Obblighi di controllo dei Fornitori esterni

Sicurezza Informatica e Cibernetica

Per fornitori classificati ad Alto Rischio Informatico e Cibernetico

Versione 9.0 aprile 2019

Area di controllo / Titolo	Descrizione del controllo	Perché è importante?
1. Governance, Politica e Standard di Sicurezza Informatica / Cibernetica	Al fine di proteggersi dai rischi Informatici/Cibernetici, il Fornitore deve disporre di processi di governance del rischio Informatico/Cibernetico che garantiscano la conoscenza del proprio ambiente tecnologico e dello stato dei controlli di sicurezza Informatica/Cibernetica, nonché di un programma di sicurezza che protegga il Fornitore dalle minacce Informatiche/Cibernetiche in conformità con la Buona Prassi del Settore (per es. NIST, SANS, ISO27001) Il Fornitore si impegna ad eseguire regolarmente la Valutazione dei Rischi relativa alla sicurezza Informatica/Cibernetica (in qualsiasi caso almeno ogni 12 mesi) nonché a implementare i controlli e a prendere i provvedimenti necessari a ridurre i rischi individuati. Qualora sia identificato un rischio concreto che potrebbe influenzare negativamente la reputazione di Barclays o i servizi erogati, il Fornitore deve darne comunicazione a Barclays. IL Fornitore deve mantenere attive le procedure approvate dal senior management e le norme per la gestione del rischio Informatico/Cibernetico del Fornitore, che devono essere verificate almeno annualmente.	In caso di mancata attuazione di questo controllo, Barclays o i propri Fornitori potrebbero non avere e non essere in grado di dimostrare di disporre di una supervisione adeguata sulla sicurezza Informatica/Cibernetica. Le procedure e gli standard documentati sono elementi essenziali per la gestione del rischio e la governance. Essi stabiliscono la visibilità sulla gestione dei controlli necessari per gestire il rischio informatico/cibernetico.

2. Uso approvato	Il Fornitore deve redigere e divulgare i Requisiti di uso accettabile, informando i propri dipendenti delle loro responsabilità. È necessario considerare i seguenti aspetti: (a) Uso di Internet; (b) Uso dei Social Media; (c) Uso di e-mail aziendali; (d) Uso di messaggistica istantanea; (e) Uso di apparecchiature fornite dal Fornitore. (f) Uso di apparecchiature non fornite dal Fornitore (ad es. portare il proprio dispositivo);. (g) Uso di dispositivi di archiviazione portatili/rimovibili; (h) Responsabilità nella gestione del Patrimonio di dati di Barclays; e (i) Elaborazione dei canali di perdita dati 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
3. Ruoli e responsabilità	Il Fornitore deve definire e comunicare i ruoli e le responsabilità per la Sicurezza Informatica/Cibernetica. Questi devono essere rivisti regolarmente (e in ogni caso almeno una volta all'anno) e dopo ogni modifica rilevante del modello operativo o dell'attività del Fornitore. I ruoli principali devono comprendere un senior executive, responsabile della Sicurezza Informatica/Cibernetica.	La chiara definizione dei ruoli e delle responsabilità supporta l'attuazione del Programma sugli Obblighi di controllo dei Fornitori esterni.
4. Rispetto dei requisiti legislativi e statutari locali	Il Fornitore deve garantire che i requisiti legislativi e statutari relativi alla Sicurezza Informatica in vigore nella giurisdizione in cui opera siano rispettati e che tale conformità sia adeguatamente documentata. N.B. Ulteriori requisiti possono essere specificati dai team locali collegati alla legislazione bancaria e ai regolamenti locali per i Fornitori che supportano Barclays Switzerland e Barclays Monaco.	La mancata conformità alla normativa locale e ai requisiti statutari potrebbe avere gravi ripercussioni sia sul Fornitore che su Barclays, incluse sanzioni e, in casi estremi, la perdita dell'autorizzazione bancaria di Barclays

