacce. • Il Fornitore deve garantire l'assegnazione della responsabilità individuale per le informazioni e i sistemi di sicurezza, assicurando che esista un'adeguata proprietà degli ambienti aziendali, delle informazioni e dei sistemi di sicurezza critici e che questa sia assegnata a persone capaci.	In caso di mancata attuazione di questo principio, Barclays o i propri Fornitori potrebbero non avere e non essere in grado di dimostrare di disporre di una supervisione adeguata in materia di Sicurezza Informatica/Cibernetica. Un solido quadro di governance della sicurezza definisce il livello di sicurezza per l'intera organizzazione.

	• Il Fornitore coordina e allinea ruoli e responsabilità per il personale, implementando, gestendo e supervisionando l'efficacia della strategia e dello schema di sicurezza con partner interni ed esterni. • Il Fornitore è tenuto ad implementare un'infrastruttura sicura e un quadro di controllo per proteggere l'organizzazione da qualsiasi minaccia (inclusa la Sicurezza Informatica) • Revisioni e valutazioni a cura di esperti indipendenti devono essere eseguite almeno una volta all'anno per garantire che l'organizzazione affronti le non conformità delle politiche, degli standard, delle procedure e degli obblighi di conformità stabiliti. **Nel caso in cui il Fornitore sia soggetto a fusione, acquisizione o qualsiasi altro cambiamento di proprietà, il Fornitore si impegna a informare Barclays (per iscritto) non appena sia legalmente in grado di farlo.**	
2. Gestione dei rischi di sicurezza	Il Fornitore deve stabilire un programma di gestione dei rischi di sicurezza che valuti, attenui e monitori efficacemente i mutevoli rischi per la sicurezza in tutto l'ambiente controllato dal Fornitore. Il programma di gestione dei rischi deve includere, a titolo esemplificativo, le seguenti aree: • il Fornitore deve disporre di un quadro di gestione dei rischi per la Sicurezza approvato dall'autorità governativa competente (ad esempio, il Consiglio di amministrazione o uno dei suoi comitati). Il piano di gestione deve essere integrato nella strategia aziendale complessiva e nel quadro di gestione dei rischi. • Allineate al quadro dei rischi, le valutazioni formali dei rischi devono essere eseguite almeno una volta all'anno o a intervalli pianificati, o essere attivate in base agli eventi, ad esempio in risposta a un incidente o alle lezioni apprese ad esso associate (e in combinazione con eventuali modifiche ai sistemi informativi) per determinare la probabilità e l'impatto di tutti i rischi identificati utilizzando metodi qualitativi e quantitativi. La probabilità e l'impatto associati al rischio intrinseco e residuo sono determinati in modo indipendente, considerando tutte le categorie di rischio (ad esempio, risultati di audit, analisi delle minacce e delle vulnerabilità e conformità normativa). • Selezionare le opzioni appropriate per il trattamento dei rischi legati alla sicurezza, tenendo conto dei risultati della valutazione del rischio.	Se questo controllo non viene implementato, i Fornitori potrebbero non essere in grado di dimostrare le misure appropriate messe in atto per gestire i rischi di sicurezza.

	• Formulare un piano di trattamento dei rischi legati alla sicurezza e i criteri di accettazione del rischio attraverso persone adeguatamente qualificate e responsabili. Tali criteri dovrebbero includere, a titolo esemplificativo ma non esaustivo, la sensibilità di tali dati e la loro criticità aziendale. • Il Fornitore deve garantire che i rischi identificati nell'ambiente siano minimizzati o eliminati attraverso l'assegnazione delle priorità di rischio e l'implementazione di misure di protezione. • I rischi dovrebbero essere mitigati a un livello accettabile. I livelli di accettazione basati su criteri di rischio devono essere stabiliti e documentati in base a tempi di risoluzione ragionevoli e all'approvazione delle parti interessate. • Le valutazioni del rischio associate ai requisiti di governance dei dati devono tenere conto di quanto segue: o Classificazione e protezione dei dati da uso non autorizzato, divulgazione, accesso, perdita, distruzione, alterazione e falsificazione. o Consapevolezza dell'ambiente in cui i dati sensibili vengono memorizzati e trasmessi attraverso applicazioni, database, server e infrastrutture di rete. o Rispetto dei periodi di conservazione definiti e dei requisiti di smaltimento a fine vita. • Il Fornitore deve effettuare almeno una valutazione annuale dei rischi per la sicurezza e, sulla base degli ambienti specifici, prendere in considerazione una cadenza più frequente. **Se il Fornitore non è in grado di rimediare o ridurre le aree di rischio sostanziale che potrebbero avere un impatto sui Dati di Barclays e/o sul servizio fornito a Barclays, deve fare un resoconto e darne comunicazione a Barclays.**	
3. Ruoli e responsabilità	Il Fornitore deve garantire che tutti gli individui che sono coinvolti nella fornitura di servizi a Barclays siano a conoscenza dei requisiti di controllo di Barclays di cui al presente documento e vi aderiscano. Secondo i requisiti di controllo di Barclays, il Fornitore deve garantire che un team di specialisti e/o individui con competenze adeguate, con ruoli e responsabilità definiti per la gestione dei requisiti di controllo di Barclays, sia creato e operi efficacemente per proteggere i servizi di Barclays. Il Fornitore deve definire e comunicare i ruoli e le responsabilità per tutti i domini di sicurezza interessati dai requisiti di controllo. Questi devono essere rivisti regolarmente (e in ogni caso almeno una volta all'anno) e dopo ogni modifica rilevante del modello	La chiara definizione dei ruoli e delle responsabilità supporta l'attuazione della procedura SCO per la Sicurezza Informatica e Cibernetica

	operativo o dell'attività del Fornitore. I ruoli principali devono comprendere un senior executive, responsabile della Sicurezza Informatica e Cibernetica. È responsabilità del Fornitore assicurarsi che i propri dipendenti/il proprio personale conoscano e rispettino i requisiti di controllo di questo standard e le politiche e gli standard associati. Il Fornitore deve nominare un punto di contatto per l'eventuale escalation che tenga i rapporti con Barclays.	
4. Uso approvato	Il Fornitore è tenuto a redigere e divulgare i Requisiti di uso accettabile, informando tutti i propri dipendenti delle loro responsabilità (compresi gli appaltatori e gli utenti terzi dei sistemi dell'organizzazione). È necessario considerare i seguenti aspetti: • Uso di Internet; • Uso del software come servizio (SaaS); • Uso degli archivi del Codice Pubblico; • Utilizzo di plugin basati su browser e freeware / shareware; • Uso dei Social Media; • Uso di e-mail aziendali; • Uso di messaggistica istantanea; • Uso di apparecchiature fornite dal Fornitore; • Uso di apparecchiature non fornite dal Fornitore (ad es. portare il proprio dispositivo); • Uso di dispositivi di archiviazione portatili/rimovibili; • Responsabilità nella gestione, nel salvataggio e nella conservazione del Patrimonio di dati di Barclays; • Elaborazione dei canali di perdita dati; e • Rischi e conseguenze dell'uso improprio delle suddette voci e/o qualsiasi risultato illegale, dannoso o offensivo derivante da tale uso improprio. Il Fornitore deve adottare misure adeguate atte ad assicurare la conformità ai requisiti di uso accettabile.	I requisiti di uso accettabile aiutano a rafforzare l'ambiente di controllo per la protezione dei Patrimoni di Dati
5. Formazione e consapevolezza	Il Fornitore deve aver istituito un programma di formazione per l'educazione e la sensibilizzazione in materia di sicurezza per tutti i dipendenti, gli appaltatori e gli utenti terzi dei sistemi dell'organizzazione e renderlo obbligatorio, se del caso. Tutti i soggetti che hanno accesso a dati/informazioni Barclays devono ricevere un'adeguata formazione per l'educazione e la sensibilizzazione e aggiornamenti periodici sulle	Formazione e consapevolezza supportano tutti gli altri controlli nell'ambito di questo programma.

	procedure tecniche e organizzative, i processi e le politiche relativi alla loro funzione professionale nell'ambito dell'organizzazione. I livelli di educazione, formazione e sensibilizzazione devono essere commisurati ai ruoli svolti e registrati su una piattaforma di gestione dell'apprendimento idonea. Il Fornitore deve garantire che, entro un mese dall'ingresso nell'organizzazione, tutto il personale sotto il proprio controllo intraprenda una formazione obbligatoria sulle informazioni di sicurezza (costantemente aggiornata per compensare l'evoluzione delle minacce e dei rischi specifici del settore), che comprenda le Migliori Prassi del Settore e di protezione dei dati di Barclays, e che tale formazione sia aggiornata almeno una volta all'anno. Ove opportuno, la formazione deve comprendere quanto segue: I gruppi ad alto rischio, come quelli con Accesso Privilegiato al sistema o che svolgono funzioni aziendali sensibili (compresi gli utenti privilegiati, i dirigenti, il personale addetto alla Sicurezza Informatica e Cibernetica e i terzi interessati), devono ricevere una formazione specifica per la consapevolezza delle situazioni in materia di Sicurezza Informatica e Cibernetica in base ai loro ruoli e alle loro responsabilità. Se e laddove appropriato, questa formazione dovrebbe essere erogata da esperti terzi esterni.	In caso di mancata attuazione di questo principio, i dipendenti interessati non saranno consapevoli dei rischi cibernetici e dei vettori di attacco e non saranno in grado di rilevare o prevenire gli attacchi.
6. Gestione degli incidenti di sicurezza	Il Fornitore deve stabilire un quadro di gestione degli Incidenti di Sicurezza che convalidi efficacemente, intensifichi in modo efficiente, contenga e risolva gli Incidenti di Sicurezza che si verificano nell'ambiente del Fornitore. Il Fornitore deve garantire di disporre di piani scritti di risposta agli incidenti su misura per ogni categoria di rischio/incidente di sicurezza conosciuto che definiscano i ruoli del personale, i meccanismi di escalation e le fasi di trattamento/gestione degli incidenti: • Convalida degli incidenti - Stabilire un processo di convalida degli incidenti che sfrutti varie fonti di dati e sia integrato in tutta l'azienda per convalidare efficacemente gli Incidenti di Sicurezza (ciò si basa sul fatto che il Fornitore disponga di meccanismi di monitoraggio e rilevamento efficaci e appropriati in tutto l'ambiente IT). • Classificazione degli incidenti - Stabilire un processo di classificazione degli incidenti che classifichi in modo efficace e rapido un incidente convalidato in tutti i tipi di evento. • Escalation dell'incidente - Stabilire meccanismi appropriati per l'escalation dell'incidente (a seconda della classificazione) ai soggetti appropriati, persone responsabili e, se del caso, specialisti esterni, permettendo di fornire una risposta rapida all'incidente.	Un processo di risposta e gestione degli incidenti aiuta a garantire che vengano rapidamente circoscritti e che ne venga impedita l'escalation.

	• Contenimento degli incidenti - Utilizzare le persone, i processi e le capacità tecnologiche per identificare in modo rapido ed efficace il vettore di attacco e, di conseguenza, contenere l'Incidente di Sicurezza nell'ambiente. • Azioni di rimedio - Sfruttare le capacità delle persone, dei processi e della tecnologia per rimediare in modo rapido ed efficace alle minacce alla sicurezza e/o ai relativi componenti nell'ambiente. Un rimedio efficace garantisce la protezione contro attacchi di natura simile in futuro. Il Fornitore deve cercare di dimostrare che le attività di risposta agli incidenti sono migliorate, ove possibile, incorporando le lezioni apprese dalle attività di rilevamento/risposta attuali e precedenti. Il Fornitore è tenuto a garantire che i team e i processi di risposta agli incidenti sono testati, almeno annualmente, per garantire che il Fornitore sia in grado di reagire agli Incidenti di Cyber Security. • Le simulazioni e i test devono dimostrare che Barclays sarà informata degli Incidenti di Sicurezza che hanno un impatto su di essa; ciò deve essere evidenziato dalla dimostrata capacità del Fornitore di contattare le persone appropriate in caso di tale incidente. • Comunicazione - Il Fornitore deve nominare un punto di contatto per gli eventuali Incidenti di Sicurezza che faccia da tramite con Barclays in caso di incidente. Il Fornitore è tenuto a comunicare a Barclays i dati di contatto delle persone e le eventuali modifiche, compresi i contatti fuori orario e i numeri di telefono. I dettagli devono includere: Nome, responsabilità all'interno dell'organizzazione, ruolo, indirizzo e-mail e numero di telefono Il Fornitore informerà Barclays (e, se del caso, farà in modo che i propri subappaltatori lo facciano) entro un ragionevole lasso di tempo dal momento in cui viene a conoscenza di qualsiasi incidente che ha un impatto o si sospetta possa avere un impatto sul servizio erogato a Barclays o sui dati di Barclays e, in ogni caso, non oltre due (2) ore dal momento in cui il Fornitore viene a conoscenza dell'Incidente di Sicurezza. Nel caso di violazione dei dati sospetta o nota (compresa una violazione della sicurezza che porta alla distruzione accidentale o illegale, perdita, alterazione, divulgazione non autorizzata o accesso ai Dati Personali), il Fornitore informerà Barclays di tali incidenti entro un periodo di tempo ragionevole dal momento in cui viene a conoscenza di tali	

	incidenti, e in ogni caso, non oltre **due (2) ore** dal momento in cui il Fornitore viene a conoscenza di tale incidente. Oltre alla notifica iniziale di cui sopra, il Fornitore trasmetterà a Barclays un rapporto entro **ventiquattro (24) ore** dal momento in cui viene a conoscenza di qualsiasi incidente che abbia un impatto sul servizio erogato a Barclays o su Informazioni/Dati di Barclays. Il rapporto deve includere i seguenti dettagli: • Data e ora in cui il Fornitore è venuto a conoscenza dell'Incidente di Sicurezza • Giurisdizioni ad impatto presunto • Tipo e breve riassunto dell'Incidente di Sicurezza • Impatto e probabili conseguenze per i servizi resi a Barclays e/o per le Informazioni/i Dati di Barclays (e, se applicabile, per le persone interessate) • Stato dell'Incidente di Sicurezza (ad esempio, sono stati chiamati gli esperti forensi, sono state informate le autorità competenti, il vettore dell'attacco è noto, è in atto il monitoraggio rafforzato, il contenimento è stato effettuato) • Azione intrapresa o pianificata per rimediare all'Incidente di Sicurezza • Dettagli dei dati compromessi Questi incidenti, così come tutti gli aggiornamenti in corso relativi agli interventi di correzione e agli avvisi agli interessati, devono essere segnalati al Barclays Supplier Manager e al Barclays Joint Operations Centre all'interno del **Barclays Chief Security Office (CSO) Joint Operations Centre (JOC) - gcsojoc@barclays.com.** **Si prega di indicare nell'oggetto dell'e-mail "[Inserire il nome del Fornitore] - Incidente di Sicurezza - Richiesta di attenzione urgente". Se l'incidente è molto urgente e deve essere segnalato immediatamente, è possibile contattare JOC sulla hotline 24/7:** • Regno Unito: +44 330 041 5586 • Stati Uniti: +1 201 499 1900 • India: +91 788 781 9890	
7. Classificazione e protezione delle informazioni	Il Fornitore deve disporre di un quadro/schema di classificazione, gestione e archiviazione delle informazioni stabilito e adeguato (allineato ai requisiti delle Migliori Prassi del Settore e/o di Barclays) che copra, a titolo esemplificativo ma non esaustivo, i seguenti aspetti: • Revisione continua di Informazioni/Dati Barclays esistenti e nuovi • Assegnazione del corretto schema di etichette informative per Informazioni/Dati Barclays.	In caso di mancata implementazione dei suddetti requisiti, i Dati di Barclays possono essere esposti a modifiche, divulgazioni e accessi non autorizzati e a danni, perdite o distruzione che possono

