Obblighi di controllo del Fornitore (SCO)

Sicurezza Informatica e Cibernetica (ICS)

Versione 12.0 ottobre 2022

Area di controllo / Titolo	Descrizione del controllo	Perché è importante
1. Uso approvato	Il Fornitore deve comunicare i requisiti di utilizzo accettabili a tutti i propri dipendenti, inclusi appaltatori, subappaltatori e subresponsabili, specificando le responsabilità di ciascuno. È necessario considerare i seguenti aspetti: • Uso di Internet; • Uso del software come servizio (SaaS); • Uso degli archivi del Codice Pubblico; • Utilizzo di plugin basati su browser e freeware / shareware; • Uso dei Social Media; • Uso di e-mail aziendali; • Uso di messaggistica istantanea; • Uso di apparecchiature fornite dal Fornitore; • Uso di apparecchiature non fornite dal Fornitore (ad es. portare il proprio dispositivo); • Uso di dispositivi di archiviazione portatili/rimovibili; • Responsabilità nella gestione, nel salvataggio e nella conservazione del Patrimonio di dati di Barclays; • Elaborazione dei canali di perdita dati; e • Rischi e conseguenze dell'uso improprio delle suddette voci e/o qualsiasi risultato illegale, dannoso o offensivo derivante da tale uso improprio. Il Fornitore deve adottare misure adeguate per assicurare la conformità ai requisiti di utilizzo accettabile.	I requisiti di uso accettabile aiutano a rafforzare l'ambiente di controllo per la protezione dei Patrimoni di Dati
2. Sicurezza del perimetro e della rete	Il Fornitore deve garantire che tutti i Sistemi e le applicazioni gestiti dallo stesso, e/o dai relativi subappaltatori/subresponsabili che supportano i servizi Barclays, siano protetti dalle **minacce alla rete in entrata e in uscita.** È necessario implementare controlli per garantire la sicurezza delle informazioni nelle reti e la protezione dei servizi connessi dall'accesso non autorizzato. Il Fornitore deve Identificare, Proteggere, Rilevare e Rispondere agli eventuali avvisi di sicurezza e violazioni.	La mancata implementazione di questo principio potrebbe comportare l'attacco delle reti esterne o interne da parte di hacker al fine di ottenere l'accesso ai servizi o ai dati contenuti.

	I Controlli di sicurezza della rete garantiscono la protezione delle informazioni nelle reti e le relative strutture di elaborazione delle informazioni di supporto devono includere, a titolo di esempio non esaustivo, le aree seguenti: • Inventario aggiornato di tutti i perimetri della rete aziendale (tramite un'Architettura/Diagramma di rete), che deve essere rivisto almeno una volta l'anno. • Connessioni esterne alla rete del Fornitore, documentate, verificate e approvate prima di stabilire la connessione, al fine di prevenire potenziali violazioni della sicurezza. • Le reti del Fornitore devono essere protette applicando principi di difesa in profondità, come la segmentazione della rete, firewall, controlli fisici di accesso alle apparecchiature di rete e così via. • Il Fornitore deve adottare tecnologie di prevenzione delle intrusioni di rete al fine di rilevare e prevenire il traffico dannoso per tutto il traffico in entrata o in uscita, aggiornare i database delle firme in linea con le migliori pratiche del settore e applicare tempestivamente gli aggiornamenti rilasciati dai fornitori delle soluzioni. • Uso di potenti firewall di rete per fornire un livello di difesa perimetrale contro attacchi di rete dolosi. • Il traffico della rete Internet deve passare attraverso un proxy configurato per filtrare le connessioni non autorizzate. • I dispositivi di rete sono protetti in modo sicuro per prevenire attacchi dolosi. • Tutte le regole di configurazione che consentono il flusso del traffico attraverso i dispositivi di rete devono essere documentate in un sistema di gestione della configurazione, con una motivazione aziendale specifica per ogni regola. • Separazione logica delle porte/interfacce per la gestione dei dispositivi dal traffico LAN/utente, controlli di autenticazione appropriati. • Scansioni regolari delle porte eseguite esternamente al perimetro della rete, al fine di rilevare le eventuali porte non autorizzate accessibili dall'esterno. • Comunicazioni sicure tra i dispositivi e le postazioni di gestione/console. • La registrazione e il monitoraggio devono includere il rilevamento e la segnalazione delle attività sospette (basandosi sul comportamento e sugli indicatori dei trigger di compromissione), ad esempio tramite un sistema SIEM. • La connessione di rete tra uffici/fornitore di servizi cloud/data center deve essere crittografata in base a un protocollo sicuro. I Dati / il Patrimonio informatico di Barclays in transito all'interno della Wide Area Network (WAN) del Fornitore devono essere criptati.	