5. Formazione e consapevolezza	Il Fornitore deve offrire Formazione e Consapevolezza (Education and Awareness - E&A) a tutti i dipendenti interessati. La E&A deve essere adeguata ai rispettivi ruoli e responsabilità e deve essere sufficiente affinché i dipendenti siano in grado di comprendere e individuare i possibili attacchi e segnalare eventuali problemi. Come misura minima, la formazione deve vertere su come rimanere on-line in sicurezza (al lavoro, a casa e in viaggio), sui rischi dell'ingegneria sociale e sulle contromisure pratiche. Il Fornitore deve accertarsi che tutto il personale (Entrante/In movimento), entro un periodo di tempo ragionevole, completi la formazione in modo da garantire la comprensione dei propri ruoli e responsabilità in materia di Sicurezza Informatica. Gli amministratori dei sistemi devono ricevere una formazione approfondita per avere maggior consapevolezza sulla Sicurezza Informatica/Cibernetica, almeno annualmente, con riferimento agli scenari/alle minacce specifiche per il loro ruolo, a come identificare le minacce Informatiche/Cibernetiche, a come proteggersi dalle minacce Informatiche/Cibernetiche e come segnalare i problemi.	Formazione e consapevolezza supportano tutti gli altri controlli nell'ambito di questo programma. In caso di mancata attuazione di questi controlli, 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. Procedura di gestione degli incidenti	Deve essere istituita e gestita una procedura di risposta agli incidenti per la tempestiva gestione e la regolare segnalazione degli incidenti che coinvolgono i dati Barclays e/o i servizi utilizzati da Barclays. Nell'ambito della procedura di risposta agli incidenti deve essere definito quanto segue: • Gli incidenti di sicurezza e le violazioni dei dati che interessano o colpiscono le attività di Barclays e/o i Servizi forniti a Barclays devono essere segnalati a quest'ultima non appena possibile, con costanti aggiornamenti sull'andamento degli interventi correttivi. • Deve essere istituita una procedura di risposta agli incidenti per la tempestiva gestione e la regolare segnalazione delle intrusioni che coinvolgono i dati Barclays e/o i Servizi utilizzati da Barclays. • Le violazioni di cui non è noto l'effetto sui sistemi Barclays e i relativi interventi correttivi/aggiornamenti devono comunque essere segnalati a Barclays a titolo informativo. • Il Fornitore deve 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 sicurezza Cibernetici individuati. I test devono includere la conferma della capacità di informare Barclays, raggiungendo i soggetti incaricati. • Dopo un incidente di sicurezza, deve essere istituita e implementata una procedura per individuare e gestire la riduzione delle vulnerabilità senza compromettere le indagini o le attività di risposta. • Il Fornitore deve disporre di processi e procedure per intraprendere un'analisi delle cause di eventi interni (al Fornitore) ed esterni. • Il Fornitore deve aver cura di eliminare le carenze individuate con un piano di intervento correttivo (azione, proprietà, data di esecuzione) comunicato a Barclays e da questa approvato.	Un processo di risposta e gestione degli incidenti aiuta a garantire che vengano rapidamente circoscritti e che ne venga impedita l'escalation.

7. Miglioramento contino	Il Fornitore deve continuamente imparare dagli eventi e applicare quanto appreso per migliorare le difese contro i rischi Cibernetici.	In caso di mancata applicazione di questi controlli, i Fornitori non saranno in grado di utilizzare quanto appreso da precedenti eventi per migliorare e rafforzare il loro ambiente di controllo.
8. Proprietà del patrimonio di dati	Il Fornitore deve nominare una persona dedicata alle comunicazioni con il titolare del patrimonio dati di Barclays.	La titolarità del Patrimonio di Dati è fondamentale per una protezione adeguata dello stesso.
9. Schema di Etichettatura delle informazioni	***Laddove appropriato****, il Fornitore deve applicare lo Schema di Etichettatura delle Informazioni di Barclays e i requisiti di gestione (Appendice B, Tabelle B1 e B2A2), o uno schema alternativo concordato con Barclays, per tutto il Patrimonio di dati conservati o elaborati per conto di Barclays. * "***laddove appropriato***" *fa riferimento al vantaggio derivante dall'etichettatura in rapporto al costo 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.
10. Gestione delle risorse	Il Fornitore deve mantenere aggiornato l'inventario accurato di tutte le risorse IT appropriate utilizzate per erogare a Barclays i servizi e deve controllarlo almeno una volta all'anno per confermare che tale inventario sia aggiornato, completo e preciso.	In caso di mancata attuazione di questi controlli, le risorse di Barclays o quelle utilizzate dai Fornitori per erogare a Barclays i servizi potrebbero risultare compromesse e comportare perdite finanziarie, perdite di dati, danni alla reputazione e richiami ufficiali.
11. Sicurezza durante il trasporto	Il Patrimonio di dati di Barclays (salvo il caso in cui sia considerato "Non riservato" o stato equivalente) deve essere protetto durante il trasporto in misura commisurata al rischio associato.	I controlli durante il trasporto proteggono i Dati di Barclays dall'intercettazione e dalla diffusione.

12. Distruzione/Cancellazione/Disattivazione di Informazioni Fisiche e Logiche	La distruzione o cancellazione del Patrimonio di dati di Barclays archiviato in formato fisico o elettronico deve avvenire in modo sicuro e commisurato ai rischi associati, accertandosi che non sia recuperabile.	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.
13. Sicurezza della rete	Il Fornitore deve garantire che tutti i Sistemi IT gestiti dal Fornitore o dai rispettivi subfornitori che supportano i servizi erogati a Barclays siano protetti da manovre o minacce laterali all'interno della rete del Fornitore (e di qualsiasi subfornitore pertinente). Il Fornitore deve prendere in considerazione i seguenti meccanismi di protezione: • la separazione logica delle porte/interfacce per la gestione dei dispositivi dal traffico degli utenti; • gli adeguati controlli di autenticazione; e • l'attivazione di tutti i controlli disponibili per la riduzione degli accessi al sistema operativo e alle applicazioni e agli agenti installati. Il Fornitore deve definire e gestire la capacità di rilevare la presenza di dispositivi non autorizzati, software identificati come dannosi e software non autorizzati ad alto rischio nella rete del Fornitore. Il Fornitore deve posizionare dei sensori di rete per rilevare le minacce a tutti i punti di ingresso e uscita del perimetro di rete. *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.*	La mancata attuazione di tale controllo, le reti esterne e interne possono essere compromesse da eventuali minacce.