	• Gestione e archiviazione di Informazioni/Dati in modo sicuro e idoneo, in linea con il livello di classificazione assegnato. • Garantire che tutto il personale sia a conoscenza dei requisiti di etichettatura, archiviazione e gestione del Fornitore/di Barclays e di come applicare la corretta classificazione delle informazioni. Il Fornitore deve fare riferimento allo Schema di etichettatura delle informazioni Barclays e ai requisiti di gestione (Appendice B, Tabella B1 e B2) o a uno schema alternativo per garantire che il Fornitore protegga e garantisca le informazioni di Barclays detenute e/o trattate. Questo requisito si applica a tutti i beni informatici detenuti o trattati per conto di Barclays.	comportare danni a livello normativo e reputazionale.
8. Gestione delle risorse IT (Hardware e Software)	Durante l'intero ciclo di vita dei beni, il Fornitore deve garantire che sia stabilito un programma efficace per la loro gestione. La gestione patrimoniale controlla il ciclo di vita dei beni dall'acquisizione alla dismissione, fornendo visibilità e sicurezza a tutte le classi di beni nell'ambiente. Il Fornitore deve mantenere un inventario completo e accurato dei beni critici per l'azienda situati in tutti i siti e/o luoghi geografici che forniscono servizi a Barclays, incluse le attrezzature Barclays ospitate nei locali del Fornitore e/o di un subappaltatore fornite da Barclays, oltre a garantire che sia svolto almeno un test annuale per confermare che l'inventario dei beni sia aggiornato, completo e accurato. Come misura minima, il processo di Gestione delle Risorse deve coprire le seguenti aree: • Tutti i beni informatici e le infrastrutture sono continuamente mappati/aggiornati. • Il patrimonio informatico e le infrastrutture sono quindi protetti in base alla loro classificazione, alla loro criticità e al loro valore commerciale. • Il Fornitore deve provvedere a controlli atti a garantire la registrazione e la manutenzione continua dei dati degli hardware durante l'intero ciclo di vita dei beni. • Il Fornitore deve mantenere un inventario aggiornato dei beni • **I fornitori con una configurazione di Livello 1, Livello 2 e Livello 3 devono mantenere un inventario aggiornato, completo e accurato dei beni (inclusi tutti gli endpoint, le apparecchiature di rete, i token RSA e/o qualsiasi bene fornito da Barclays).**	Un inventario completo e accurato del patrimonio di dati è essenziale per garantire controlli appropriati. In caso di mancata attuazione di questo principio, le attività di Barclays o le attività di Fornitori al servizio di Barclays potrebbero risultare compromesse e comportare perdite finanziarie, perdite di dati, danni alla reputazione e richiami ufficiali.

	• Il Fornitore deve eseguire annualmente la riconciliazione di tutti i beni di Barclays (Hardware e Software) e fornire a Barclays la relativa attestazione (Chief Security Office - team ECAM). • Assicurarsi che i beni non autorizzati siano rimossi dalla rete o messi in quarantena e che l'inventario sia aggiornato tempestivamente. • Mantenere un elenco aggiornato di tutti i software autorizzati necessari per l'erogazione dei servizi di Barclays. • Assicurarsi che solo le applicazioni software o i sistemi operativi attualmente supportati e che ricevono gli aggiornamenti del fornitore siano aggiunti all'inventario dei software autorizzato dell'organizzazione. Il software non supportato deve essere etichettato come non supportato nel sistema di inventario. Il software vicino alla fine del ciclo di vita deve anche essere etichettato come tale nel sistema di inventario. Il Fornitore deve garantire l'implementazione tempestiva di procedure efficaci ed efficienti per la mitigazione delle tecnologie non supportate e la fine del ciclo di vita, la dismissione e la distruzione di beni e dati per eliminare il rischio di compromissione dei dati.	
9. Smaltimento/distruzione di beni fisici e dati Rimanenza di informazioni elettroniche	La distruzione o cancellazione del Patrimonio Informatico di Barclays, archiviato in formato fisico o elettronico, deve avvenire in modo sicuro e commisurato ai rischi associati, accertandosi che i Dati di Barclays non siano recuperabili. Il Fornitore deve aver adottato politiche e procedure efficaci per valutare e stabilire continuamente il momento in cui la distruzione o la cancellazione dei beni informatici di Barclays memorizzati in forma fisica o elettronica è appropriata e necessaria, ai sensi del contratto o per scopi di sicurezza delle informazioni, legali o normativi. Tramite richiesta scritta, Barclays può anche chiedere la distruzione del proprio patrimonio di informazioni. Il Fornitore deve stabilire le procedure con processi aziendali di supporto e misure tecniche implementate per lo smaltimento sicuro e la rimozione/cancellazione sicura dei dati Barclays (comprese le copie di backup) da tutti i supporti di memorizzazione, garantendo che i dati non siano recuperabili con qualsiasi mezzo informatico forense. I dati Barclays memorizzati nei media devono essere cancellati ad un livello sufficiente in modo che non siano recuperabili, utilizzando preferibilmente tecniche appropriate di cancellazione dei dati come secure wipe, purging, data clearing, o distruzione dei dati o metodo basato su software per sovrascrivere i dati o utilizzare il quadro standard del	La distruzione sicura del Patrimonio ti dati aiuta a garantire che tale Patrimonio di dati Barclays non possa essere recuperato per attività di violazione o furto dei dati o per finalità dannose.

	settore sullo smaltimento dei dati (NIST). Tutte le attrezzature devono essere smaltite alla fine della loro vita operativa (difettose, smantellate a causa del servizio, ritirate o non più necessarie, utilizzate in una dimostrazione o come prototipo, ecc.) I servizi di cancellazione dei dati possono essere utilizzati per apparecchiature che devono essere riutilizzate. I requisiti di smaltimento si applicano al Fornitore quarto/alle agenzie in subappalto utilizzati per fornire il servizio a Barclays. Le informazioni cartacee possono essere smaltite per distruzione almeno secondo lo standard P4 DIN66399 utilizzando un trituratore a taglio trasversale (sono incluse le informazioni della carta di pagamento) oppure possono essere incenerite conformemente a BS EN15713:2009. Per Barclays, le prove dell'eliminazione dei dati devono essere conservate, fornendo un processo di verifica, evidenze e tracciamento, e devono includere: • Prova della distruzione e/o dello smaltimento (inclusa la data in cui sono stati eseguiti e il metodo utilizzato). • Registri di controllo del sistema per la cancellazione. • Certificati di smaltimento dati. • Chi ha effettuato lo smaltimento (compresi eventuali partner di smaltimento, terzi o appaltatori). • Deve essere generato un rapporto di distruzione e verifica per confermare il successo o il fallimento di qualsiasi processo di distruzione/cancellazione (cioè un processo di sovrascrittura deve fornire un rapporto che indichi nel dettaglio eventuali settori che non è stato possibile cancellare). Durante l'uscita, il Fornitore deve garantire che i Dati Barclays siano distrutti in modo sicuro su notifica e autorizzazione di Barclays.	
10. Sicurezza del perimetro e della rete	Il Fornitore deve garantire che tutti i Sistemi IT gestiti dal Fornitore o dai rispettivi subfornitori che supportano i servizi Barclays siano protetti dalle minacce in **entrata e in uscita presenti nella rete** del Fornitore (e di qualsiasi subfornitore pertinente). Il Fornitore deve monitorare, rilevare, prevenire e, se necessario, porre rimedio al flusso di informazioni che si trasferisce attraverso reti con diversi livelli di fiducia con particolare attenzione alle violazioni della sicurezza.	La mancata implementazione di questo principio potrebbe comportare l'attacco delle reti esterne o interne da parte di hacker al fine di ottenere l'accesso ai servizi o ai dati contenuti.

	I meccanismi di integrità della rete devono includere, a titolo esemplificativo, le seguenti aree: • Mantenere un inventario aggiornato di tutti i perimetri della rete dell'organizzazione (attraverso un'Architettura di Rete/Diagramma). • La progettazione e l'implementazione della rete, così come le potenziali vulnerabilità e la necessità di eliminare e rinnovare le infrastrutture della rete, devono essere riviste almeno una volta all'anno o nel caso in cui vi sia un requisito legato ad un evento che causa cambiamenti. • Tutti i collegamenti esterni alla rete del Fornitore devono essere documentati, devono passare attraverso un firewall e devono essere verificati e approvati prima di stabilire la connessione al fine di prevenire violazioni della sicurezza. • Le reti dei Fornitori sono protette mediante l'applicazione di principi di difesa in profondità (ad es. segmentazione della rete, firewall, controlli fisici di accesso alle apparecchiature di rete, ecc.) • Il Fornitore deve disporre di tecnologie di prevenzione delle intrusioni in rete per rilevare e impedire l'ingresso di traffico dannoso nella rete. • Uso di potenti firewall di rete per fornire un livello di difesa perimetrale contro attacchi di rete dolosi. • Il traffico della rete Internet deve passare attraverso un proxy configurato per filtrare le connessioni non autorizzate. • Assicurarsi che la registrazione e il monitoraggio siano abilitati. • I dispositivi di rete sono protetti in modo sicuro per prevenire attacchi dolosi. • Separazione logica delle porte/interfacce per la gestione dei dispositivi dal traffico degli utenti; controlli di autenticazione appropriati. • Tutte le regole di configurazione che consentono il flusso del traffico attraverso i dispositivi di rete devono essere documentate in un sistema di gestione della configurazione con una specifica motivazione aziendale per ogni regola. • Negare la comunicazione su porte TCP o UDP o il traffico di applicazioni non autorizzati per garantire che solo ai protocolli autorizzati sia consentito attraversare il perimetro di rete in entrata o in uscita tramite le porte di rete dedicate. • Eseguire regolari verifiche tentando l'ingresso nel perimetro di ogni rete protetta per rilevare eventuali connessioni non autorizzate. • Comunicazioni sicure tra i dispositivi e le postazioni di gestione/console.	

	• Configurare i sistemi di monitoraggio per registrare i pacchetti di rete che passano attraverso il perimetro in ciascuno dei perimetri della rete dell'organizzazione. • La connessione di rete tra uffici/fornitore di servizi cloud/data center deve essere crittografata in base a un protocollo sicuro. I Dati / il Patrimonio informatico di Barclays in transito all'interno della Wide Area Network (WAN) del Fornitore devono essere criptati. • Il Fornitore deve rivedere annualmente le regole del firewall (Firewall esterno e interno). • Tutti gli accessi wireless alla rete sono soggetti a protocolli di autorizzazione, autenticazione, segmentazione e criptazione per prevenire le violazioni della sicurezza. • Il Fornitore deve garantire che l'accesso alla rete interna sia monitorato e consentito esclusivamente ai dispositivi autorizzati, tramite adeguati controlli di accesso alla rete. • L'accesso remoto alla rete del Fornitore deve utilizzare l'autenticazione a più fattori. • Il Fornitore deve avere una rete dedicata per i servizi da erogare a Barclays. Il Fornitore deve garantire che i server utilizzati per fornire il servizio a Barclays non siano distribuiti su reti non affidabili (reti al di fuori del perimetro di sicurezza dell'utente, che sono al di fuori del controllo amministrativo dell'utente, ad esempio, per l'accesso a Internet) senza adeguati controlli di sicurezza. Il Fornitore che ospita le Informazioni Barclays (incluso il subappaltatore) in un data center o spazio cloud deve possedere una certificazione di Migliori Prassi del Settore per la gestione della sicurezza. Rete T2 e T3 - • La rete T2 deve essere separata in modo logico dalla rete aziendale del Fornitore da un Firewall e tutto il traffico in entrata e in uscita deve essere limitato e monitorato. • La configurazione del percorso deve garantire solo le connessioni alla rete Barclays e non deve condurre ad altre reti del Fornitore. • Il router Supplier Edge che si collega ai gateway extranet di Barclays deve essere configurato in modo sicuro con un concetto di limitazione dei controlli di porte, protocolli e servizi;	

	○ Assicurarsi che la registrazione e il monitoraggio siano abilitati. *N.B. Il termine "rete" come utilizzato in questo controllo si riferisce a qualsiasi rete non-Barclays per cui il Fornitore è responsabile, dell'inclusione delle reti del subfornitore.*	
11. Rifiuto di rilevamento del servizio (Denial of Service Detection)	Il Fornitore deve mantenere la capacità di rilevare e proteggere dagli attacchi Rifiuto di servizio (Denial of Service - DoS) e Rifiuto di servizio diffuso (Distributed Denial of Services - DDoS). Il Fornitore deve accertarsi che i servizi di supporto per i canali Internet o esterni erogati a Barclays godano di un'adeguata protezione DoS per garantire la disponibilità. Se il Fornitore ospita un'applicazione che è connessa a Internet e che contiene dati riservati o che sostiene un servizio di categoria di resilienza 0 o 1, questa deve essere protetta fino al livello 7 utilizzando tecnologie appropriate che devono essere approvate da Barclays.	In caso di mancata attuazione di questo principio, Barclays e i suoi Fornitori potrebbero non essere in grado di impedire che un attacco di tipo Denial of Service vada a buon fine.
12. Lavoro a distanza (accesso remoto)	L'accesso remoto alla rete di Barclays tramite applicazioni Citrix di Barclays e/o dati di Barclays residenti/archiviati all'interno di ambienti/reti gestiti dal Fornitore, se il Fornitore o uno dei rispettivi subappaltatori accede ai Dati di Barclays o ai Dati Personali di Barclays o a qualsiasi informazione sensibile trasmessa al Fornitore in base alla necessità di conoscere, sia in forma fisica che virtuale, per accedere, condividere o trattare a distanza, in particolare quando il personale può lavorare da casa, il Fornitore richiederà la previa approvazione di Barclays (Chief Security Office - ECAM Team) per questi accordi. Come misura minima, il Fornitore deve garantire che i seguenti componenti siano istituiti per l'accesso remoto: • L'accesso remoto alla rete del Fornitore deve essere criptato durante il trasferimento dei dati e utilizzare sempre l'autenticazione a più fattori. • L'accesso alla rete Barclays deve avvenire tramite l'applicazione Barclays Citrix con Token RSA (Hard & Soft) fornito da Barclays. • Il Fornitore deve mantenere un inventario di tutti i token RSA (Hard & Soft) forniti da Barclays e un processo di gestione che includa la revisione e il monitoraggio dell'assegnazione, dell'utilizzo e della restituzione dei token (Hard token). • Il Fornitore deve conservare le registrazioni delle persone a cui è stato chiesto di lavorare da remoto e le motivazioni di tale richiesta	I controlli di Accesso Remoto aiutano a garantire che i dispositivi non autorizzati e non sicuri non siano collegati all'ambiente Barclays da remoto.

	• Il Fornitore deve eseguire la riconciliazione di tutti gli utenti remoti su base trimestrale e fornire un'attestazione a Barclays (Chief Security Office - team ECAM). • Barclays disattiverà prontamente le credenziali di autenticazione nel caso in cui tali credenziali non siano state utilizzate per un periodo di tempo (tale periodo di non utilizzo non deve superare un mese). • Il Fornitore deve garantire che l'endpoint utilizzato per il collegamento da remoto ai sistemi informativi di Barclays sia configurato in modo sicuro e in conformità con le Migliori Prassi del Settore (ad es. livello delle patch, stato dell'anti-malware, soluzione di rilevamento e risposta degli endpoint EDR, registrazione ecc.). • I servizi che hanno accesso alla stampa remota tramite l'applicazione Barclays Citrix devono essere approvati e autorizzati da Barclays (Chief Security Office - ECAM Team). Il fornitore deve mantenere i registri ed eseguire la riconciliazione trimestrale. • I dispositivi personali/BYOD non devono essere autorizzati ad accedere all'ambiente Barclays e/o ai dati Barclays presenti/memorizzati all'interno dell'ambiente gestito dal Fornitore (che include, a titolo esemplificativo ma non esaustivo, il personale del Fornitore, i consulenti, gli operatori di emergenza, gli appaltatori e i partner di servizi gestiti (MPS)). Quando agli endpoint (Laptop/Desktop) viene concesso l'accesso alla rete Barclays tramite le applicazioni Barclays Citrix su Internet, il Fornitore deve installare lo strumento End Point Analysis (EPA) fornito da Barclays per convalidare la sicurezza degli endpoint e la conformità del sistema operativo; solo ai dispositivi che superano i controlli End Point Analysis sarà concesso l'accesso remoto alla rete Barclays tramite l'applicazione Barclays Citrix. Se il Fornitore non è in grado di installare o utilizzare lo strumento EPA, è necessario informare il responsabile del Fornitore di Barclays. Nota: Barclays disattiverà entro **ventiquattro (24) ore** le credenziali di autenticazione non appena sarà notificato che l'accesso non è più necessario (ad es. licenziamento di un dipendente, riassegnazione di un progetto, ecc.).	
13. Gestione dei registri di sicurezza	Il Fornitore deve garantire l'esistenza di un quadro di audit e di gestione dei registri consolidato che confermi che i sistemi e i processi IT chiave, comprese le applicazioni, le apparecchiature di rete, i database, gli endpoint, i dispositivi di sicurezza, l'infrastruttura e i server producano i registri richiesti, in conformità con le Migliori Prassi del Settore e le linee guida. Tali registri devono essere adeguatamente protetti,	La mancata implementazione di questo controllo potrebbe comportare l'impossibilità da parte dei Fornitori di rilevare e rispondere all'uso improprio o dannoso dei

tenuti a livello centrale e conservati dal Fornitore per un periodo minimo di 12 mesi o sulla base delle categorie sottostanti secondo un rapporto adeguato.

