Obblighi di controllo dei Fornitori esterni

Sicurezza Informatica e Cibernetica

Per fornitori classificati a Basso Rischio Informatico e Cibernetico

Versione 9.0 aprile 2019

Titolo di controllo	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 e Cibernetica, nonché di un programma di sicurezza che protegga il Fornitore dalle minacce Cibernetiche in conformità con la Buona Prassi del Settore (per es. NIST, SANS, ISO27001) e i requisiti specifici applicabili. Il Fornitore si impegna ad eseguire regolarmente la Valutazione dei Rischi relativa alla sicurezza Informatica/Cibernetica nonché a implementare i controlli e a prendere i provvedimenti necessari a ridurre i rischi individuati. IL Fornitore deve mantenere attive le procedure approvate dal senior management e le norme per la gestione del rischio Informatico/Cibernetico del Fornitore. Il Fornitore deve definire i ruoli e le responsabilità per la Sicurezza Informatica/Cibernetica.	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. 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. • Il Fornitore deve aver cura di eliminare le carenze individuate con un piano di intervento correttivo (azione, proprietà, data di esecuzione) comunicato a Barclays.	Un processo di risposta e gestione degli incidenti aiuta a garantire che vengano rapidamente circoscritti e che ne venga impedita l'escalation.
3. 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	La mancata attuazione di questo controllo potrebbe rendere Barclays, la rete e gli endpoint dei Fornitori vulnerabili agli attacchi Cibernetici.

	protezione da malware e firewall dell'host e siano predisposti comandi per contenere i tentativi di sfruttamento.	
4. Cloud Computing	Qualsiasi uso di servizi di cloud computing (pubblico/privato/di comunità/ibrido). SaaS/PaaS/IaaS impiegati come parte dei servizi resi a Barclays devono essere adeguatamente protetti. 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.
5. Protezione contro i malware	È necessario attivare controlli e strumenti anti-malware per ottenere un'adeguata protezione contro i software maligni come virus e altri tipi di malware.	Le soluzioni anti-malware sono fondamentali per la protezione dei Patrimoni di dati Barclays contro i codici maligni.
6. 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). In base ai servizi erogati a Barclays, il Fornitore deve prendere in considerazione i seguenti meccanismi di protezione: **Collegamenti esterni:** Tutti i collegamenti esterni alla rete 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 dei dati. **Accesso wireless:** Tutti gli accessi wireless alla rete devono essere soggetti a protocolli di autorizzazione, autenticazione, segregazione e criptazione per prevenire le violazioni della sicurezza. **Individuazione/prevenzione delle intrusioni:** Sulla rete devono essere impiegati strumenti e sistemi di individuazione e prevenzione delle intrusioni a tutti i livelli e i dati in uscita devono essere monitorati di conseguenza per rilevare eventuali violazioni della sicurezza cibernetica, tra cui le Minacce Avanzate Permanenti (Advanced Persistent Threats - APT). **Rifiuto di servizio diffuso (Distributed Denial of Service - DDoS):**	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.

	È necessario implementare nella rete e nei principali sistemi un metodo di difesa per l'accesso avanzato al fine di proteggere in qualsiasi momento dall'interruzione dei servizi a causa di Attacchi Cibernetici. *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.*	
7. Protezione delle applicazioni	Lo sviluppo da parte del Fornitore di software / applicazioni garantisce che tutte le principali attività di sicurezza siano state inserite nelle procedure di sviluppo software per prevenire interruzioni di servizio, vulnerabilità della sicurezza e violazioni della Sicurezza Cibernetica. 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. Il Fornitore deve garantire che il codice sorgente sia eseguito, memorizzato e inviato a Barclays in modo sicuro.	I controlli che tutelano lo sviluppo di applicazioni aiutano a garantirne la sicurezza al momento della distribuzione.
8. 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 / test di penetrazione delle infrastrutture IT e delle 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. Il Fornitore deve disporre di un'adeguata procedura di registrazione, smistamento e risposta per le vulnerabilità identificate.	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.
9. Tecnologie di protezione dei dati e 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. 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 dati o i sistemi che li contengono o li elaborano devono essere protetti da manomissioni fisiche, perdita, danni o attacchi e configurazioni o modifiche non appropriati. La distruzione o	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.

	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. I sistemi devono essere configurati in modo sicuro per prevenire violazioni ingiustificate. È necessario eseguire il monitoraggio, la verifica e la registrazione dei sistemi per rilevare eventuali attività improprie o dannose.	
10. 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.	Controlli LAM appropriati aiutano a garantire la protezione dei Patrimoni di dati da un uso improprio.

	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; • la revisione periodica della procedura di accesso dell'Utente; • 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. • 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. 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.).	
11. 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);	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.

	• Scambio non sicuro di informazioni con terze parti; e • Stampa o copia inadeguata di informazioni;	
12. 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 B2), 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.
13. 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.

Appendice A: Glossario

Definizione	
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).
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.
Distruzione / Cancellazione	L'azione di sovrascrivere, cancellare o distruggere fisicamente informazioni in modo tale che non possano essere recuperate.
Minacce Avanzate Permanenti (Advanced Persistent Threats - APT)	Una minaccia avanzata permanente (APT) è un attacco clandestino alla rete informatica in cui una persona o un gruppo ottiene l'accesso non autorizzato a una rete che rimane non rilevato per un periodo prolungato.
Patrimonio di dati	Qualsiasi informazione che abbia valore, considerata nei termini dei requisiti di riservatezza, integrità e disponibilità. Qualsiasi singola informazione o insieme di informazioni che abbia valore per l'organizzazione. Generalmente raggruppate ad alto livello (di procedure aziendali).
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.
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 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.

	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.	• 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 (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 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. • 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.	• 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 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 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.	• 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.

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 C2) 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 C, Tabella C1), 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 C2 dell'Appendice C. * "***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 B: 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 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 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 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 C: Schema di Etichettatura delle informazioni di Barclays

Tabella C1: 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 B)

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	• Strategie e budget. • Stime delle performance. • Remunerazione dei dipendenti e dati personali.

	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 C2: 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. • 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. • 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 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 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.