14. Difesa del perimetro	Il Fornitore deve conservare un inventario delle connessioni a rete esterne, di host accessibili in Internet e dei trasferimenti di dati utilizzati per ritrasmettere i dati a Barclays o a terzi (inclusi, tra l'altro, eventuali subfornitori del Fornitore) In base alle esposizioni al rischio e alle esigenze aziendali deve essere implementata sul perimetro una configurazione di rete multizona isolata. Solo i dispositivi che richiedono o facilitano l'accesso a/da reti esterne devono essere collocati sul perimetro.	Una protezione appropriata del perimetro aiuta a garantire che la rete e i Patrimoni di dati di Barclays siano adeguatamente protetti.
15. Accesso alla rete e accesso remoto	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. Se è consentito l'accesso remoto ai Patrimoni di dati Barclays archiviati in ambienti gestiti dal Fornitore, sono necessarie l'autenticazione a due fattori e l'autorizzazione dell'end point, basate sull'identità dell'Utente, sul tipo di dispositivo e sulla posizione di sicurezza del dispositivo (per esempio, il livello patch, lo stato anti-malware, i dispositivi mobili con o senza rooting, ecc.). L'accesso remoto agli ambienti Barclays non è fornito di default per la connessione dalla sede del Fornitore/per il supporto di out of office/out of business. Qualsiasi accesso remoto deve essere approvato dalle funzioni di Barclays pertinenti (compreso il Chief Security Office).	I controlli di accesso alla rete aiutano a garantire che dispositivi non sicuri non vengano collegati alla rete del Fornitore, introducendo nuove vulnerabilità.
16. Rifiuto di rilevamento del servizio (Denial of Service Detection)	Il Fornitore deve implementare e mantenere la capacità di rilevare gli attacchi al Rifiuto di Servizio (Denial of Service - DoS). 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 i criteri di disponibilità concordati con Barclays.	In caso di mancata attuazione di questo controllo, Barclays e i propri Fornitori potrebbero non essere in grado di impedire che un attacco di tipo Denial of Service vada a buon fine.

17. Monitoraggio / registrazione	Il fornitore deve garantire che il monitoraggio 24/7 delle infrastrutture IT per potenziali eventi di sicurezza cibernetica sia effettivamente svolto. Il Fornitore deve raccogliere e correlare i dati degli eventi estratti dalle fonti dei sistemi applicabili e analizzarli per individuare e studiare gli attacchi/incidenti. In seguito all'individuazione di incidenti di rilievo e/o di violazioni dei controlli di sicurezza, il Fornitore deve garantire il rispetto della Procedura di Gestione degli Incidenti (di cui al paragrafo 6 qui sopra). Tutti i sistemi principali, incluse le applicazioni principali, devono essere impostati dal Fornitore per la registrazione degli eventi principali e il tempo di sistema tra i sistemi deve essere sincronizzato dal Fornitore tramite il Protocollo dei Tempi di Rete (Network Time Protocol - NTP). I registri devono essere centralizzati, adeguatamente protetti e conservati dal Fornitore per almeno 12 mesi. 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	In caso di mancata attuazione di questo controllo, i Fornitori non saranno in grado di rilevare e rispondere alle violazioni della sicurezza Cibernetica o di recuperare e imparare dagli eventi Cibernetici verificatisi sulla loro rete analizzando i relativi registri.
18. Suddivisione del Patrimonio di dati	Il Fornitore deve conservare il Patrimonio di dati Barclays su rete isolata (in modo logico e/o fisico) da altri clienti.	Una rete isolata aiuta a garantire l'adeguata protezione del Patrimonio di dati di Barclays da diffusione non autorizzata.