Categoria	Sistemi a impatto basso / Servizio	Sistemi a impatto medio / Servizio	Sistemi a impatto elevato / Servizio
Conservazione dei registri	3 mesi	6 mesi	12 mesi

Come misura minima, il processo di gestione dei log di sicurezza deve coprire le seguenti aree:

- Il Fornitore deve stabilire politiche e procedure per la gestione dei registri.
- Il Fornitore deve creare e mantenere un'infrastruttura di gestione dei registri.
- Il Fornitore deve definire i ruoli e le responsabilità dei singoli e dei team che devono essere coinvolti nella gestione dei registri.
- Raccogliere, gestire e analizzare i registri di audit degli eventi per contribuire a monitorare, rilevare, comprendere o recuperare in seguito a un attacco.
- Abilitare la registrazione del sistema per includere informazioni dettagliate come la fonte di un evento, la data, l'utente, la marca temporale, gli indirizzi di origine, gli indirizzi di destinazione e altri elementi utili.
- Di seguito alcuni esempi di registri di eventi:
    - IDS/IPS, Router, Firewall, Web Proxy, Software per l'accesso remoto (VPN), Server di autenticazione, Applicazioni, Registri per database.
    - Login riusciti, tentativi di login falliti (ad esempio ID utente o password sbagliati), creazione, modifica e cancellazione di account utente
    - Registri di modifica della configurazione.
- Servizi Barclays relativi ad applicazioni aziendali e sistemi di infrastrutture tecniche su cui deve essere abilitata la registrazione delle Migliori Prassi del Settore pertinenti, compresi quelli che sono stati esternalizzati o che sono "in clouding".
- Analisi dei registri degli eventi relativi alla sicurezza (compresa la normalizzazione, l'aggregazione e la correlazione).
- Sincronizzazione delle marche temporali nei registri degli eventi con una fonte comune e affidabile
- Protezione dei registri degli eventi relativi alla sicurezza (ad es. tramite cifratura, MFA, controllo degli accessi e backup).

loro servizi o dei dati forniti entro periodi di tempo ragionevoli.

	• Adottare le azioni necessarie per risolvere i problemi individuati e rispondere agli Incidenti di Sicurezza Informatica in modo rapido ed efficace. • Implementazione di Security Information and Event Management (SIEM) o di strumenti di analisi dei registri per la correlazione e l'analisi dei registri. • Implementazione di strumenti adeguati per eseguire l'aggregazione centrale e la correlazione in tempo reale di attività anomale, allarmi di rete e di sistema, e informazioni rilevanti su eventi e minacce informatiche da più fonti, sia interne che esterne, per rilevare e prevenire meglio i molteplici attacchi informatici. Gli eventi principali registrati devono comprendere quelli che potrebbero compromettere la riservatezza, l'integrità e la disponibilità dei Servizi resi a Barclays e potrebbero contribuire all'identificazione o alla ricerca di incidenti di rilievo e/o violazioni dei diritti di accesso che si verificano in relazione ai Sistemi del Fornitore	
14. Difese contro i malware	In linea con le Migliori Prassi del Settore, il Fornitore deve aver posto in essere politiche e procedure stabilite, nonché processi aziendali di supporto e misure tecniche implementate, per prevenire l'esecuzione di malware sull'intero ambiente IT. Il Fornitore deve garantire che la protezione dai malware venga applicata in ogni momento a tutte le risorse IT applicabili per prevenire interruzioni del servizio o violazioni della sicurezza. La protezione dai malware deve avere o includere, a titolo esemplificativo ma non esaustivo, quanto segue: • Software anti-malware gestito a livello centrale per monitorare e difendere l'ambiente IT dell'organizzazione. • Garanzia che il software anti-malware dell'organizzazione aggiorni regolarmente e in conformità con le Migliori Prassi del Settore il proprio motore di scansione e il database delle firme. • Inviare tutti gli eventi di rilevamento di malware agli strumenti di amministrazione anti-malware aziendali e ai server di registro degli eventi per l'analisi e gli avvisi. • Il Fornitore deve implementare controlli appropriati per la protezione contro il malware mobile e gli attacchi ai dispositivi mobili che si connettono a Barclays o alle reti del Fornitore e che accedono ai dati di Barclays. • È necessario che esistano procedure per lo svolgimento regolare di riunioni/forum (ad esempio su base mensile) per discutere potenziali vulnerabilità/aggiornamenti necessari. Devono essere adottate azioni	Le soluzioni anti-malware sono fondamentali per la protezione dei Patrimoni di dati Barclays contro i Codici Maligni.

	correttive in modo prioritario e tempestivo. Le registrazioni delle segnalazioni, dei forum e delle azioni correttive intraprese devono essere conservate. Nota: Anti-malware per includere il rilevamento di (ma non solo) codici mobili non autorizzati, virus, spyware, software key logger, botnet, worm, trojan, ecc.	
15. Standard per la configurazione sicura	Il Fornitore deve disporre di un quadro di riferimento consolidato per garantire che tutti i sistemi/apparecchiature di rete configurabili siano configurati in modo sicuro conformemente alle Migliori Prassi del Settore (ad es. NIST, SANS, CIS). Il processo standard di configurazione deve coprire, a titolo esemplificativo, le seguenti aree: • Stabilisce politiche, procedure / misure organizzative e strumenti per consentire l'implementazione degli standard di configurazione della sicurezza secondo le Migliori Prassi del Settore per tutti i dispositivi di rete e i sistemi operativi, le applicazioni e i server autorizzati. • Esegue controlli regolari (annuali) sull'applicazione delle norme per garantire che il mancato rispetto degli standard di sicurezza di base sia prontamente corretto. Sono in atto controlli e monitoraggi adeguati per garantire che sia mantenuta l'integrità delle costruzioni/apparecchiature. • I sistemi e i dispositivi di rete sono configurati in modo da funzionare secondo i principi di sicurezza (ad es. concetto di limitazione dei controlli di porte, protocolli e servizi, nessun software non autorizzato, rimozione e disabilitazione degli account utente non necessari, modifica delle password di default degli account, rimozione del software non necessario, ecc.) Garantire che la gestione della configurazione regoli gli standard di configurazione sicura in tutte le classi di beni e che rilevi, avverta e risponda efficacemente alle modifiche o alle deviazioni della configurazione.	I controlli delle norme della struttura aiutano a proteggere il Patrimonio di dati da accesso non autorizzato La conformità alle strutture e ai controlli standard che garantiscono l'autorizzazione delle modifiche aiuta a garantire la protezione del Patrimonio di dati Barclays
16. Sicurezza dell'endpoint	Il Fornitore deve garantire che gli endpoint utilizzati per accedere alla rete di Barclays o per accedere/elaborare il Patrimonio informatico / i Dati di Barclays siano configurati per la protezione dagli attacchi dolosi. Devono essere utilizzate le Migliori Prassi del Settore e la costruzione della sicurezza degli endpoint deve includere, a titolo esemplificativo ma non esaustivo: • Crittografia del disco. • Disattivare tutti i software/servizi/porte non necessari.	La mancata attuazione di questo controllo potrebbe rendere Barclays, la rete e gli endpoint dei Fornitori vulnerabili agli attacchi Cibernetici.

	• Disattivare l'accesso ai diritti di amministrazione per l'utente locale. • Il personale del Fornitore non potrà modificare le impostazioni di base come il Service Pack predefinito, la partizione di sistema e i servizi predefiniti, ecc. • La porta USB deve essere disabilitata per vietare la copia dei dati Barclays su supporti esterni • Aggiornato con le ultime firme antivirus e patch di sicurezza. • Prevenzione della perdita di dati limitata al divieto di taglia-copia-incolla e stampa-schermo dei dati Barclays • Come impostazione predefinita, l'accesso alla stampante deve essere disabilitato. • Il Fornitore deve limitare la capacità di accedere a siti di social network, servizi di webmail e siti con la possibilità di memorizzare informazioni su Internet come google drive, Dropbox, iCloud. • La condivisione / il trasferimento del Patrimonio informatico / dei Dati di Barclays durante l'utilizzo di strumenti/software di messaggistica istantanea devono essere disabilitati. • Capacità e processi per rilevare software non autorizzati identificati come dannosi e impedire l'installazione di software non autorizzati. Nota: i supporti rimovibili/dispositivi portatili devono essere disabilitati per impostazione predefinita e abilitati solo per legittimi motivi di lavoro. Il Fornitore deve mantenere immagini o modelli sicuri per tutti i sistemi dell'azienda sulla base degli standard di configurazione approvati dall'organizzazione. Qualsiasi nuova implementazione del sistema o sistema esistente che venga compromesso deve essere raffigurato utilizzando una di queste immagini o modelli. Quando agli endpoint (Laptop/Desktop) viene concesso l'accesso alla rete Barclays tramite le applicazioni Barclays Citrix su Internet, il Fornitore deve installare lo strumento End Point Analysis (EPA) fornito da Barclays per convalidare la sicurezza degli endpoint e la conformità del sistema operativo; solo ai dispositivi che superano i controlli End Point Analysis sarà concesso l'accesso remoto alla rete Barclays tramite l'applicazione Barclays Citrix. Se il Fornitore non è in grado di installare o utilizzare lo strumento EPA, è necessario informare il responsabile del Fornitore di Barclays. Dispositivi mobili utilizzati per i servizi Barclays - 1. Il Fornitore deve assicurarsi di implementare le funzionalità di gestione dei dispositivi mobili (MDM) per controllare e gestire in modo sicuro durante	

	l'intero ciclo di vita i dispositivi mobili che hanno accesso e/o contengono informazioni classificate Barclays, riducendo il rischio di compromissione dei dati. 2. Il Fornitore deve garantire l'implementazione delle funzionalità di blocco e cancellazione remota dei dispositivi mobili per proteggere le informazioni in caso di smarrimento, furto o compromissione di un dispositivo. 3. Crittografare i dati dei dispositivi mobili (Dati di Barclays).	
17. Prevenzione della fuga di dati	Il Fornitore deve disporre di un quadro di riferimento consolidato per garantire che sia in atto la protezione contro la fuga di dati inopportuna garantendo una protezione che include i seguenti canali di fuga di dati (a titolo esemplificativo): • Trasferimento non autorizzato di informazioni al di fuori della rete interna/rete del Fornitore. o E-mail o Internet/Web Gateway (inclusi archiviazione on-line e webmail) o DNS • Perdita o furto del Patrimonio di dati di Barclays da supporti elettronici portatili (comprese le informazioni elettroniche su laptop, dispositivi mobili e supporti portatili). • Trasferimento non autorizzato di informazioni a supporti portatili. • Scambio non sicuro di informazioni con terze parti (quarte parti o subfornitori). • Stampa o copia inadeguata di informazioni.	Occorre applicare in modo efficace controlli appropriati al fine di assicurare che l'accesso alle informazioni Barclays sia riservato a coloro che hanno reale necessità di consultarli (riservatezza) e che i dati siano protetti contro le modifiche non autorizzate (integrità) e possano essere recuperati e trasmessi quando richiesto (disponibilità). In caso di mancata implementazione dei suddetti requisiti, i dati sensibili Barclays possono essere esposti a modifiche, divulgazioni e accessi non autorizzati e a danni, perdite o distruzione che possono comportare sanzioni legali e normative, danneggiamento della reputazione e perdite o interruzioni dell'attività
18. Sicurezza dei dati	Il Fornitore deve garantire che il Patrimonio informatico / i Dati di Barclays affidati/presenti nella rete del Fornitore si trovino in una condizione di sicurezza dei dati adeguata ottenuta attraverso una combinazione di crittografia, dispositivi sicuri per accedere ai dati, protezione dell'integrità e tecniche di prevenzione della perdita di dati. È importante prestare la dovuta attenzione a limitare l'accesso al Patrimonio informatico / ai Dati di Barclays, compresi i dati personali, e rendere sicuro tale accesso. I controlli sulla sicurezza dei dati devono coprire, a titolo esemplificativo ma non esaustivo, le seguenti aree: 1. Il Fornitore è obbligato in ogni momento a rispettare tutte le leggi sulla protezione dei dati applicabili. 2. Devono essere stabilite politiche e procedure, e implementati processi / misure organizzative aziendali e misure tecniche di supporto, in modo da	

	inventariare, documentare e mantenere i flussi di dati per i dati presenti (permanentemente o temporaneamente) nelle applicazioni del servizio (fisiche e virtuali) geograficamente distribuite e dei componenti di rete e di sistema dell'infrastruttura e/o condivisi con terze parti diverse. 3. Mantenere un inventario di tutte le informazioni sensibili /riservate (Patrimonio informatico / Dati di Barclays) memorizzate, elaborate o trasmesse dal Fornitore. 4. Stabilire uno standard di classificazione dei dati per garantire che le informazioni sensibili (Patrimonio informatico / Dati di Barclays) siano classificate e protette in modo appropriato. 5. Garantire che tutti i dati Barclays siano classificati ed etichettati in base allo standard di classificazione e protezione delle informazioni. 6. Protezione dei dati archiviati; a. Come misura minima, crittografare i dati archiviati per impedire lo sfruttamento di informazioni sensibili tramite l'accesso non autorizzato. 7. Monitoraggio delle attività del database; a. Monitorare e registrare l'accesso al database e l'attività per identificare rapidamente ed efficacemente le attività dannose. 8. Protezione dei dati in uso; a. Garantire che la visualizzazione e l'uso delle informazioni sensibili sia controllato attraverso le capacità di gestione degli accessi per proteggere dallo sfruttamento le informazioni sensibili. b. Utilizzare tecnologie di mascheramento e offuscamento dei dati per proteggere efficacemente i dati sensibili in uso dalla divulgazione involontaria e/o dallo sfruttamento malevolo. 9. Protezione dei dati in transito; a. Sfruttare le forti capacità di crittografia per garantire la protezione dei dati durante il transito. b. Solitamente la crittografia dei dati in transito è ottenuta utilizzando la crittografia Trasporto o Carico utile (Messaggio o Campo selettivo). I meccanismi di cifratura del trasporto includono, a titolo esemplificativo: • Protocollo Transport Layer Security (TLS) (seguendo le Migliori Prassi del Settore della crittografia moderna, incluso l'uso/il rifiuto di protocolli e cifrari) • Tunneling sicuro (Secure Tunneling - IPsec)	

	• Guscio di sicurezza (Secure Shell - SSH) c. I protocolli di sicurezza del trasporto devono essere configurati in modo da evitare la negoziazione di algoritmi più deboli e/o lunghezze di chiave più brevi, quando entrambi i punti finali supportano l'opzione più forte. 10. Backup dei dati – a. Si devono prendere i dovuti provvedimenti per garantire che le Informazioni ricevano un adeguato back-up e siano recuperabili (e possano essere recuperate in un tempo ragionevole) conformemente ai requisiti concordati con Barclays. b. Assicurarsi che i backup siano adeguatamente protetti tramite sicurezza fisica o crittografia quando vengono memorizzati, così come quando vengono spostati attraverso la rete. Sono compresi i backup remoti e i servizi cloud. c. Accertarsi che tutti i dati Barclays siano automaticamente e regolarmente sottoposti a backup.	
19. Sicurezza del software applicativo	Il Fornitore deve sviluppare le applicazioni utilizzando pratiche di codifica sicura e operando in un ambiente sicuro. Se il Fornitore sviluppa delle applicazioni per l'utilizzo da parte di Barclays o che sono utilizzate a supporto dei servizi resi a Barclays, il Fornitore deve stabilire un quadro di sviluppo sicuro per prevenire violazioni della sicurezza e per individuare e rimediare alle vulnerabilità nel codice durante il processo di sviluppo. La sicurezza del software applicativo deve coprire, a titolo esemplificativo ma non esaustivo, le seguenti aree:	I controlli che tutelano lo sviluppo di applicazioni aiutano a garantirne la sicurezza al momento della distribuzione.