	• Il Fornitore deve esaminare le regole dei firewall (esterno e interno) almeno una volta l'anno. • Il Fornitore deve garantire che l'accesso alla rete interna venga monitorato tramite appropriati controlli di accesso alla rete. • Solo i dispositivi autorizzati (dispositivi forniti da terze parti con strutture sicure e non BYOD) devono essere avere la possibilità di connettersi alla rete del Fornitore. • Tutti gli accessi wireless alla rete devono essere soggetti a protocolli di autorizzazione, autenticazione, segmentazione e crittografia avanzata, al fine di prevenire le violazioni della sicurezza. • L'accesso remoto alla rete del Fornitore deve utilizzare l'autenticazione a più fattori. • Il Fornitore deve predisporre una rete logicamente isolata per i servizi da erogare a Barclays. Il Fornitore deve garantire che le applicazioni e i server utilizzati per fornire servizi a Barclays non siano distribuiti su reti non affidabili (reti al di fuori del perimetro di sicurezza dell'utente, che non rientrano nell'ambito del controllo amministrativo, ad esempio per l'accesso a Internet) senza controlli di sicurezza adeguati. Il Fornitore che ospita le Informazioni di Barclays (inclusi i subappaltatori e i subresponsabili) in un data center o cloud deve possedere una certificazione che confermi l'applicazione delle Migliori pratiche del settore per la gestione della sicurezza. Rete T2 e T3 - • La rete T2 deve essere separata in modo logico dalla rete aziendale del Fornitore da un Firewall e tutto il traffico in entrata e in uscita deve essere limitato e monitorato. • La configurazione del percorso deve garantire solo le connessioni alla rete Barclays e non deve condurre ad altre reti del Fornitore. • Il router Edge/terminale dell'ultimo miglio del Fornitore che si collega ai gateway Extranet di Barclays deve essere configurato in modo sicuro, applicando controlli di limitazione per porte, protocolli e servizi. o La registrazione e il monitoraggio devono includere il rilevamento e la segnalazione delle attività sospette (basandosi sul comportamento e sugli indicatori dei trigger di compromissione), ad esempio tramite un sistema SIEM. Il provider terzo deve garantire che tutti i sistemi e le applicazioni utilizzati per fornire servizi che Barclays considera ad alto rischio, segnalandoli al vendor, siano segmentati in rete in base ai principi seguenti:	

	i. È necessario adottare un approccio di segmentazione per limitare l'esposizione al rischio, prevenire i movimenti laterali nella rete e ridurre il rischio di trasmissione in rete. Le applicazioni devono essere implementate in segmenti autonomi, al fine di limitare al massimo il rischio. Esempio: Area Pagamenti rapidi. ii. Ove possibile, tutte le infrastrutture e i dati relativi alle applicazioni aziendali devono essere distribuiti in una Zona applicativa sicura e autocontenuta, separata dalla rete interna di Barclays, utilizzando una tecnologia applicativa approvata dal CSO (ad esempio firewall di rete, una soluzione di segmentazione approvata). Nota - Alcuni scenari possono giustificare la suddivisione dei componenti in più zone, applicazioni e database, ad esempio quando vengono utilizzate piattaforme condivise. Ogni applicazione deve essere valutata singolarmente, adottando l'approccio più appropriato definito e concordato insieme a un Consulente per la sicurezza del CSO. iii. I servizi devono essere separati fisicamente o logicamente. Il fabric di rete sottostante (come il cablaggio e gli switch) può essere condiviso con altre applicazioni e servizi, ossia i segmenti possono essere definiti in modo logico senza necessariamente applicare una separazione fisica dal resto della rete di Barclays. iv. Le zone applicative devono limitare i flussi di traffico da e verso le altre zone (compresa la rete CIPE interna) esclusivamente a quelli richiesti per il funzionamento del servizio e di qualsiasi strumento di gestione, monitoraggio e sicurezza approvato. Le configurazioni devono indicare le porte, i protocolli e gli indirizzi IP specifici per i percorsi di comunicazione consentiti, mentre tutte le altre comunicazioni devono essere soggette a restrizioni per impostazione predefinita. Le regole che contengono intervalli dovrebbero essere evitate, approvandole solo come eccezione, al fine di garantire che siano abilitati solo i requisiti minimi di connettività. v. I container devono essere nettamente separati da efficaci controlli logici che impediscano il movimento laterale tra gli stessi, al fine di implementare l'isolamento. La compromissione di un container non deve determinare la compromissione degli altri container eseguiti nello stesso host/cluster. vi. Tutte le implementazioni della segmentazione devono offrire una funzionalità di gestione centralizzata delle policy, con la capacità di, o l'integrazione necessaria per, verificare e segnalare la conformità alle policy (vedere il documento Conformità dei firewall), fornendo anche un registro verificabile delle modifiche. vii. Ove possibile e fattibile, devono essere applicati controlli/ispezioni stateful. viii. Le funzionalità di segmentazione devono essere "fail-safe" di modo che, ad esempio in caso di errore di una funzionalità, i set di regole approvati per bloccare o consentire il traffico rimangano applicati.	