19. Codici maligni / protezione malware	Laddove supportato a livello di sistema operativo, ai Sistemi IT, ai Servizi IT e ai Dispositivi IT deve essere sempre applicata la protezione contro i malware al fine di prevenire l'interruzione del servizio o eventuali violazioni della sicurezza. Il fornitore deve: • Adottare e mantenere aggiornata la protezione contro i Codici Maligni / Malware, conformemente alla Buona Prassi del Settore (per esempio NIST, ISO27001); e • Adottare una protezione contro il trasferimento di codici maligni ai Sistemi di Barclays, ai clienti di Barclays e ad altre terze parti, in conformità con i metodi standard del settore (per esempio NIST, ISO27001).	Le soluzioni anti-malware sono fondamentali per la protezione dei Patrimoni di dati Barclays contro i codici maligni.
20. Standard di Sicurezza della Struttura e Riconciliazione delle Modifiche di Sicurezza	Il Fornitore deve definire e implementare le norme sulla struttura per tutti i software pronti all'uso configurabili, utilizzati in grandi quantità (per esempio, sistemi operativi, database) e il firmware di infrastrutture comunemente utilizzate (per esempio, SAN o dispositivi di rete). Eventuali non conformità a tali norme devono essere corrette. Le modifiche alla sicurezza (per esempio, modifiche alla configurazione della sicurezza, modifica di privilegi di account) devono sempre creare un registro, conservato in un ambiente a prova di manomissione. Tra le modifiche applicate e quelle autorizzate deve essere effettuata la riconciliazione. I sistemi host e i dispositivi di rete che sono parte dei sistemi del Fornitore devono essere configurati in modo da funzionare in conformità alla Buona Prassi del Settore (per esempio, NIST, SANS, ISO27001).	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
21. Tecnologie di protezione della sicurezza	Per gestire le minacce di attacchi Cibernetici attuali ed emergenti occorre adottare tecnologie appropriate con uno standard di controlli uniforme, allo scopo di prevenire l'invio, l'esecuzione, lo sfruttamento e il furto di dati.	In caso di mancata attuazione di questo controllo, il Patrimonio di dati di Barclays potrebbe non essere sufficientemente protetto da attacchi Cibernetici.

22. Sicurezza dell'endpoint	Il Fornitore deve garantire che gli endpoint utilizzati per accedere alla rete di Barclays o per elaborare i Dati di Barclays siano configurati per la protezione dagli attacchi. Questo include, in modo indicativo ma non esaustivo, limitare l'area di attacco disabilitando il software/i servizi/le porte non necessarie, verificare che tutte le versioni in uso rientrino nei periodi di supporto pubblico, che ci siano e siano adeguatamente configurati sistemi di protezione da malware e firewall dell'host e siano predisposti comandi per contenere i tentativi di sfruttamento.	La mancata attuazione di questo controllo potrebbe rendere Barclays, la rete e gli endpoint dei Fornitori vulnerabili agli attacchi Cibernetici.
23. Rilevamento di dispositivi e software non autorizzati	Il Fornitore deve garantire di disporre della capacità e dei processi necessari a rilevare dispositivi non autorizzati, software identificati come maligni e software non autorizzati ad alto rischio.	In caso di mancata attuazione di questo controllo, i Fornitori potrebbero non essere in grado di rilevare, rimuovere o disabilitare un dispositivo o un software non autorizzato o maligno, esponendo le attività di Barclays ad attacchi Cibernetici.
24. Prevenzione della fuga di dati	Il rischio di perdita dati per le Informazioni collegate ai servizi che il Fornitore eroga a Barclays insorgente dalla rete o dai dispositivi fisici deve essere valutato e ridotto al minimo. È necessario considerare i seguenti canali di perdita dati: • Trasferimento non autorizzato di informazioni al di fuori della rete interna/rete del fornitore. • 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 (subfornitori); • Stampa o copia inadeguata di informazioni; • Errori od omissioni commessi nella classificazione ed etichettatura del patrimonio; e • Perdita non autorizzata di Informazioni tramite il Sistema di Nome a Dominio (Domain Name System - DNS)	Controlli appropriati per la prevenzione della fuga di dati sono un elemento vitale per la Protezione delle Informazioni, che aiuta garantire che le Informazioni di Barclays non vengano perse.

25. Archiviazione sicura e procedura	Devono essere attuati controlli per proteggere il Patrimonio di dati (relativi ai servizi che il Fornitore eroga a Barclays) ovunque sia conservato o trattato (questo vale per i dati conservati come parte di metodi strutturati e non strutturati).	I Patrimoni di dati sono generalmente conservati insieme e pertanto comportano una concentrazione del rischio e devono essere protetti.
26. Backup e Recupero	Si devono prendere i dovuti provvedimenti per garantire che le Informazioni ricevano un adeguato back-up e siano recuperabili conformemente ai requisiti concordati con il Titolare del Patrimonio dati di Barclays e che la sicurezza del Patrimonio dati sia mantenuta per tutta la procedura. La frequenza e il metodo di back-up devono essere concordati con il Titolare del Patrimonio di dati I patrimoni di dati di cui è stato effettuato il back-up devono avere controlli definiti per garantire che l'accesso avvenga esclusivamente quando necessario.	I back-up sono copie dei Patrimoni di dati e come tali devono essere sottoposti agli stessi controlli.