	• Gli standard di codifica sicura devono essere in vigore e adottati conformemente alle Migliori Prassi del Settore per prevenire le vulnerabilità di sicurezza e le interruzioni del servizio che, allo stesso tempo, difendono da possibili vulnerabilità ben note. • Stabilire pratiche di codifica sicure e adeguate al linguaggio di programmazione. • Tutte le attività di sviluppo devono essere svolte in un ambiente non produttivo. • Mantenere ambienti separati per i sistemi di produzione e non. Gli sviluppatori non devono avere un accesso non monitorato agli ambienti di produzione. • Separazione dei compiti per gli ambienti di produzione e non. • I sistemi sono sviluppati in linea con le Migliori Prassi del Settore di Secure Development (ad esempio OWASP). • Il codice deve essere conservato in modo sicuro e soggetto ai controlli della Garanzia di Qualità. • Il codice deve essere adeguatamente protetto da modifiche non autorizzate una volta che il test è stato confermato e consegnato in produzione. • Per il software sviluppato dal Fornitore utilizzare solo componenti aggiornati di terze parti di fiducia. • Applicare strumenti di analisi statica e dinamica per verificare il rispetto delle pratiche di codifica sicura. • Il Fornitore deve garantire che i dati attuali (compresi i Dati Personali) non saranno utilizzati in ambienti non produttivi. • Le applicazioni e le interfacce di programmazione (API) devono essere progettate, sviluppate, implementate e testate conformemente alle migliori pratiche di settore (ad es. OWASP per le applicazioni web). Il Fornitore è tenuto a proteggere le applicazioni web distribuendo firewall per applicazioni web (WAF) che esaminano tutto il traffico verso l'applicazione web per verificare che non vi siano attacchi di applicazioni web esistenti e comuni. Per le applicazioni che non sono basate sul web, devono essere implementati firewall specifici per le applicazioni, se tali strumenti sono disponibili per il tipo di applicazione dato. Se il traffico è criptato, il dispositivo dovrebbe trovarsi 'dietro' la criptazione o essere in grado di decriptare il traffico prima dell'analisi. Se nessuna delle due opzioni è appropriata, dovrebbe essere implementato un firewall per applicazioni web basate su host.	
20. Logical Access Management (LAM)	L'accesso alle Informazioni deve essere limitato, tenendo in debita considerazione l'esigenza di conoscere (need-to-know), il Privilegio minimo e i principi di segregazione	Controlli LAM appropriati aiutano a garantire la protezione dei

	delle mansioni. Spetta al titolare del Patrimonio di dati decidere chi ha necessità di accedere e il tipo di accesso. • Il principio need-to-know prevede che le persone possano accedere solo alle informazioni che hanno necessità di conoscere al fine di svolgere le mansioni autorizzate. Ad esempio, se un dipendente tratta esclusivamente con clienti situati nel Regno Unito non hanno necessità di conoscere Informazioni relative a clienti situati negli Stati Uniti. • Il principio del Privilegio minimo prevede che le persone possano avere solo il livello minimo di privilegio necessario per svolgere le mansioni autorizzate. Ad esempio, se un dipendente ha bisogno di visualizzare l'indirizzo di un cliente ma non deve modificarlo, il "Privilegio minimo" di cui necessita è l'accesso in sola lettura, che può essere ottenuto al posto dell'accesso in scrittura. • Il principio di segregazione delle mansioni prevede che almeno due persone siano responsabili per le diverse parti di qualsiasi attività al fine di prevenire errori e frodi. Ad esempio, un dipendente che chiede la creazione di un account non può essere il soggetto che approva la richiesta. Il Fornitore deve accertare che l'accesso alle Informazioni Personali sia gestito in modo appropriato e limitato a coloro che hanno necessità di accedere per erogare il servizio. I processi di gestione dell'accesso devono essere definiti secondo le Migliori Prassi del Settore e devono includere quanto segue: • Il Fornitore è tenuto a garantire che le procedure e le decisioni di gestione degli accessi siano documentate e si applichino a tutti i sistemi IT (che memorizzano o elaborano patrimoni di dati Barclays); una volta implementate, inoltre, devono fornire controlli appropriati per quanto riguarda: Joiner / Mover / Leaver / Accesso remoto. • Occorre provvedere ai controlli ai fini dell'autorizzazione per assicurare che la procedura relativa alla concessione, alla modifica e alla revoca dell'accesso comprenda un livello di autorizzazione commisurato ai privilegi in corso di concessione. • Occorre provvedere ai controlli atti ad assicurare che le procedure di gestione degli accessi comprendano processi appropriati di verifica dell'identità. • Ogni account deve essere associato a una singola persona, che sarà responsabile di tutte le attività svolte utilizzando l'account.	Patrimoni di dati da un uso improprio. I controlli della gestione degli accessi aiutano a garantire che solo gli Utenti approvati possano accedere ai Patrimoni di dati.

	• Ricertificazione dell'accesso - Occorre provvedere ai controlli atti ad assicurare che i permessi di accesso siano riesaminati almeno ogni 12 mesi, al fine di verificare che siano commisurati allo scopo. • Tutti i permessi di accesso privilegiato devono essere riesaminati almeno ogni sei (6) mesi; inoltre, occorre implementare controlli adeguati per quanto riguarda le richieste di accesso privilegiato. • Controlli sui trasferimenti – Accesso modificato entro ventiquattro (24) ore dalla data di trasferimento (conservando le registrazioni pertinenti); • Controlli sui congedi – Tutti gli accessi logici utilizzati per fornire a Barclays i servizi, rimossi entro ventiquattro (24) ore dalla data del congedo (conservando le registrazioni pertinenti); • Accesso remoto - I controlli sugli accessi remoti devono essere autorizzati esclusivamente tramite procedure approvate da Barclays (Chief Security Office - ECAM team) e gli accessi remoti devono utilizzare l'Autenticazione a Più Fattori. • Autenticazione - Lunghezza e complessità delle password adeguate, frequenza delle modifiche delle password, autenticazione a più fattori, gestione sicura delle credenziali delle password o altri controlli devono essere seguiti secondo le Migliori Prassi del Settore. • Gli account inattivi non utilizzati da almeno 60 giorni consecutivi devono essere sospesi/disabilitati (conservando le registrazioni pertinenti). • Le password di account interattivi devono essere cambiate almeno ogni 90 giorni e devono essere diverse dalle dodici (12) precedenti. • Gli account privilegiati devono essere cambiati dopo ogni uso e almeno ogni 90 giorni. • Gli account interattivi devono essere disabilitati dopo un massimo di cinque (5) tentativi consecutivi di accesso non riusciti o un numero di tentativi inferiore, se le Migliori Prassi del Settore lo impongono.	
21. Gestione della vulnerabilità	Il Fornitore deve far sì che vengano stabilite politiche e procedure a supporto dei processi / delle misure organizzative e che siano implementate misure tecniche per il monitoraggio efficace, il rilevamento tempestivo e la correzione delle vulnerabilità all'interno di applicazioni gestite o di proprietà del Fornitore, della rete infrastrutturale e dei componenti di sistema per garantire l'efficienza dei controlli di sicurezza implementati.	La mancata attuazione di questo controllo potrebbe comportare l'utilizzo di queste vulnerabilità dei sistemi per condurre attacchi informatici che possono dare luogo a danni a livello normativo e reputazionale.

La gestione delle vulnerabilità deve coprire, a titolo esemplificativo ma non esaustivo, le seguenti aree:

- Definizione dei ruoli, delle responsabilità e delle competenze per il monitoraggio, il reporting, l'escalation e la correzione.
- Strumenti e infrastrutture adeguati per la scansione delle vulnerabilità.
- Svolgere regolarmente scansioni delle vulnerabilità (con la cadenza indicata dalle Migliori Prassi del Settore) che identifichino efficacemente le vulnerabilità note e sconosciute in tutte le classi di attività dell'ambiente.
- Utilizzare un processo di valutazione del rischio per dare priorità al rimedio delle vulnerabilità scoperte.
- Stabilire un processo di validazione per il rimedio delle vulnerabilità che verifichi in modo rapido ed efficace tale rimedio in tutte le classi di attività nell'ambiente.
- Accertarsi che le vulnerabilità siano affrontate in modo efficace attraverso robuste attività di bonifica e gestione delle patch per ridurre il rischio di sfruttamento delle vulnerabilità (la correzione deve avvenire in modo tempestivo e conformemente alle Migliori Prassi del Settore).
- Confrontare regolarmente i risultati di scansioni consecutive delle vulnerabilità per verificare che queste ultime siano state corrette in modo tempestivo.

Per i servizi erogati dai Fornitori relativamente a **infrastruttura/applicazioni in Hosting** per conto di Barclays.

- In caso di identificazione di vulnerabilità critiche/elevate, il Fornitore deve informare immediatamente Barclays.
- Il Fornitore deve rimediare alle vulnerabilità secondo le voci della tabella sottostante o in accordo con Barclays (Chief Security Office - ECAM team).

Priorità	Classificazione	Giorni di chiusura (massimo)
P1	Critica	15
P2	Alta	30
P3	Media	60

	<table><tr><td>P4</td><td>Bassa</td><td>180</td></tr><tr><td>P5</td><td>A titolo informativo</td><td>360</td></tr></table> Tutti i problemi di sicurezza e le vulnerabilità che potrebbero avere un impatto concreto sull'infrastruttura di hosting di Barclays/le applicazioni web fornite dal Fornitore, che il Fornitore ha deciso di accettare a rischio, devono essere comunicati/notificati a Barclays tempestivamente e concordati per iscritto con Barclays (Chief Security Office - team ECAM).	
22. Gestione degli aggiornamenti	Il Fornitore deve far sì che vengano stabilite politiche e procedure a supporto dei processi / delle misure organizzative aziendali e che siano implementate misure tecniche per monitorare/tracciare la necessità di patch e distribuire patch di sicurezza al fine di gestire l'intero ambiente/edificio del Fornitore. Il Fornitore deve garantire che le più recenti patch di sicurezza siano applicate ai sistemi/attività/reti/applicazioni in modo tempestivo e conformemente alle Migliori Prassi del Settore, accertandosi che: • il Fornitore controlli tutte le patch su sistemi che rappresentano accuratamente la configurazione dei sistemi di produzione target prima dell'implementazione della patch nei sistemi di produzione e che il corretto funzionamento del servizio di patch sia verificato dopo ogni attività di patch. Se in un sistema non può essere installata una patch, adottare le contromisure appropriate. • Tutte le modifiche IT fondamentali devono essere registrate, verificate e approvate prima dell'implementazione tramite una procedura di gestione delle modifiche solida e approvata al fine di prevenire qualsiasi interruzione del servizio o violazione della sicurezza. • Il Fornitore deve garantire che le patch si riflettano negli ambienti di produzione e di disaster recovery (DR).	La mancata implementazione di questo controllo può dare luogo alla vulnerabilità dei servizi rispetto ai problemi di sicurezza che potrebbero compromettere i dati dei clienti, causare perdite di servizio o consentire altre attività dannose.
23. Simulazione di minaccia/ Test di penetrazione/	Il Fornitore deve coinvolgere un provider indipendente specializzato in servizi di sicurezza per eseguire una valutazione della sicurezza IT/simulazione della minaccia alle infrastrutture IT, compreso il disaster recovery, e alle applicazioni web relative ai servizi che il Fornitore eroga a Barclays.	In caso di mancata attuazione di questo controllo, i Fornitori potrebbero non essere in grado di valutare le minacce informatiche a

<table>
<tr>
<td>Valutazione della sicurezza IT</td>
<td>Questa procedura deve essere ripetuta almeno una volta all'anno per individuare le vulnerabilità che potrebbero essere sfruttate per violare la riservatezza dei dati di Barclays tramite attacchi cibernetici. Tutte le vulnerabilità devono ottenere la massima priorità e devono essere tracciate fino alla risoluzione. Il test deve essere svolto in linea con le Migliori Prassi del Settore.

Per i servizi erogati dai Fornitori relativamente all'infrastruttura/applicazione di Hosting per conto di Barclays.

• Il Fornitore deve informare e concordare con Barclays l'entità della valutazione della sicurezza, in particolare le date di inizio e fine, per prevenire l'interruzione delle attività principali di Barclays.
• Tutte le questioni di cui si è deciso di accettare il rischio devono essere comunicate e concordate con Barclays (Chief Security Office - ECAM team).
• Il Fornitore deve condividere con Barclays annualmente l'ultimo rapporto di valutazione della sicurezza (Chief Security Office - ECAM team)
• In caso di identificazione di vulnerabilità critiche/elevate, il Fornitore deve informare immediatamente Barclays.
• Il Fornitore deve rimediare alle vulnerabilità secondo le voci della tabella sottostante o in accordo con Barclays (Chief Security Office - ECAM team).

<table>
<tr><th>Priorità</th><th>Classificazione</th><th>Giorni di chiusura (massimo)</th></tr>
<tr><td>P1</td><td>Critica</td><td>15</td></tr>
<tr><td>P2</td><td>Alta</td><td>30</td></tr>
<tr><td>P3</td><td>Media</td><td>60</td></tr>
<tr><td>P4</td><td>Bassa</td><td>180</td></tr>
<tr><td>P5</td><td>A titolo informativo</td><td>360</td></tr>
</table>
</td>
<td>cui sono soggetti e l'idoneità e solidità delle proprie difese.