	ix. Qualsiasi traffico tra sistemi di produzione e non di produzione nelle zone applicative deve essere consentito solo come eccezione e deve essere registrato. **Indicazioni per il Cliente dei Servizi Cloud (Fornitore) utilizzato per la fornitura dei servizi a Barclays** Il Cliente dei Servizi Cloud (CSC, Cloud Service Customer) deve garantire l'implementazione di controlli appropriati per la sicurezza della rete al fine di salvaguardare il servizio Barclays. • Il Cliente dei Servizi Cloud (CSC, Cloud Service Customer) deve definire i propri requisiti di separazione delle reti al fine di ottenere l'isolamento del tenant nell'ambiente condiviso di un servizio cloud e verificare che il provider di servizi cloud soddisfi tali requisiti. • Il criterio di controllo dell'accesso applicato dal Cliente del Servizio Cloud per l'uso dei servizi di rete deve specificare i requisiti per l'accesso degli utenti a ciascun servizio cloud separato utilizzato. *Nota. Ai fini del presente controllo, il termine "rete" si riferisce a qualsiasi rete non appartenente a Barclays sotto la responsabilità del Fornitore, incluse le reti dei relativi subappaltatori.*	
3. Rifiuto di rilevamento del servizio (Denial of Service Detection)	Il Fornitore deve garantire la capacità di rilevare e proteggere la rete dagli attacchi Denial of Service (DoS) e Distributed Denial of Services (DDoS). Il Fornitore deve garantire che i canali esterni o connessi a Internet utilizzati per supportare i servizi erogati a Barclays dispongano di una protezione DDoS/DoS adeguata per garantire la disponibilità. Se il Fornitore ospita **sistemi e applicazioni che forniscono servizi** e contengono dati di Barclays, o supportando un servizio con categoria di resilienza 0 o 1, tali sistemi e applicazioni devono disporre di una protezione adeguata dagli attacchi DoS, al fine di garantire la disponibilità.	Se questo principio non viene applicato, Barclays e il Fornitore potrebbero non riuscire a sventare gli attacchi di tipo Denial of Service.
4. Lavoro a distanza (accesso remoto)	**Accesso remoto alla rete Barclays** L'accesso remoto alla rete Barclays tramite l'applicazione Citrix di Barclays non viene fornito per impostazione predefinita. Per accedere alla rete Barclays da sedi, postazioni esterne o postazioni domiciliari non approvate, e tramite qualsiasi metodo di accesso remoto, è necessario ottenere preventivamente l'approvazione e l'autorizzazione di Barclays (Chief Security Office - Team ECAM (externalcyberassurance@barclayscorp.com).	I controlli di Accesso Remoto aiutano a garantire che i dispositivi non autorizzati e non sicuri non siano collegati all'ambiente Barclays da remoto.

	Il Fornitore deve garantire l'implementazione dei controlli seguenti per l'accesso remoto: • L'accesso remoto alla rete del Fornitore deve essere soggetto a crittografia avanzata e autenticazione a più fattori. • L'accesso alla rete Barclays deve avvenire tramite l'applicazione Barclays Citrix con Token RSA (Hard & Soft) fornito da Barclays • Il Fornitore deve mantenere un inventario di tutti i token RSA (Hardware e Software) forniti da Barclays. L'uso dei token deve essere supportato da un processo di gestione, che deve includere la revisione e il monitoraggio degli eventi di assegnazione, perdita/furto, utilizzo e restituzione dei token (Token hardware). • Il Fornitore deve mantenere un registro aggiornato e corretto dei propri dipendenti autorizzati a lavorare da remoto, con la giustificazione aziendale per ogni dipendente approvato, inclusi i subappaltatori e i subresponsabili. • **Ogni tre mesi, il Fornitore deve effettuare la riconciliazione di tutti i dipendenti autorizzati ad accedere da remoto, seguita da una presentazione dei risultati formali a Barclays (Chief Security Office - Team ECAM (externalcyberassurance@barclayscorp.com).** • Appena verrà informata che un determinato accesso non è più necessario (ad esempio in caso di licenziamento di un dipendente, riassegnazione di un progetto e così via), Barclays provvederà a disattivare le relative credenziali di autenticazione **entro ventiquattro (24) ore.** • Barclays disattiverà prontamente le credenziali di autenticazione nel caso in cui tali credenziali non siano state utilizzate per un periodo di tempo (tale periodo di non utilizzo non deve superare un mese). • Il Fornitore deve garantire che l'endpoint utilizzato per il collegamento da remoto ai sistemi informativi di Barclays sia configurato in modo sicuro (indicando ad esempio il livello delle patch, lo stato della protezione anti-malware e così via). • I servizi che hanno accesso alla stampa remota tramite l'applicazione Barclays Citrix devono essere approvati e autorizzati da Barclays (Chief Security Office - Team ECAM - **externalcyberassurance@barclayscorp.com**). Il Fornitore deve mantenere i registri ed eseguire la riconciliazione trimestrale. • **I dispositivi personali/BYOD non devono essere autorizzati ad accedere all'ambiente Barclays e/o ai dati Barclays presenti/memorizzati all'interno dell'ambiente gestito dal Fornitore (che include il Personale, i Consulenti, i Lavoratori occasionali, gli appaltatori e i Partner di servizi gestiti, nonché i subappaltatori e i subresponsabili del Fornitore).**	