27. 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 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. Questi principi devono essere applicati sulla base del rischio, tenendo conto del tasso di riservatezza delle informazioni. Ogni account deve essere associato a una singola persona, che sarà responsabile di tutte le attività svolte utilizzando l'account. Questo non preclude l'uso di Account Condivisi ma ogni singola persona sarà responsabile per ciascun Account Condiviso. I processi di gestione dell'accesso devono essere definiti secondo la Buona Prassi del Settore e devono includere, come minimo, quanto segue: • l'attivazione di un solido processo di autorizzazione prima di creare/modificare/cancellare gli account; • una procedura di revisione dell'accesso per gli Utenti Periodici da seguire almeno una volta all'anno al fine di convalidare l'accesso utente	Controlli LAM appropriati aiutano a garantire la protezione dei Patrimoni di dati da un uso improprio.

	• i controlli sui trasferimenti – modifica/rimozione dell'accesso entro 5 giorni lavorativi dalla data di trasferimento; • i controlli sui congedi – rimozione entro 24 ore dalla data di congedo di tutti gli accessi logici utilizzati per fornire a Barclays i servizi e rimozione entro 7 giorni di tutti gli accessi secondari; e • gli account dormienti non utilizzati da almeno 60 giorni consecutivi devono essere sospesi.	
28. Metodi di accesso	Le attività svolte sotto un unico account devono essere riconducibili a una singola persona. È necessario adottare misure tecniche e procedure atte ad applicare l'adeguato livello di accesso al Patrimonio di dati. I controlli di sicurezza relativi agli account (ad es. solide procedure di autenticazione o break-glass) devono essere commisurati al rischio di compromissione o uso improprio dell'account. I metodi di accesso devono essere definiti secondo la Buona Prassi del Settore e devono includere, come minimo, quanto segue: • 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. Gli accessi remoti per i Servizi di Barclays devono essere autorizzati tramite procedure approvate dai team Barclays pertinenti e devono applicare l'autenticazione multifattoriale.	I controlli della gestione degli accessi aiutano a garantire che solo gli Utenti approvati possano accedere ai Patrimoni di dati.

29. Protezione delle applicazioni	Le applicazioni devono essere sviluppate utilizzando procedure di codifica sicure e in ambienti protetti. Se il Fornitore sviluppa delle applicazioni per l'utilizzo da parte di Barclays o che sono utilizzate a supporto dei servizi resi a Barclays, devono essere presenti processi e controlli per individuare e rimediare alle vulnerabilità nel codice durante il processo di sviluppo. I codici binari delle applicazioni devono essere protetti da modifiche non autorizzate durante la distribuzione e quando si trovano nella libreria sorgente. Il Fornitore garantisce che, per lo sviluppo del sistema, è attiva la segregazione delle mansioni e garantisce che gli sviluppatori del sistema non hanno accesso ai dati attuali, salvo in caso di emergenza in cui tale accesso è protetto con controlli adeguati come le procedure break-glass. In queste circostanze, tali attività sono registrate e sono soggette a verifica indipendente.	I controlli che tutelano lo sviluppo di applicazioni aiutano a garantirne la sicurezza al momento della distribuzione.
30. Gestione della vulnerabilità	Il Fornitore deve disporre di un'adeguata procedura di registrazione, smistamento e risposta per le vulnerabilità identificate. Il Fornitore deve istituire la capacità di identificazione e classificazione delle vulnerabilità di sicurezza nei Sistemi IT e nei software basate sui rischi presenti su tutte le piattaforme utilizzate dall'organizzazione. Il Fornitore deve garantire che la gestione delle vulnerabilità sia trattata nell'ambito dell'attività operativa ordinaria, inclusi i processi per individuare e valutare i rischi di vulnerabilità, per eliminare e porre rimedio alle vulnerabilità in tutti i sistemi e per prevenire l'introduzione di nuove vulnerabilità durante i processi di cambiamento e l'introduzione di nuovi sistemi. Tutti i problemi di sicurezza e le vulnerabilità che potrebbero avere un impatto concreto sui sistemi di Barclays o sui servizi che il Fornitore eroga a Barclays di cui il Fornitore ha deciso di accettare il rischio devono essere prontamente comunicati a Barclays e concordati per iscritto con Barclays. Il Fornitore deve installare in modo tempestivo gli aggiornamenti per la Sicurezza IT e la gestione delle vulnerabilità attraverso una procedura interna (del Fornitore) approvata, al fine di prevenire violazioni della sicurezza. I sistemi del Fornitore che per qualsiasi motivo non possono essere aggiornati devono contenere misure idonee a proteggere il sistema vulnerabile.	La mancata attuazione di questo controllo potrebbe comportare l'utilizzo di queste vulnerabilità dei sistemi per condurre attacchi Cibernetici contro Barclays e i suoi Fornitori.

31. Simulazione di minaccia/ Test di penetrazione/ Valutazione della sicurezza IT	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 e alle applicazioni relative ai servizi che il Fornitore eroga a Barclays. 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. Tutte le questioni di cui si è deciso di accettare il rischio devono essere comunicate e concordate con 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.	In caso di mancata attuazione di questo controllo, i Fornitori potrebbero non essere in grado di valutare le Minacce Cibernetiche a cui sono soggetti e l'idoneità e solidità delle proprie difese.