Le informazioni di Barclays possono essere divulgate e/o può verificarsi una perdita del servizio che può dare luogo a danni a livello normativo o reputazionale.</td>
</tr>
<tr>
<td>24. Crittografia</td>
<td>• Motivazione della crittografia - Il Fornitore deve documentare la motivazione per l'utilizzo della tecnologia crittografica ed esaminarla per assicurarsi che sia ancora adatta allo scopo.</td>
<td>Una protezione e algoritmi criptati aggiornati e adeguati garantiscono</td>
</tr>
</table>

	• Procedure del ciclo di vita della crittografia - Il Fornitore deve porre in essere e mantenere una serie documentata di procedure di gestione del ciclo di vita della crittografia che descrivano in dettaglio i processi end-to-end per la gestione delle chiavi dalla generazione, al caricamento, alla distribuzione fino alla distruzione. • Approvazione delle operazioni manuali - Il Fornitore deve garantire che tutti gli eventi gestiti dall'uomo per le chiavi e i certificati digitali, compresa la registrazione e la generazione di nuove chiavi e certificati, siano approvati ad un livello appropriato e che sia conservata una registrazione dell'approvazione. • Certificati digitali - Il Fornitore deve garantire che tutti i certificati siano ottenuti da una serie di Autorità di Certificazione (CA) approvate e controllate che dispongono di servizi di revoca e di politiche di gestione dei certificati e deve accertarsi che i certificati autofirmati siano utilizzati solo se tecnicamente non esiste la possibilità di supportare una soluzione basata su CA e deve disporre di controlli manuali per garantire l'integrità, l'autenticità delle chiavi e il raggiungimento tempestivo della revoca e del rinnovo. • Generazione di chiavi e criptoperiodo - Il Fornitore deve garantire che tutte le chiavi siano generate in modo casuale da un hardware certificato o da un CSPRNG (Cryptographically Secure Pseudo Random Number Generator - Generatore di numeri pseudo casuali crittograficamente sicuro) presente nel software. o Il Fornitore deve garantire che tutte le chiavi siano soggette ad un criptoperiodo di tempo limitato e definito per la loro sostituzione o disattivazione. Ciò deve essere in linea anche con il National Institute of Standards and Technology (NIST) e con le Migliori Prassi del Settore applicabili. • Protezione della conservazione delle chiavi - Il Fornitore deve garantire che le chiavi crittografiche segrete/private esistano solo nelle seguenti forme: o nel confine crittografico di un dispositivo/modulo hardware di sicurezza certificato. o In forma criptata sotto un'altra chiave stabilita o derivata da una password. o In componenti separati suddivisi tra gruppi di custodi distinti. o Cancellare nella memoria dell'host per il periodo dell'operazione di crittografia, a meno che non sia richiesta la protezione HSM. • Il Fornitore deve garantire che le chiavi siano generate e conservate entro i confini della memoria degli HSM per le chiavi ad alto rischio. Sono compresi: o Chiavi per i servizi regolamentati in cui la protezione HSM è obbligatoria. o Certificati che rappresentano Barclays da parte delle CA.	la protezione costante dei Patrimoni di dati di Barclays.

	o Certificati Root, Issuing, OCSP e RA (autorità di registrazione) utilizzati per l'emissione di Certificati a protezione dei servizi Barclays. o Chiavi che proteggono i repository aggregati memorizzati di chiavi, credenziali di autenticazione o dati PII. • Backup e conservazione delle chiavi - Il Fornitore mantiene un backup di tutte le chiavi per evitare l'interruzione del servizio nel caso in cui le chiavi si danneggino o richiedano il ripristino. L'accesso ai back-up è limitato a postazioni sicure che applicano il principio di 'split knowledge' e il doppio controllo. I backup delle chiavi devono avere una protezione crittografica almeno pari a quella delle chiavi in uso. • Inventario - Il Fornitore mantiene un inventario completo e aggiornato dell'uso della crittografia nei servizi che fornisce a Barclays, che descrive in dettaglio tutte le chiavi crittografiche, i certificati digitali e il software e l'hardware di crittografia gestiti dal Fornitore per prevenire danni in caso di incidente. Per dimostrare ciò, l'inventario revisionato viene firmato almeno ogni trimestre e fornito a Barclays. Gli inventari devono comprendere, se del caso: o Il Team di supporto IT o Le attività collegate o Algoritmi, lunghezza delle chiavi, ambiente, gerarchia delle chiavi, autorità di certificazione, impronte digitali, protezione dell'archiviazione delle chiavi e scopo tecnico e operativo. • Scopo funzionale e operativo - Le chiavi devono avere un unico scopo funzionale e operativo e non devono essere condivise tra più servizi o al di fuori dei servizi Barclays. • Processo di verifica - Il Fornitore deve eseguire e conservare la prova della revisione dei registri verificabili ogni trimestre almeno per tutti gli eventi di gestione del ciclo di vita delle chiavi e dei certificati che dimostrino una catena di custodia completa per tutte le chiavi, compresa la generazione, la distribuzione, il carico e la distruzione per rilevare qualsiasi uso non autorizzato. • Hardware - Il Fornitore conserva i dispositivi hardware in aree sicure e mantiene un processo di verifica per tutto il ciclo di vita della chiave per garantire che la catena di custodia dei dispositivi crittografici non sia compromessa. Questo processo viene rivisto su base trimestrale. o Il Fornitore deve garantire che l'hardware crittografico sia certificato almeno per il livello 2 di FIPS140-2 e che raggiunga il livello 3 nella Sicurezza Fisica e Gestione delle chiavi crittografiche o PCI HSM. Il Fornitore può scegliere di consentire l'utilizzo di smartcard basate su chip o di e-Token certificati FIPS come hardware accettabile per la	

	memorizzazione di chiavi che rappresentano e sono detenute da singole persone o clienti quando si trovano fuori sede. • Chiave compromessa - Il Fornitore mantiene e monitora un piano per le chiavi compromesse per garantire che le chiavi di ricambio siano generate indipendentemente dalla chiave compromessa per evitare che quest'ultima fornisca informazioni sulla sua sostituzione. Se si verifica un incidente di compromesso, Barclays deve essere notificato al **Barclays Chief Security Office (CSO) Joint Operations Centre (JOC) - gcsojoc@barclays.com.** • Solidità degli algoritmi e delle chiavi - Il Fornitore garantisce che gli algoritmi e la lunghezza delle chiavi in uso sono conformi al National Institute of Standards and Technology (NIST) e alle Migliori Prassi del Settore applicabili.	
25. Cloud Computing	Il Fornitore deve garantire che il servizio cloud utilizzato per i servizi Barclays deve avere un quadro di controlli di sicurezza ben definito per proteggere i concetti fondamentali di riservatezza, integrità e disponibilità e per garantire che i controlli di sicurezza siano in atto e funzionino efficacemente per proteggere i servizi Barclays. Per garantire che l'uso di tutta la tecnologia cloud sia sicuro, il Fornitore deve essere certificato ISO/IEC 27017 o 27001 o SOC 2 o avere un quadro di sicurezza simile per il cloud o agire secondo le Migliori Prassi del Settore con un sistema consolidato e misure di sicurezza implementate. Accertarsi che il Fornitore di servizi cloud sia certificato secondo le Migliori Prassi del Settore, compresi i controlli appropriati equivalenti all'ultima versione della Cloud Security Alliance, Cloud Controls Matrix (CCM). Spetta al Fornitore garantire i controlli di sicurezza dei dati relativi al Patrimonio informatico / ai Dati di Barclays, compresi i dati personali all'interno del cloud e il fornitore di servizi cloud CSP è responsabile della sicurezza del servizio cloud. Il Fornitore rimane responsabile della configurazione e del monitoraggio dell'implementazione dei controlli di sicurezza per una protezione attiva da qualsiasi incidente di sicurezza, comprese le violazioni dei dati. Il Fornitore deve implementare misure di sicurezza in tutti gli aspetti del servizio fornito, compreso il modello di responsabilità condivisa del cloud, in modo tale da salvaguardare la riservatezza, l'integrità, la disponibilità e l'accessibilità, riducendo al minimo la possibilità che persone non autorizzate abbiano accesso alle informazioni di Barclays e ai servizi utilizzati da Barclays. I controlli di sicurezza in cloud devono coprire,	La mancata implementazione di questo controllo cloud potrebbe compromettere i Dati Barclays e tale condizione può dare luogo a danni a livello normativo o reputazionale.

	a titolo esemplificativo ma non esaustivo, i seguenti domini per i modelli di distribuzione (IaaS/PaaS/SaaS): • Meccanismi di governance e responsabilità • Gestione delle identità e degli accessi • Sicurezza della rete (compresa la connettività) • Sicurezza dei dati (Transito/Sosta/Archiviazione) • Crittografia, criptazione e gestione delle chiavi - CEK • Registrazione e monitoraggio • Virtualizzazione • Separazione dei servizi Il Patrimonio informatico / i Dati di Barclays compresi i dati personali memorizzati nel Cloud come parte del servizio reso a Barclays devono essere approvati da Barclays (Chief Security Office - team ECAM). Se i dati sensibili (personali e riservati) sono conservati presso un fornitore di servizi cloud, il Fornitore si impegna a comunicare a Barclays i luoghi, le zone dati e le zone dati di failover dove questi dati saranno conservati.	
26. Spazio dedicato alla banca (Bank Dedicated Space - BDS)	Per i servizi forniti che richiedono uno Spazio Bancario Dedicato (Bank Dedicated Space - BDS) ufficiale, devono essere attivati requisiti fisici e tecnici BDS specifici. (Se BDS è un requisito per il servizio, saranno applicabili i requisiti di controllo.) I diversi tipi di BDS sono: Livello 1 (Prima classe) - L'intera infrastruttura IT è gestita da **Barclays** attraverso la fornitura di una LAN, WAN & Desktop gestita da **Barclays** ad un sito Fornitore con uno spazio dedicato Barclays. Livello 2 (Business class) - L'intera infrastruttura IT è gestita dal **Fornitore** e si collega ai gateway Extranet di **Barclays** - i dispositivi LAN, WAN & Desktop sono di proprietà e gestiti dal Fornitore. Livello 3 (Classe Economy) - L'intera infrastruttura IT è gestita dal **Fornitore** e si collega ai gateway Internet **Barclays** - i dispositivi LAN, WAN & Desktop sono di proprietà e gestiti dal Fornitore.	La mancata implementazione di questo controllo impedisce di attivare gli adeguati controlli fisici e tecnici provocando ritardi o interruzione dell'erogazione del servizio o violazioni della sicurezza informatica / incidenti di sicurezza.

26.1 BDS - Separazione fisica	L'area fisica occupata deve essere dedicata a Barclays e non condivisa con altre società / altri venditori. Deve essere logicamente e fisicamente separata.
26.2 BDS - Controllo dell'accesso fisico	• Il Fornitore deve porre in essere un processo di accesso fisico che copra i metodi di accesso e l'autorizzazione al BDS nel luogo in cui vengono erogati i servizi. • L'ingresso e l'uscita verso le aree BDS devono essere limitati e monitorati da meccanismi di controllo dell'accesso fisico per garantire che l'accesso sia consentito solo al personale autorizzato. • Una carta d'accesso elettronica autorizzata per accedere alle aree BDS degli uffici. • Il Fornitore deve effettuare controlli trimestrali per garantire che solo le persone autorizzate abbiano accesso alle aree BDS. Le eccezioni vengono studiate a fondo fino alla risoluzione. • I diritti di accesso vengono rimossi entro 24 ore per tutti gli utenti soggetti a spostamenti o dimissioni (conservando le registrazioni pertinenti). • Utilizzare i guardiani per pattugliare abitualmente l'interno delle aree BDS per identificare efficacemente gli accessi non autorizzati o le attività potenzialmente dannose. • Per l'accesso a BDS devono essere svolti controlli automatici di sicurezza, tra cui: In caso di personale autorizzato: o Tesserino identificativo con foto sempre visibile o Sono utilizzati lettori ottici di card o Sono attivi dispositivi anti-pass back • Il Fornitore deve disporre di processi e procedure per il controllo e il monitoraggio di persone esterne, comprese le terze parti con accesso fisico alle aree BDS a scopo di manutenzione e pulizia.
26.3 BDS - Videosorveglianza	• Implementare la videosorveglianza per le aree BDS per individuare efficacemente gli accessi non autorizzati o le attività dannose e contribuire alle indagini. • Tutti i punti di entrata e uscita dell'area BDS devono essere videosorvegliati. • Le telecamere di sicurezza sono posizionate in modo appropriato e forniscono immagini chiare e identificabili in ogni momento per catturare attività dannose e contribuire alle indagini. Il Fornitore deve conservare le riprese TVCC catturate per 30 giorni e tutte le registrazioni TVCC e i registratori devono essere posizionati in modo sicuro per evitare la modifica, la cancellazione o la visione "casuale" di eventuali schermi TVCC associati e l'accesso alle registrazioni deve essere controllato e limitato solo alle persone autorizzate.
26.4 BDS - Accesso alla rete Barclays e ai token di	• Ciascun utente che vuole autenticarsi sulla rete Barclays dall'area BDS, può utilizzare esclusivamente un dispositivo di autenticazione a più fattori fornito da Barclays. • Il Fornitore deve conservare i registri delle persone a cui sono stati forniti i token di autenticazione Barclays e deve eseguire una riconciliazione su base trimestrale.

autenticazione Barclays	• Barclays disattiverà entro ventiquattro (24) ore le credenziali di autenticazione non appena sarà notificato che l'accesso non è più necessario (ad es. licenziamento di un dipendente, riassegnazione di un progetto, ecc.). • Barclays disattiverà prontamente le credenziali di autenticazione nel caso in cui tali credenziali non siano state utilizzate per un periodo di tempo (tale periodo di non utilizzo non deve superare un mese). • I servizi che hanno accesso alla stampa remota tramite l'applicazione Barclays Citrix devono essere approvati e autorizzati da Barclays (Chief Security Office - ECAM Team). Il Fornitore deve mantenere i registri ed eseguire la riconciliazione trimestrale. Riferirsi al controllo - 12. Lavoro a distanza (accesso remoto)
26.5 BDS - Supporto di Out of Office	L'accesso remoto all'area BDS non è fornito di default per il supporto di out of office/out of business/work from home. Qualsiasi Accesso Remoto deve essere approvato dalle funzioni di Barclays pertinenti (compreso il Chief Security Office – ECAM team)
26.6 BDS - Sicurezza della rete	• Mantenere un inventario aggiornato di tutti i perimetri della rete dell'organizzazione (attraverso un'Architettura di Rete/Diagramma). • La progettazione e l'implementazione della rete deve essere rivista almeno una volta all'anno. • La rete BDS deve essere separata in modo logico dalla rete aziendale del Fornitore da un Firewall e tutto il traffico in entrata e in uscita deve essere limitato e monitorato. • La configurazione del percorso deve garantire solo le connessioni alla rete Barclays e non deve condurre ad altre reti del Fornitore. • Il router Supplier Edge che si collega ai gateway extranet di Barclays deve essere configurato in modo sicuro con un concetto di limitazione dei controlli di porte, protocolli e servizi; o Assicurarsi che la registrazione e il monitoraggio siano abilitati. • La rete BDS deve essere monitorata e consentita esclusivamente ai dispositivi autorizzati, tramite adeguati controlli di accesso alla rete Riferirsi al controllo - 10. Sicurezza del perimetro e della rete
26.7 BDS - Rete wireless	Le reti wireless devono essere disabilitate per il segmento delle reti Barclays in cui si erogano i servizi di Barclays.
26.8 BDS - Sicurezza degli endpoint	È necessario configurare in modo sicuro e conformemente alle Migliori Prassi del Settore la struttura dei desktop dei computer che utilizzano la rete BDS. Devono essere messe in atto le Migliori Prassi del Settore e la struttura di sicurezza dei dispositivi endpoint deve includere, a titolo esemplificativo ma non esaustivo: • crittografia del disco;

	• disattivare tutti i software/servizi/porte non necessari; • disattivare l'accesso ai diritti di amministrazione per l'utente locale • il personale del Fornitore non potrà modificare le impostazioni di base come il Service Pack predefinito e i servizi predefiniti, ecc.; • la porta USB deve essere disabilitata per vietare la copia dei dati Barclays su supporti esterni; • aggiornata con le ultime firme antivirus e patch di sicurezza; • prevenzione della perdita di dati limitata al divieto di taglia-copia-incolla e stampa-schermo o stampa schermo dei dati Barclays; • come impostazione predefinita, l'accesso alla stampante deve essere disabilitato; • la condivisione / il trasferimento del Patrimonio informatico / dei Dati di Barclays durante l'utilizzo di strumenti/software di messaggistica istantanea devono essere disabilitati; • capacità e processi per rilevare software non autorizzati identificati come dannosi e impedire l'installazione di software non autorizzati; Riferirsi al controllo - 16. Sicurezza dell'endpoint	

26.9 BDS - E-mail e Internet	• La connettività di rete deve essere configurata in modo sicuro per limitare le e-mail e l'attività Internet sulla rete BDS.
	• Il Fornitore deve limitare la capacità di accedere a siti di social network, servizi di webmail e siti con la possibilità di memorizzare informazioni su Internet come google drive, Dropbox, iCloud.
	• Il trasferimento non autorizzato di dati Barclays al di fuori della rete BDS deve essere protetto dalla perdita di dati:
	  • E-mail
	  • Internet/Web Gateway (inclusi archiviazione on-line e webmail)
	• Applicare filtri URL basati sulla rete che limitano la capacità di un sistema di connettersi solo a siti web interni o Internet dell'organizzazione del Fornitore
	• Bloccare tutti gli allegati e/o la funzione di caricamento sui siti web.
	• Accertarsi che siano ammessi solo i browser web e i client di posta elettronica completamente supportati.	

26.10 BDS - BYOD/Dispositivo personale	**I dispositivi personali/BYOD non devono essere autorizzati ad accedere all'ambiente Barclays e/o ai dati Barclays**	
Diritto di ispezione	I Fornitori devono consentire a Barclays, previo preavviso scritto di Barclays di almeno dieci (10) giorni lavorativi, di svolgere un controllo di sicurezza di qualsiasi luogo o tecnologia utilizzati dal Fornitore o dai Subfornitori per sviluppare, testare, migliorare, eseguire la manutenzione o gestire i sistemi del Fornitore utilizzati per i Servizi, al fine di controllare il rispetto degli obblighi da parte del Fornitore. Il Fornitore deve inoltre	In caso di mancato accordo i Fornitori non saranno in grado di fornire la piena garanzia della conformità a tali obblighi di sicurezza.

	consentire a Barclays di svolgere un'ispezione almeno una volta all'anno o subito dopo il verificarsi di un incidente di sicurezza. Eventuali non-conformità individuate da Barclays durante un'ispezione devono essere sottoposte a valutazione dei rischi da parte di Barclays, che specificherà una tempistica per la relativa correzione. Il Fornitore è quindi tenuto a completare eventuali interventi correttivi entro tale periodo. Il Fornitore deve fornire tutta l'assistenza ragionevolmente richiesta da Barclays in relazione alle ispezioni effettuate e la documentazione presentata durante l'ispezione deve essere completata e restituita a Barclays.	

Appendice A: Glossario

Definizioni	
Account	Serie di credenziali (per esempio, ID utente e password) che consentono di gestire gli accessi ai sistemi IT tramite controlli sugli accessi logici.
Backup, Back-up	Un backup o la procedura di esecuzione del backup si riferisce alla realizzazione di copie dei dati che possono essere utilizzate per ripristinare gli originali dopo un evento di perdita dati.
Spazio dedicato alla banca	BDS (Bank Dedicated Space - Spazio Bancario Dedicato) indica i locali posseduti o controllati dai Membri del Gruppo del Fornitore o dai Subfornitori che sono dedicati in esclusiva a Barclays in cui sono realizzati o erogati i Servizi.
Migliori Prassi del Settore	Utilizzo delle migliori e attuali prassi, processi, standard e certificazioni leader di mercato, esercitando quel grado di abilità e cura che ci si potrebbe ragionevolmente aspettare da un'organizzazione professionale altamente qualificata, esperta e leader di mercato, impegnata nella fornitura di servizi uguali o simili a quelli forniti a Barclays.
BYOD	Bring your own devices (Portare i propri dispositivi)
Crittografia	L'applicazione di teorie matematiche per sviluppare tecniche e algoritmi che possono essere applicati ai dati per garantire di raggiungere obiettivi come la riservatezza, l'integrità dei dati e/o l'autenticazione.
Sicurezza cibernetica	L'applicazione di tecnologie, processi, controlli e misure organizzative per proteggere sistemi informatici, reti, programmi, dispositivi e dati da attacchi digitali che possono comportare (a titolo esemplificativo ma non esaustivo), divulgazione non autorizzata, distruzione, perdita, alterazione, furto o danni a hardware, software o Dati.
Dati	La registrazione di fatti, concetti o istruzioni su un supporto di memorizzazione per la comunicazione, il recupero e l'elaborazione con mezzi automatici e la presentazione come informazione comprensibile per l'uomo.
Rifiuto del servizio (Attacco)	Tentativo di rendere non disponibile per gli utenti cui è destinata una risorsa informatica.
Distruzione / Cancellazione	L'azione di sovrascrivere, cancellare o distruggere fisicamente informazioni in modo tale che non possano essere recuperate.
ECAM	Team Esterno di Cyber Assurance e Monitoraggio che valuta la posizione di sicurezza del Fornitore
Criptazione	La trasformazione di un messaggio (dati, vocale o video) in un formato privo di senso che non può essere compreso da lettori non autorizzati. Questa trasformazione avviene da formato di testo a formato cifrato.
HSM	Hardware Security Module (Modulo di sicurezza hardware). Un dispositivo dedicato che fornisce la generazione, la memorizzazione e l'utilizzo sicuro delle chiavi crittografiche, compresa l'accelerazione dei processi crittografici.
Patrimonio di dati	Qualsiasi informazione che abbia valore, considerata nei termini dei requisiti di riservatezza, integrità e disponibilità. Oppure qualsiasi singola Informazione o insieme di Informazioni che abbia valore per l'organizzazione.
Titolare del patrimonio di dati	Il dipendente nell'ambito dell'organizzazione che è responsabile della classificazione di un patrimonio e della sua corretta gestione.
Privilegio minimo	Il livello minimo di accesso/permesso che consente a un Utente o account di svolgere il proprio ruolo aziendale.

Dispositivo di rete/Apparecchiature di rete	Qualsiasi dispositivo IT collegato ad una rete che viene utilizzato per gestire, supportare o controllare una rete. Possono essere inclusi, a titolo esemplificativo, router, switch, firewall, bilanciatori di carico.
Codice nocivo	Software scritto con l'intenzione di eludere la procedura di sicurezza di un sistema IT, dispositivo o applicazione. Tra gli esempi troviamo virus, Trojan e worm.
Multi-Factor Authentication (MFA - Autenticazione a più fattori)	Autenticazione che richiede due o più diverse tecniche di autenticazione. Un esempio è l'uso di un token di sicurezza, dove il successo dell'autenticazione dipende da qualcosa che è in possesso della persona (cioè il token di sicurezza) e da qualcosa che l'utente conosce (cioè il PIN del token di sicurezza).
Dati personali	Qualsiasi informazione relativa a una persona fisica identificata o identificabile ("persona interessata"); una persona fisica identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento a un identificatore come nome, codice fiscale, dati di localizzazione, identificatore on-line o a uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica.
Accesso privilegiato	Assegnazione di accesso speciale (al di sopra dello standard), permessi o facoltà a un utente, processo o computer.
Account privilegiato	Un account che fornisce un livello di controllo elevato su un sistema IT specifico. Questi account di solito sono usati per la manutenzione, l'amministrazione della sicurezza e le modifiche di configurazione dei sistemi IT. A titolo esemplificativo, si possono citare gli account "amministratore", "radice" e Unix con uid=0, account di supporto, di amministrazione della sicurezza e di amministrazione del sistema e amministratore locale.
Accesso remoto	Tecnologia e tecniche utilizzate per dare agli utenti autorizzati l'accesso alle reti e ai sistemi di un'organizzazione da un luogo fuori sede.
Sistema	Un sistema, nel contesto del presente documento, si riferisce a persone, procedure, attrezzature IT e software. Gli elementi di questa entità composita sono utilizzati insieme nell'ambiente operativo o di supporto per svolgere una determinata attività o raggiungere una finalità specifica, con funzione di supporto o quale requisito di missione.
Deve, è tenuto a	Questa definizione significa che le implicazioni saranno pienamente comprese e attentamente valutate.
Incidente di sicurezza	Sono definiti incidenti di sicurezza gli eventi che comprendono, a titolo esemplificativo ma non esaustivo: • Tentativi (falliti o riusciti) di accesso non autorizzato ad un sistema o ai rispettivi dati. • Interruzione indesiderata o rifiuto di servizio. • Uso non autorizzato di un sistema per l'elaborazione o la memorizzazione dei dati. • Modifiche alle caratteristiche hardware, firmware o software del sistema senza che il proprietario ne sia a conoscenza o fornisca istruzioni o consenso. • Vulnerabilità dell'applicazione che comporta un accesso non autorizzato ai dati.

Appendice B: Schema di Etichettatura delle informazioni di Barclays

Tabella B1: Schema di Etichettatura delle informazioni di Barclays

Etichetta	Definizione	Esempi
Segrete	Le informazioni devono essere classificate come **Segrete** se la loro divulgazione non autorizzata potrebbe avere un impatto negativo su Barclays, valutato nell'ambito dell'Enterprise Risk Management Framework (ERMF - Quadro di gestione del rischio d'impresa) come "Critico" (a livello finanziario o non finanziario). Queste informazioni sono destinate a un target specifico e non devono essere divulgate ulteriormente senza l'autorizzazione dell'autore. Il target può comprendere destinatari esterni su esplicita autorizzazione del titolare delle informazioni.	• Informazioni su potenziali fusioni e acquisizioni • Informazioni di pianificazione strategica, a livello aziendale e organizzativo • Determinate informazioni sulla configurazione di sicurezza • Determinati risultati di audit e rapporti • Verbali dei comitati esecutivi • Dettagli di Autenticazione o Identificazione e verifica (ID&V) – cliente e collega • Grandi volumi di informazioni sui titolari di carte • Previsioni di profitto e risultati finanziari annuali (prima della divulgazione pubblica) • Qualsiasi punto che rientri nell'ambito di un Non-Disclosure Agreement (NDA - Accordo di non divulgazione) ufficiale
Riservata – Interna	Le informazioni devono essere classificate come **Riservata - Interna** se i destinatari previsti sono solo dipendenti Barclays autenticati e Managed Service Providers (MSP - Provider di servizi gestiti) in possesso di un contratto attivo che riguarda un target specifico. La divulgazione non autorizzata potrebbe avere un impatto negativo su Barclays, valutato nell'ambito dell'ERMF come "Principale" o "Limitato" (a livello finanziario o non finanziario). Queste informazioni non sono destinate alla diffusione generale ma possono essere inoltrate o condivise dai destinatari secondo il principio need-to-know.	• Strategie e budget • Stime delle performance • Remunerazione dei dipendenti e Dati Personali • Valutazioni di vulnerabilità
Riservata – Esterna	Le informazioni devono essere classificate come **Riservata - Esterna** se i destinatari previsti sono dipendenti Barclays autenticati e MSP in possesso di un contratto attivo che riguarda un target specifico o parti esterne autorizzate dal titolare delle informazioni. La divulgazione non autorizzata potrebbe avere un impatto negativo su Barclays, valutato nell'ambito dell'ERMF come "Principale" o "Limitato" (a livello finanziario o non finanziario).	• Nuovi piani di prodotto • Contratti con i clienti • Contratti legali • Informazioni relative a clienti singoli/a basso volume da inviare all'esterno • Comunicazioni relative ai clienti. • Nuovi materiali per offerte (ad es. prospetti, promemoria per offerte) • Documenti di ricerca definitivi

	Queste informazioni non sono destinate alla diffusione generale ma possono essere inoltrate o condivise dai destinatari secondo il principio need-to-know.	• Informazioni essenziali non pubbliche (Material Non-Public Information - MNPI) esterne a Barclays • Tutti i report di ricerca • Alcuni materiali di marketing • Commenti del mercato • Risultati di audit e rapporti
Non riservate	Le informazioni destinate alla diffusione generale o la cui divulgazione non avrebbe un impatto negativo sull'organizzazione devono essere classificate come Non riservate.	• Materiali di marketing • Pubblicazioni • Annunci pubblici • Annunci di lavoro • Informazioni che non influiscono su Barclays

Tabella B2: Schema di Etichettatura delle informazioni di Barclays - Requisiti di gestione

*** Informazioni sulla configurazione di sicurezza dei sistemi, risultati di audit e documenti personali possono essere classificati come Riservati - Interni o Segreti a seconda dell'impatto sull'attività aziendale della loro divulgazione non autorizzata

Fase del ciclo di vita	Segrete	Riservata – Interna	Riservata – Esterna
Creazione e introduzione	• Ai Patrimoni di Dati deve essere assegnato un Titolare delle Informazioni.	• Ai Patrimoni di Dati deve essere assegnato un Titolare delle Informazioni.	• Ai Patrimoni di Dati deve essere assegnato un Titolare delle Informazioni.
Conservazione	• I patrimoni di dati (sia fisici sia elettronici) non devono essere conservati in luoghi in cui persone non autorizzate possano visualizzarli o accedervi. • I patrimoni di dati elettronici memorizzati devono essere protetti tramite criptaggio o controlli compensativi appropriati, qualora sussista un rischio elevato di accesso agli stessi da parte di persone non autorizzate.	• I dati (sia fisici che elettronici) non devono essere conservati in aree pubbliche (ivi comprese le aree pubbliche nei locali a cui i visitatori possono avere accesso non controllato). • Le informazioni non devono essere lasciate in aree pubbliche nei locali a cui i visitatori possono avere accesso non controllato.	• I patrimoni di dati (sia fisici sia elettronici) non devono essere conservati in luoghi in cui persone non autorizzate possano visualizzarli o accedervi. • I patrimoni di dati elettronici memorizzati devono essere protetti tramite criptaggio o controlli compensativi appropriati, qualora sussista un rischio elevato di accesso agli stessi da parte di persone non autorizzate.

	• Tutte le chiavi private che sono utilizzate per proteggere i dati, l'identità e/o la reputazione di Barclays devono essere protette da moduli per la sicurezza dell'hardware certificati FIPS 140-2 Livello 3 o superiore (HSM).		
Accesso e uso	• Non si deve lavorare su patrimoni di dati (sia fisici sia elettronici), né lasciarli incustoditi in luoghi in cui persone non autorizzate possano visualizzarli o accedervi. È possibile lavorare su patrimoni di dati se sussistono controlli adeguati (per esempio schermi per la privacy). • Si devono usare strumenti di stampa sicuri per stampare i patrimoni di dati. • I patrimoni di dati elettronici devono essere protetti mediante controlli Logical Access Management appropriati	• I dati (sia fisici che elettronici) non devono essere lasciati in aree pubbliche all'esterno dei locali. • I dati (sia fisici che elettronici) non devono essere lasciati in aree pubbliche nei locali a cui i visitatori possono avere accesso non controllato. • Se necessario, i patrimoni di dati elettronici devono essere protetti mediante controlli Logical Access Management appropriati	• Non si deve lavorare su patrimoni di dati (sia fisici sia elettronici), né lasciarli incustoditi in luoghi in cui persone non autorizzate possano visualizzarli o accedervi. È possibile lavorare su patrimoni di dati se sussistono controlli adeguati (per esempio schermi per la privacy). • I patrimoni di dati stampati devono essere recuperati immediatamente dalla stampante. Ove ciò non sia possibile, occorre usare strumenti di stampa sicuri. • I dati elettronici devono essere protetti mediante controlli Logical Access Management appropriati
Condivisione	• Le copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile su ciascuna pagina. • Le buste contenenti copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile sul lato frontale ed essere chiuse con un sigillo che riveli eventuali tentativi di manomissione. Prima della distribuzione, inoltre, devono essere inserite in una seconda busta priva di etichetta. • I patrimoni di dati elettronici devono essere corredati di chiara etichetta informativa. Le copie elettroniche dei documenti di più pagine devono essere corredate di etichetta informativa visibile su ciascuna pagina.	• Le copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile. L'etichetta deve essere apposta per lo meno sulla copertina. • I patrimoni di dati elettronici devono essere corredati di chiara etichetta informativa. • I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione. • I patrimoni di dati devono essere distribuiti esclusivamente ai dipendenti dell'organizzazione o a individui vincolati a quest'ultima da un obbligo contrattuale appropriato o per assolvere a un'esigenza aziendale chiaramente riconosciuta, come una negoziazione contrattuale.	• Le copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile. L'etichetta deve essere apposta per lo meno sulla copertina. • Le buste contenenti copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile sul lato frontale. • I patrimoni di dati elettronici devono essere corredati di chiara etichetta informativa. Le copie elettroniche dei documenti di più pagine devono essere corredate di etichetta informativa visibile su ciascuna pagina. • I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione.