32. Gestione delle modifiche e degli aggiornamenti	I Dati Barclays e i sistemi utilizzati per memorizzarli o elaborarli devono essere protetti contro le modifiche non appropriate che possono comprometterne la disponibilità o l'integrità. Il Fornitore si impegna a sviluppare e implementare una strategia di gestione degli aggiornamenti che sia supportata da controlli e da procedure di gestione degli aggiornamenti nonché da documentazione operativa. Non appena saranno disponibili, devono essere installati in modo tempestivo gli aggiornamenti della Sicurezza IT e della vulnerabilità della sicurezza attraverso una procedura approvata al fine di prevenire qualsiasi violazione della sicurezza. I Sistemi del Fornitore che per qualsiasi motivo non possono essere aggiornati devono contenere le misure di sicurezza idonee a proteggere il sistema vulnerabile. Tutte le modifiche devono essere eseguite conformemente alla procedura di gestione delle modifiche del Fornitore approvata. Le applicazioni open source sono verificate per rilevare eventuali vulnerabilità salienti. Il Fornitore garantisce che saranno implementate le risoluzioni delle emergenze se disponibili e approvate, a meno che tale condizione non comporti maggiori rischi operativi. I Sistemi del Fornitore che per qualsiasi motivo non possono essere aggiornati devono contenere le misure di sicurezza idonee a proteggere completamente il sistema vulnerabile. Tutte le modifiche devono essere eseguite conformemente alla procedura di gestione delle modifiche del Fornitore.	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.
33. Crittografia	Il Fornitore deve esaminare e valutare la tecnologia crittografica e gli algoritmi che utilizza per accertarsi che siano adatti allo scopo. L'efficacia della criptazione utilizzata deve essere commisurata alla propensione al rischio, poiché può avere un impatto operativo o sulle prestazioni. Le implementazioni crittografiche devono rispettare i requisiti e gli algoritmi definiti.	Una protezione e algoritmi criptati aggiornati e adeguati garantiscono la protezione costante dei Patrimoni di dati di Barclays.

34. Cloud Computing	Qualsiasi uso di servizi di cloud computing (pubblico/privato/di comunità/ibrido) come ad es. SaaS/PaaS/IaaS impiegati come parte dei servizi resi a Barclays secondo gli accordi deve essere verificato e approvato dai team Barclays pertinenti (tra cui il Chief Security Office) e i controlli finalizzati alla protezione dei dati e dei servizi di Barclays devono essere in linea con il profilo di rischio e la criticità dei Patrimoni di dati per prevenire la perdita di dati e le violazioni cibernetiche.	La mancata implementazione di questo principio potrebbe compromettere i Patrimoni di dati di Barclays, non protetti in modo idoneo; tale condizione potrebbe dare luogo a provvedimenti normativi o causare danni alla reputazione.
35. Diritto di ispezione	I Fornitori devono consentire a Barclays, previo preavviso scritto di Barclays di almeno dieci 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 consentire a Barclays di svolgere un'ispezione 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 dovrà quindi completare eventuali interventi correttivi entro tale periodo. Il Fornitore si impegna a fornire tutta l'assistenza ragionevolmente richiesta da Barclays in relazione alle ispezioni effettuate.	In caso di mancato accordo i Fornitori non saranno in grado di fornire la piena garanzia della conformità a tali obblighi di sicurezza.
36. Spazio dedicato alla banca	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 indicati nell'Appendice C.)	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 cibernetica.

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.
Account condiviso	Un account concesso a uno o più dipendenti, a consulenti, collaboratori esterni o personale temporaneo che siano stati autorizzati ad accedere quando non è possibile usare account individuali a causa della natura del sistema a cui si accede.
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.
Autenticazione a più fattori	Autenticazione che utilizza 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).
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.
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.
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 codificato.
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.
Distruzione / Cancellazione	L'azione di sovrascrivere, cancellare o distruggere fisicamente informazioni in modo tale che non possano essere recuperate.
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.
Privilegio minimo	Il livello minimo di accesso/permesso che consente a un Utente o account di svolgere il proprio ruolo aziendale.
Rifiuto del servizio (Attacco)	Tentativo di rendere non disponibile per gli utenti cui è destinata una risorsa informatica.

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.
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.
Titolare del patrimonio di dati	Il dipendente nell'ambito dell'organizzazione che è responsabile della classificazione di un patrimonio e della sua corretta gestione.
Utente	Un account assegnato a un dipendente, consulente, collaboratore esterno o lavoratore temporaneo del Fornitore che sia autorizzato ad accedere a un sistema senza privilegi elevati.

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) ufficiale.
Riservata – Interna	Le informazioni devono essere classificate come Riservata - Interna se i destinatari previsti sono solo dipendenti Barclays autenticati e Managed	• Strategie e budget. • Stime delle performance. • Remunerazione dei dipendenti e dati personali.