	• I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione. • I patrimoni di dati devono essere distribuiti esclusivamente ai dipendenti dell'organizzazione o a individui vincolati a quest'ultima da un obbligo contrattuale appropriato o per assolvere a un'esigenza aziendale chiaramente riconosciuta, come una negoziazione contrattuale. • I Patrimoni di Dati devono essere distribuiti esclusivamente alle persone specificamente autorizzate a riceverli dal Titolare del Patrimonio di Dati. • I patrimoni di dati non devono essere inviati via fax. • Durante il transito al di fuori della rete interna, i patrimoni di dati elettronici devono essere criptati tramite un dispositivo di protezione crittografica approvato. • Occorre implementare una catena di custodia dei patrimoni di dati elettronici.		• I patrimoni di dati devono essere distribuiti esclusivamente ai dipendenti dell'organizzazione o a individui vincolati a quest'ultima da un obbligo contrattuale appropriato o per assolvere a un'esigenza aziendale chiaramente riconosciuta, come una negoziazione contrattuale. • I patrimoni di dati devono essere distribuiti esclusivamente alle persone che hanno necessità di riceverli per motivi connessi alla loro attività. • I patrimoni di dati non devono essere inviati via fax, a meno che il mittente non abbia verificato che i destinatari sono pronti a ritirare il fax. • Durante il transito al di fuori della rete interna, i patrimoni di dati elettronici devono essere criptati tramite un dispositivo di protezione crittografica approvato.
Archiviazione ed eliminazione	• Le copie cartacee dei patrimoni di dati devono essere eliminate tramite un servizio di eliminazione riservato. • Le copie dei patrimoni di dati elettronici devono essere cancellate in modo tempestivo anche dai "cestini" del sistema o da dispositivi analoghi. • I supporti su cui sono stati memorizzati i patrimoni di dati elettronici segreti devono essere depurati in modo appropriato prima o durante l'eliminazione.	• Le copie cartacee dei patrimoni di dati devono essere eliminate tramite un servizio di eliminazione riservato. • Le copie dei patrimoni di dati elettronici devono essere cancellate in modo tempestivo anche dai "cestini" del sistema o da dispositivi analoghi.	• Le copie cartacee dei patrimoni di dati devono essere eliminate tramite un servizio di eliminazione riservato. • Le copie dei patrimoni di dati elettronici devono essere cancellate in modo tempestivo anche dai "cestini" del sistema o da dispositivi analoghi.

Segreto bancario

Ulteriori controlli solo per giurisdizioni che prevedono il segreto bancario (Svizzera/Monaco)

Area di controllo / Titolo	Descrizione del controllo	Perché è importante?
1. Ruoli e responsabilità	Il Fornitore deve definire e comunicare ruoli, responsabilità e competenze per la gestione dei Dati identificativi del cliente (Client Identifying Data - CID). Il Fornitore deve rivedere i documenti che specificano ruoli, responsabilità e competenze per i CID dopo qualsiasi modifica sostanziale al modello operativo (o alle attività) del Fornitore o almeno una volta all'anno e consegnarli alla pertinente giurisdizione che prevede il segreto bancario. I ruoli principali devono comprendere un senior executive, responsabile per la protezione e la supervisione di tutte le attività collegate ai CID (fare riferimento all'Appendice A per la definizione di CID). Il numero delle persone che accedono al CID deve essere ridotto al minimo, in base al principio della necessità di conoscere.	La chiara definizione dei ruoli e delle responsabilità supporta l'attuazione del Programma sugli Obblighi di controllo dei Fornitori esterni.
2. Segnalazione di violazione dei CID	Occorre implementare controlli, processi e procedure documentati per assicurare che qualsiasi violazione che ha ripercussioni sui CID sia segnalata e gestita. Il Fornitore deve rispondere a qualsiasi violazione dei requisiti di gestione (come definiti nella tabella B2) e segnalarla immediatamente all'entità Barclays pertinente che prevede il Segreto Bancario (al massimo entro 24 ore). Deve essere istituita e regolarmente verificata una procedura di risposta agli incidenti per la tempestiva gestione e regolare segnalazione degli eventi che riguardano i CID. Il Fornitore deve aver cura di eliminare le carenze individuate con un piano di intervento correttivo (azione, proprietà, data di esecuzione) comunicato alla relativa giurisdizione che prevede il segreto bancario. Le azioni correttive devono essere attuate dal Fornitore in modo tempestivo. Nel caso in cui il Fornitore esterno eroghi servizi di consulenza, e un dipendente di tale Fornitore abbia innescato incidenti per la prevenzione della perdita di dati, la Banca notificherà l'incidente al Fornitore e, se del caso, la Banca ha il diritto di richiedere la sostituzione del dipendente.	Un processo di risposta agli incidenti aiuta a garantire che vengano rapidamente circoscritti e che ne venga impedita l'escalation. Qualsiasi violazione che riguarda i CID può comportare seri danni reputazionali e ammende per Barclays, oltre alla perdita dell'autorizzazione bancaria in Svizzera e Monaco

3. Formazione e consapevolezza	I dipendenti del Fornitore che accedono ai CID e/o li gestiscono devono ricevere un'adeguata formazione* che copra i Requisiti di Segretezza bancaria dei CID dopo ogni modifica dei regolamenti o almeno una volta all'anno. Il Fornitore deve garantire che tutto il nuovo personale alle proprie dipendenze (che ha accesso ai CID e/o li gestisce), entro un periodo di tempo ragionevole (circa 3 mesi), completi un corso di formazione che garantisca la comprensione delle rispettive responsabilità rispetto ai CID. Il Fornitore deve tenere traccia dei dipendenti che completano la formazione. * le giurisdizioni che prevedono il segreto bancario forniscono le linee guida sui contenuti previsti per il corso di formazione.	Formazione e consapevolezza supportano tutti gli altri controlli nell'ambito di questo programma.
4. Schema di Etichettatura delle informazioni	*Laddove appropriato**, il Fornitore deve applicare lo Schema di Etichettatura delle Informazioni di Barclays (Appendice E, Tabella E1), o uno schema alternativo concordato con la giurisdizione che prevede il segreto bancario, per tutto il Patrimonio di dati conservati o elaborati per conto della stessa. I requisiti di gestione per i dati CID sono esposti nella Tabella E2 dell'Appendice E. * "*laddove appropriato*" *fa riferimento al vantaggio derivante dall'etichettatura in rapporto al rischio che comporta. Per esempio, non sarebbe appropriato etichettare un documento se, così facendo, si violassero i requisiti normativi antimanomissione.*	Un inventario completo e accurato del patrimonio di dati è essenziale per garantire controlli appropriati.
5. Cloud Computing/Archiviazione esterna	L'uso del cloud computing e/o dell'archiviazione esterna dei CID (in server non ubicati nella giurisdizione che prevede il segreto bancario o esterni alle infrastrutture del Fornitore) nell'ambito di servizi resi per tale giurisdizione deve essere approvato dai corrispondenti team locali pertinenti (tra cui il Chief Security Office, Conformità e Legal); inoltre devono essere implementati i necessari controlli conformemente alle leggi e alle normative applicabili della giurisdizione che prevede il segreto bancario pertinente per proteggere i CID rispetto al profilo ad alto rischio che presentano.	La mancata implementazione di questo principio potrebbe compromettere i dati del Cliente (CID) protetti in modo non idoneo; tale condizione può dare luogo a provvedimenti normativi o generare danni alla reputazione.

Appendice C: Glossario

** I dati identificativi del cliente sono dati speciali che tengono conto delle leggi sul Segreto Bancario in vigore in Svizzera e Monaco. A tal fine, i controlli qui elencati sono complementari a quelli elencati in precedenza.

Termine	Definizione
CID	Client Identifying Data (Dati identificativi del cliente)
CIS	Cyber and Information Security (Sicurezza cibernetica e informatica)
Dipendente del Fornitore	Qualsiasi persona assunta direttamente dal Fornitore come dipendente a tempo indeterminato, o qualsiasi persona che eroga servizi al Fornitore per un periodo di tempo limitato (come un consulente)
Patrimonio	Qualsiasi singola informazione o insieme di informazioni che abbia valore per l'organizzazione
Sistema	Un sistema, nel contesto del presente documento, si riferisce a persone, procedure, attrezzature IT e software. Gli elementi di questa entità composita sono utilizzati insieme nell'ambiente operativo o di supporto per svolgere una determinata attività o raggiungere una finalità specifica, con funzione di supporto o quale requisito di missione.
Utente	Un account assegnato a un dipendente, consulente, consulente esterno o lavoratore temporaneo del Fornitore che sia autorizzato ad accedere a un sistema di proprietà di Barclays senza privilegi elevati.

Appendice D: DEFINIZIONE DI DATI IDENTIFICATIVI DEL CLIENTE

ICID Diretti (DCID) possono essere definiti come identificatori unici (di proprietà del cliente), che consentono, in quanto tali e di per sé, di identificare un cliente senza accedere ai dati contenuti nelle applicazioni bancarie di Barclays. Tali dati devono essere inequivocabili, non soggetti a interpretazione e possono comprendere informazioni come nome, cognome, nome dell'azienda, firma, ID dei social network, ecc. I CID diretti si riferiscono a dati del cliente che non sono di proprietà della banca o creati da quest'ultima.

I CID Indiretti (ICID) sono suddivisi in 3 livelli

- L1 ICID possono essere definiti come identificatori unici (di proprietà della Banca) che permettono di identificare in modo univoco un cliente nel caso in cui sia disposto l'accesso alle applicazioni bancarie o ad altre applicazioni di terze parti. L'identificatore deve essere inequivocabile, non soggetto a interpretazioni e può includere identificatori come numero di conto, codice IBAN, numero di carta di credito, ecc.
- L2 ICID possono essere definite come informazioni (di proprietà del cliente) che, unitamente ad altre, forniscono conclusioni sull'identità di un cliente. Mentre queste informazioni non possono essere utilizzate per identificare un cliente di per sé, possono essere usate insieme ad altre informazioni per identificare un cliente. L2 ICID devono essere protetti e gestiti con la stessa diligenza utilizzata per i D CID.
- L3 ICID possono essere definiti come identificatori unici ma anonimizzati (di proprietà della Banca) che permettono di identificare un cliente che dispone dell'accesso alle applicazioni bancarie. La differenza con L1 ICID risiede nella Classificazione delle Informazioni come Riservate - Esterne invece di Segreto Bancario, che significa che non sono soggette agli stessi controlli.

Fare riferimento alla Figura 1 CID Schema Decisionale per una panoramica del metodo di classificazione.

Gli L1 ICID Diretti e Indiretti non devono essere condivisi con persone esterne alla Banca e devono rispettare in qualsiasi momento il principio need-to-know. Gli L2 ICID possono essere condivisi sulla base del principio need-to-know ma non possono essere condivisi unitamente a qualsiasi altra parte di CID. Condividendo più parti di CID esiste la possibilità di creare una 'combinazione tossica' che potenzialmente potrebbe rivelare l'identità del cliente. Si crea una combinazione tossica con la combinazione di almeno due L2 ICID. Gli L3 ICID possono essere condivisi poi ché non sono classificati come informazioni a livello di Segreto Bancario a meno che l'uso ripetuto dello stesso identificatore possa dare luogo all'ottenimento di dati L2 ICID sufficienti a rivelare l'identità del cliente.

Classificazione delle informazioni	Segreto bancario			Riservata – Interna
Classificazione	CID diretto (DCID)	CID indiretto (ICID)		
		Indiretto (L1)	Potenzialmente indiretto (L2)	Identificatore impersonale (L3)
Tipo di informazione	Nome del cliente	Numero contenitore / ID contenitore	Luogo di nascita	Qualsiasi identificatore strettamente interno dell'applicazione di hosting/elaborazione del CID
	Nome della società	Numero MACC (conto liquidità soggetto a ID Contenitore Avaloq)	Data di nascita	Identificatore dinamico
	Estratto conto	ID SDS	Nazionalità	ID Party Role CRM
	Firma	IBAN	Carica in azienda	ID contenitore esterno
	ID social network	Dettagli di registrazione eBanking	Situazione familiare	
	Numero passaporto	Numero cassetta di sicurezza	Codice postale	
	Numero telefonico	Numero carta di credito	Condizioni di salute	
	Indirizzo e-mail	Messaggio SWIFT	Maggior valore di posizione/transazione	
	Qualifica lavorativa o PEP (Persona esposta politicamente)	ID Business Partner interno	Ultima visita cliente	
	Pseudonimo		Lingua	
	Indirizzo IP		Sesso	
	Numero fax		Data di scadenza CC	
			Contatto principale	
			Luogo di nascita	
			Data di apertura del conto	

Esempio: Se si invia un'e-mail o si condivide un documento con persone esterne (comprese terze parti in Svizzera/Monaco) o colleghi interni di un'altra consociata/sussidiaria situata in Svizzera/Monaco o altri Paesi (ad es. Regno Unito)

1. Nome del cliente

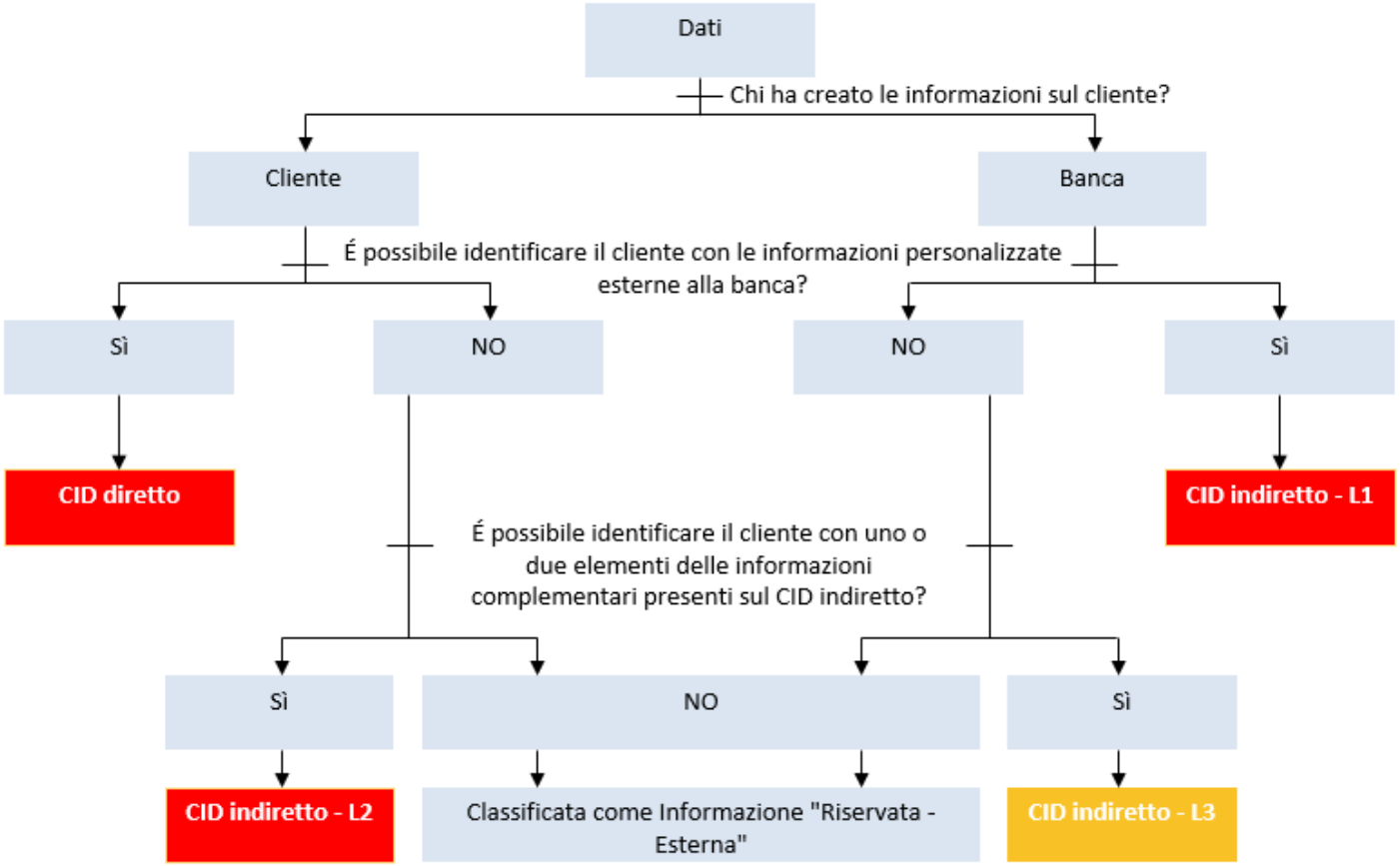
   (DCID) = Violazione del segreto bancario

2. ID contenitore

   (L1 ICID) = Violazione del segreto bancario

3. Condizioni di salute + Nazionalità

(L2 ICID) + (L2 ICID) = Violazione del segreto bancario


Dati
Chi ha creato le informazioni sul cliente?
Cliente
Banca
É possibile identificare il cliente con le informazioni personalizzate esterne alla banca?
Sì
NO
NO
Sì
CID diretto
CID indiretto - L1
É possibile identificare il cliente con uno o due elementi delle informazioni complementari presenti sul CID indiretto?
Sì
NO
Sì
CID indiretto - L2
Classificata come Informazione "Riservata - Esterna"
CID indiretto - L3

Appendice E: Schema di Etichettatura delle informazioni di Barclays

Tabella E1: Schema di Etichettatura delle informazioni di Barclays

** L'etichetta Segreto Bancario è specifica per le giurisdizioni che prevedono il segreto bancario.

Etichetta	Definizione	Esempi
Segreto bancario	Informazioni che sono collegate ai Dati identificativi del cliente svizzero (CID) Diretti o Indiretti. La classificazione 'Segreto Bancario' si applica alle informazioni che sono collegate ai Dati identificativi del cliente, Diretti o Indiretti. Di conseguenza, l'accesso da parte di tutti i dipendenti, anche se ubicati nella giurisdizione di appartenenza, non è appropriato. L'accesso a queste informazioni è necessario solo a chi ne ha bisogno per poter svolgere le proprie mansioni ufficiali o per assolvere gli obblighi contrattuali. Se destinati a personale non autorizzato, sia interno che esterno, nessuna divulgazione, accesso o condivisione autorizzati, sia internamente che esternamente all'entità che detiene tali informazioni, può avere un impatto critico e può dar luogo a procedimenti penali con conseguenze civili e amministrative come ammende e perdita dell'autorizzazione bancaria.	• Nome del cliente • Indirizzo del cliente • Firma • Indirizzo IP del cliente (altri esempi nell'Appendice D)

Etichetta	Definizione	Esempi
Segrete	Le informazioni devono essere classificate come Segrete se la loro divulgazione non autorizzata potrebbe avere un impatto negativo su Barclays, valutato nell'ambito dell'Enterprise Risk Management Framework (ERMF - Quadro di gestione del rischio d'impresa) come "Critico" (a livello finanziario o non finanziario).	• Informazioni su potenziali fusioni e acquisizioni. • Informazioni di pianificazione strategica, a livello aziendale e organizzativo. • Determinate informazioni sulla configurazione di sicurezza. • Determinati risultati di audit e rapporti

	Queste informazioni sono destinate a un target specifico e non devono essere divulgate ulteriormente senza l'autorizzazione dell'autore. Il target può comprendere destinatari esterni su esplicita autorizzazione del titolare delle informazioni.	• Verbali dei comitati esecutivi • Dettagli di Autenticazione o Identificazione e verifica (ID&V) – cliente e collega. • Grandi volumi di informazioni sui titolari di carte. • Previsioni di profitto e risultati finanziari annuali (prima della divulgazione pubblica). • Qualsiasi punto che rientri nell'ambito di un Non-Disclosure Agreement (NDA) ufficiale.
Riservata – Interna	Le informazioni devono essere classificate come Riservata - Interna se i destinatari previsti sono solo dipendenti Barclays autenticati e Managed Service Providers (MSP - Provider di servizi gestiti) in possesso di un contratto attivo che riguarda un target specifico. La divulgazione non autorizzata potrebbe avere un impatto negativo su Barclays, valutato nell'ambito dell'ERMF come "Principale" o "Limitato" (a livello finanziario o non finanziario). Queste informazioni non sono destinate alla diffusione generale ma possono essere inoltrate o condivise dai destinatari secondo il principio need-to-know.	• Strategie e budget. • Stime delle performance. • Remunerazione dei dipendenti e Dati Personali. • Valutazioni di vulnerabilità. • Risultati di audit e rapporti.
Riservata – Esterna	Le informazioni devono essere classificate come Riservata - Esterna se i destinatari previsti sono dipendenti Barclays autenticati e MSP in possesso di un contratto attivo che riguarda un target specifico o parti esterne autorizzate dal titolare delle informazioni. La divulgazione non autorizzata potrebbe avere un impatto negativo su Barclays, valutato nell'ambito dell'ERMF come "Principale" o "Limitato" (a livello finanziario o non finanziario).	• Nuovi piani di prodotto. • Contratti con i clienti. • Contratti legali. • Informazioni relative a clienti singoli/a basso volume da inviare all'esterno. • Comunicazioni relative ai clienti. • Nuovi materiali per offerte (ad es. prospetti, promemoria per offerte). • Documenti di ricerca definitivi. • Informazioni essenziali non pubbliche (Material Non-Public Information - MNPI) esterne a Barclays. • Tutti i report di ricerca

	Queste informazioni non sono destinate alla diffusione generale ma possono essere inoltrate o condivise dai destinatari secondo il principio need-to-know.	• Alcuni materiali di marketing. • Commenti del mercato.
Non riservate	Informazioni destinate alla diffusione generale o la cui divulgazione non avrebbe un impatto sull'organizzazione.	• Materiali di marketing. • Pubblicazioni. • Annunci pubblici. • Annunci di lavoro. • Informazioni che non influiscono su Barclays.

Tabella E2: Schema di Etichettatura delle informazioni - Requisiti di gestione

** I requisiti di gestione specifici per i dati CID atti a garantire la loro riservatezza secondo gli obblighi normativi

Fase del ciclo di vita	Requisiti del Segreto bancario
Creazione e Etichettatura	Come per "Riservata – Interna" e: • Ai patrimoni di dati deve essere assegnato un proprietario CID.
Conservazione	Come per "Riservata – Esterna" e: • I dati devono essere archiviati su supporti removibili solo per il periodo espressamente necessario per lo svolgimento di attività specifiche, per le verifiche normative o per le attività di auditing esterne. • Grandi quantità di Patrimoni di dati soggetti a Segreto Bancario non devono essere archiviate su dispositivi/supporti portatili. Per ulteriori informazioni, contattare il Team Sicurezza Cibernetica e Informatica locale (Cyber and Information Security - CIS). • Secondo il principio need-to-know o need-to have, i patrimoni di dati (sia fisici che elettronici) non devono essere conservati in luoghi dove possono essere visti o consultati da persone non autorizzate. • Per la salvaguardia del patrimonio (sia fisico che elettronico), devono essere rispettate le prassi per un luogo di lavoro sicuro come Scrivania Libera e Desktop Bloccato. • Per l'archiviazione dei dati possono essere utilizzati supporti rimovibili solo per il periodo di tempo espressamente necessario e devono essere custoditi in luogo sicuro quando non sono utilizzati. • I trasferimenti di dati ad-hoc su dispositivi/supporti portatili richiedono l'approvazione del titolare dei dati, dell'ufficio conformità e del CIS.

Accesso e uso	Come per "Riservata – Esterna" e: • I dati non devono essere eliminati / visualizzati off-site (dei locali di Barclays) senza autorizzazione formale del Titolare del CID (o soggetto incaricato). • I dati non devono essere eliminati / visualizzati al di fuori della giurisdizione di registrazione del cliente senza autorizzazione formale del Titolare del CID (o soggetto incaricato) e del cliente (rinuncia / procura limitata). • Quando si trasportano i dati fisici off-site è necessario seguire la prassi di lavoro sicuro da remoto che garantisce l'impossibilità di realizzare attività di shoulder surfing.
	• Accertarsi che le persone non autorizzate non possano osservare o accedere ai dati elettronici che contengono i CID attraverso l'uso di applicazioni aziendali ad accesso limitato.
Condivisione	Come per "Riservata – Esterna" e: • I dati devono essere diffusi solo conformemente al 'principio need to know' E all'interno dei sistemi informativi e tra il personale delle giurisdizioni che danno origine al Segreto Bancario. • Il trasferimento di dati su base ad-hoc con l'utilizzo di supporti rimovibili richiede l'approvazione del titolare del patrimonio di dati e del CIS. • Le comunicazioni elettroniche devono essere criptate durante il trasferimento. • La copia fisica dei dati inviata via e-mail deve essere inoltrata utilizzando un servizio che preveda la conferma di ricevimento. • I patrimoni di dati devono essere distribuiti solo conformemente al 'principio need to know'.
Archiviazione ed Eliminazione	Come per "Riservata – Esterna"

*** Informazioni sulla configurazione di sicurezza dei sistemi, risultati di audit e documenti personali possono essere classificati come Riservati - Interni o Segreti a seconda dell'impatto sull'attività aziendale della loro divulgazione non autorizzata

Fase del ciclo di vita	Riservata – Interna	Riservata – Esterna	Segrete
Creazione e introduzione	• Ai Patrimoni di Dati deve essere assegnato un Titolare delle Informazioni.	• Ai Patrimoni di Dati deve essere assegnato un Titolare delle Informazioni.	• Ai Patrimoni di Dati deve essere assegnato un Titolare delle Informazioni.
Conservazione	• I dati (sia fisici che elettronici) non devono essere conservati in aree pubbliche (ivi comprese le aree pubbliche nei locali a cui i visitatori possono avere accesso non controllato). • Le informazioni non devono essere lasciate in aree pubbliche nei locali a cui i visitatori possono avere accesso non controllato.	• I patrimoni di dati (sia fisici sia elettronici) non devono essere conservati in luoghi in cui persone non autorizzate possano visualizzarli o accedervi. • I patrimoni di dati elettronici memorizzati devono essere protetti tramite criptaggio o controlli compensativi appropriati, qualora sussista un rischio elevato di accesso agli stessi da parte di persone non autorizzate.	• I patrimoni di dati (sia fisici sia elettronici) non devono essere conservati in luoghi in cui persone non autorizzate possano visualizzarli o accedervi. • I patrimoni di dati elettronici memorizzati devono essere protetti tramite criptaggio o controlli compensativi appropriati, qualora sussista un rischio elevato di accesso agli stessi da parte di persone non autorizzate. • Tutte le chiavi private che sono utilizzate per proteggere i dati, l'identità e/o la reputazione di Barclays devono essere protette da moduli per la sicurezza dell'hardware certificati FIPS 140-2 Livello 3 o superiore (HSM).

Accesso e uso	• I dati (sia fisici che elettronici) non devono essere lasciati in aree pubbliche all'esterno dei locali. • I dati (sia fisici che elettronici) non devono essere lasciati in aree pubbliche nei locali a cui i visitatori possono avere accesso non controllato. • Se necessario, i patrimoni di dati elettronici devono essere protetti mediante controlli Logical Access Management appropriati	• Non si deve lavorare su patrimoni di dati (sia fisici sia elettronici), né lasciarli incustoditi in luoghi in cui persone non autorizzate possano visualizzarli o accedervi. È possibile lavorare su patrimoni di dati se sussistono controlli adeguati (per esempio schermi per la privacy). • I patrimoni di dati stampati devono essere recuperati immediatamente dalla stampante. Ove ciò non sia possibile, occorre usare strumenti di stampa sicuri. • I dati elettronici devono essere protetti mediante controlli Logical Access Management appropriati	• Non si deve lavorare su patrimoni di dati (sia fisici sia elettronici), né lasciarli incustoditi in luoghi in cui persone non autorizzate possano visualizzarli o accedervi. È possibile lavorare su patrimoni di dati se sussistono controlli adeguati (per esempio schermi per la privacy). • Si devono usare strumenti di stampa sicuri per stampare i patrimoni di dati. • I patrimoni di dati elettronici devono essere protetti mediante controlli Logical Access Management appropriati
Condivisione	• Le copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile. L'etichetta deve essere apposta per lo meno sulla copertina. • I patrimoni di dati elettronici devono essere corredati di chiara etichetta informativa. • I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione.	• Le copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile. L'etichetta deve essere apposta per lo meno sulla copertina. • Le buste contenenti copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile sul lato frontale.	• Le copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile su ciascuna pagina. • Le buste contenenti copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile sul lato frontale ed essere chiuse con un sigillo che riveli eventuali tentativi di manomissione. Prima della distribuzione, inoltre, devono essere inserite in una seconda busta priva di etichetta.

	• I patrimoni di dati devono essere distribuiti esclusivamente ai dipendenti dell'organizzazione o a individui vincolati a quest'ultima da un obbligo contrattuale appropriato o per assolvere a un'esigenza aziendale chiaramente riconosciuta, come una negoziazione contrattuale.	• I patrimoni di dati elettronici devono essere corredati di chiara etichetta informativa. Le copie elettroniche dei documenti di più pagine devono essere corredate di etichetta informativa visibile su ciascuna pagina. • I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione. • I patrimoni di dati devono essere distribuiti esclusivamente ai dipendenti dell'organizzazione o a individui vincolati a quest'ultima da un obbligo contrattuale appropriato o per assolvere a un'esigenza aziendale chiaramente riconosciuta, come una negoziazione contrattuale. • I patrimoni di dati devono essere distribuiti esclusivamente alle persone che hanno necessità di riceverli per motivi connessi alla loro attività. • I patrimoni di dati non devono essere inviati via fax, a meno che il mittente non abbia verificato che i destinatari sono pronti a ritirare il fax.	• I patrimoni di dati elettronici devono essere corredati di chiara etichetta informativa. Le copie elettroniche dei documenti di più pagine devono essere corredate di etichetta informativa visibile su ciascuna pagina. • I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione. • I patrimoni di dati devono essere distribuiti esclusivamente ai dipendenti dell'organizzazione o a individui vincolati a quest'ultima da un obbligo contrattuale appropriato o per assolvere a un'esigenza aziendale chiaramente riconosciuta, come una negoziazione contrattuale. • I Patrimoni di Dati devono essere distribuiti esclusivamente alle persone specificamente autorizzate a riceverli dal Titolare del Patrimonio di Dati. • I patrimoni di dati non devono essere inviati via fax. • Durante il transito al di fuori della rete interna, i patrimoni di dati elettronici devono essere criptati tramite un dispositivo di protezione crittografica approvato.

		• Durante il transito al di fuori della rete interna, i patrimoni di dati elettronici devono essere criptati tramite un dispositivo di protezione crittografica approvato.	• Occorre implementare una catena di custodia dei patrimoni di dati elettronici.
Archiviazione ed eliminazione	• Le copie cartacee dei patrimoni di dati devono essere eliminate tramite un servizio di eliminazione riservato. • Le copie dei patrimoni di dati elettronici devono essere cancellate in modo tempestivo anche dai "cestini" del sistema o da dispositivi analoghi.	• Le copie cartacee dei patrimoni di dati devono essere eliminate tramite un servizio di eliminazione riservato. • Le copie dei patrimoni di dati elettronici devono essere cancellate in modo tempestivo anche dai "cestini" del sistema o da dispositivi analoghi.	• Le copie cartacee dei patrimoni di dati devono essere eliminate tramite un servizio di eliminazione riservato. • Le copie dei patrimoni di dati elettronici devono essere cancellate in modo tempestivo anche dai "cestini" del sistema o da dispositivi analoghi. • I supporti su cui sono stati memorizzati i patrimoni di dati elettronici segreti devono essere depurati in modo appropriato prima o durante l'eliminazione.