	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.	• 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). Queste informazioni non sono destinate alla diffusione generale ma possono essere inoltrate o condivise dai destinatari secondo il principio need-to-know.	• 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 • 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 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	Riservata – Interna	Riservata – Esterna	Segrete
Creazione e introduzione	• Ai patrimoni di dati deve essere assegnato un proprietario delle informazioni.	• Ai patrimoni di dati deve essere assegnato un proprietario delle informazioni.	• Ai patrimoni di dati deve essere assegnato un proprietario 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.	• 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).	• 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).

	• Se necessario, i patrimoni di dati elettronici devono essere protetti mediante controlli Logical Access Management appropriati	• 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	• 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. • 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 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 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. • I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione.

		• 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.	• 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 proprietario delle informazioni. • 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.
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.

Appendice C: Spazio dedicato alla Banca (Bank Dedicated Space - BDS) – Requisiti di controllo (NB: Verificare con il responsabile del Sourcing se necessario)

Area di controllo	Titolo di controllo	Descrizione del controllo
Spazio dedicato alla banca	Separazione fisica	L'area fisica occupata deve essere dedicata a Barclays e non condivisa con altre società / altri venditori.
Spazio dedicato alla banca	Controllo dell'accesso fisico	Per l'accesso a BDS devono essere svolti controlli automatici di sicurezza, tra cui: 1) In caso di personale autorizzato; i) Tesserino identificativo con foto sempre visibile ii) Sono utilizzati lettori ottici di card iii) Sono attivi dispositivi anti-pass back 2) Controlli di visitatori/venditori i) Registro firme ii) Tesserino identificativo ad uso temporaneo sempre visibile
Spazio dedicato alla banca	Controllo dell'accesso fisico	È necessario configurare degli allarmi per la segnalazione tramite un sistema di accesso centralizzato con controllo degli accessi verificabile
Spazio dedicato alla banca	Controllo dell'accesso fisico e gestione	Il monitoraggio dei controlli che garantiscono l'idoneità degli accessi è concesso all'area BDS e alle altre aree critiche L'accesso all'area BDS è consentito solo agli addetti alle pulizie e al personale di supporto come elettricisti, manutentori AC e così via
Spazio dedicato alla banca	Accesso remoto - ID&V	Ciascun utente che vuole autenticarsi sulla rete Barclays dall'area BDS, può utilizzare esclusivamente un dispositivo di autenticazione a più fattori fornito da Barclays
Spazio dedicato alla banca	Accesso remoto - Token	L'installazione di software RSA e token deve essere eseguita dal personale autorizzato che dispone dell'approvazione per operare nell'area BDS
Spazio dedicato alla banca	Accesso remoto - 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. Qualsiasi accesso remoto deve essere approvato dalle funzioni di Barclays pertinenti (compreso il Chief Security Office)

Spazio dedicato alla banca	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
Spazio dedicato alla banca	Ambiente di sviluppo software, testing e sviluppo	Il Fornitore deve accertarsi che gli sviluppi di software siano eseguiti solo per i programmi di proprietà di Barclays all'interno dello Spazio dedicato alla banca (BDS).
Spazio dedicato alla banca	Controlli di rete - Trasmissioni	Tutte le informazioni devono essere trasmesse in modo sicuro tra l'ambiente BDS e Barclays e la gestione dei dispositivi di rete deve essere eseguita usando protocolli sicuri
Spazio dedicato alla banca	Controlli di rete - Percorso	La configurazione del percorso deve garantire solo le connessioni alla rete Barclays e non deve condurre ad altre reti
Spazio dedicato alla banca	Controlli di rete - Wireless	Le reti wireless non devono essere utilizzate nel segmento delle reti Barclays per erogare i servizi.

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 i ruoli e le responsabilità per la gestione dei Dati identificativi del cliente (Client Identifying Data - CID). Il Fornitore deve rivedere i documenti che specificano ruoli e responsabilità 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)	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 e processi 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 alla pertinente giurisdizione che prevede il segreto bancario (al massimo entro 24 ore). Deve essere istituita 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.	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* per l'implementazione dei Requisiti di Segretezza bancaria dei CID dopo ogni nuova 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 D, Tabella D1), 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 D2 dell'Appendice D. * "***laddove appropriato***" *fa riferimento al vantaggio derivante dall'etichettatura in rapporto al costo 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 indicazioni della giurisdizione che prevede il segreto bancario pertinente per proteggere i CID da eventuali carenze relative 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.

** 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

I CID 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 che dispone dell'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 DCID.

- **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 qualsia si 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 poiché 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	Nome	ID elaborazione interna
	Nome della società	Numero MACC (conto liquidità soggetto a ID Contenitore Avaloq)	Data di nascita	Identificatore unico statico
	Estratto conto	Indirizzo	Nazionalità	Identificatore dinamico
	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		Cognome	

	Qualifica lavorativa o PEP (Persona esposta politicamente)		Ultima visita cliente	
	Pseudonimo		Lingua	
	Indirizzo IP		Sesso	
	Numero fax		Data di scadenza CC	
			Contatto principale	
			Luogo di nascita	
			Data di apertura del conto	
			Maggior valore di posizione/transazione	

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

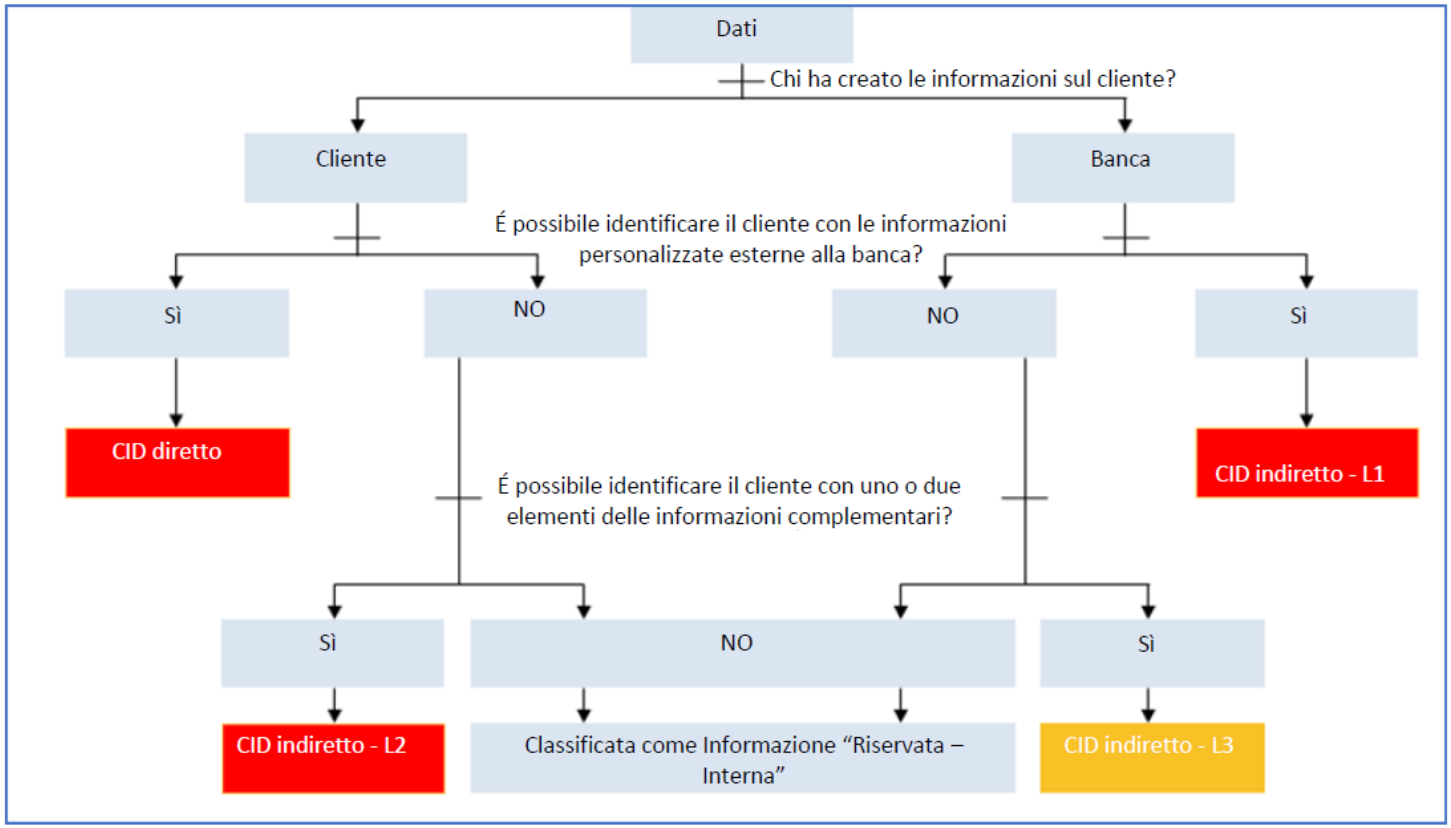
   (DCID) = Violazione del segreto bancario

2. ID contenitore

   (L1 ICID) = Violazione del segreto bancario

3. Condizioni di salute + Nazionalità

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



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). 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) 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.	• 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.

	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.	• 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 • 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 proprietario delle informazioni.	• Ai patrimoni di dati deve essere assegnato un proprietario delle informazioni.	• Ai patrimoni di dati deve essere assegnato un proprietario 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).	• 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 (sia fisici sia elettronici) non devono essere conservati in luoghi in cui persone non autorizzate possano visualizzarli o accedervi.

	• Le informazioni non devono essere lasciate in aree pubbliche nei locali a cui i visitatori possono avere accesso non controllato.	• 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 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.	• 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 copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile su ciascuna pagina.

	• 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 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 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.	• 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. • 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 proprietario delle informazioni. • 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.
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.