<table>
<tr>
<td></td>
<td>Nota: l'accesso remoto alla rete e ai dati di Barclays non è consentito se non specificamente approvato e autorizzato da Barclays.

Accesso remoto ai dati Barclays presenti nell'ambiente o nella rete del Fornitore

L'accesso remoto ai dati di Barclays residenti/archiviati e/o elaborati nell'ambiente gestito dal Fornitore non è disponibile per impostazione predefinita. Per accedervi da sedi, postazioni esterne o postazioni domiciliari non approvate il Fornitore deve richiedere l'autorizzazione di Barclays (Chief Security Office - Team ECAM - externalcyberassurance@barclayscorp.com).

• L'accesso remoto alla rete del Fornitore deve essere soggetto a crittografia avanzata, durante il trasferimento dei dati, e autenticazione a più fattori.
• Il Fornitore deve conservare le registrazioni delle persone che lavorano da remoto e delle motivazioni per l'accesso remoto.
• Il Fornitore deve eseguire la riconciliazione di tutti gli utenti remoti ogni tre mesi
• Appena un determinato accesso non risulterà più necessario (ad esempio in caso di licenziamento di un dipendente, riassegnazione di un progetto e così via), il Fornitore provvederà a disattivare le relative credenziali di autenticazione entro ventiquattro (24) ore.
• Il Fornitore deve garantire che l'endpoint utilizzato per il collegamento da remoto ai dati di Barclays sia configurato in modo sicuro (indicando ad esempio il livello delle patch, lo stato della protezione anti-malware e così via).
• I dispositivi personali/BYOD non devono essere autorizzati ad accedere ai dati Barclays presenti/memorizzati all'interno dell'ambiente gestito dal Fornitore (che include il Personale, i Consulenti, i Lavoratori occasionali, gli appaltatori e i Partner di servizi gestiti).</td>
<td></td>
</tr>
<tr>
<td>5. Gestione dei registri di sicurezza</td>
<td>Il Fornitore deve implementare un framework gestito e approvato e ben consolidato per la gestione dei registri e degli audit. Tale framework deve includere i sistemi IT essenziali, tra cui applicazioni, apparecchiature di rete, dispositivi di sicurezza e server impostati in modo da registrare gli eventi chiave. Il Fornitore deve garantire che i registri siano centralizzati e adeguatamente protetti contro la manomissione e/o la cancellazione. Deve inoltre conservarli per il periodo più lungo fra un minimo di 12 mesi e il periodo imposto dalla legge.
<table>
<tr><th>Categoria</th><th>Sistemi a impatto basso / Servizio</th><th>Sistemi a impatto medio / Servizio</th><th>Sistemi a impatto elevato / Servizio</th></tr>
</table>
</td>
<td>Se questo controllo non viene implementato, il Fornitore potrebbe non riuscire a rilevare e rispondere in tempi ragionevoli all'uso inappropriato o dannoso dei suoi dati o servizi.</td>
</tr>
</table>

Conservazione dei registri	3 mesi	6 mesi	12 mesi

Il framework di gestione dei registri di sicurezza deve coprire le aree seguenti:

- Il Fornitore deve stabilire politiche e procedure per la gestione dei registri.
- Il Fornitore deve creare e mantenere un'infrastruttura di gestione dei registri.
- Il Fornitore deve definire i ruoli e le responsabilità dei singoli e dei team che devono essere coinvolti nella gestione dei registri.
- Raccolta, gestione e analisi dei registri di audit degli eventi al fine di contribuire a monitorare, rilevare, comprendere e/o recuperare in seguito a un attacco.
- Abilitare la registrazione del sistema per includere informazioni dettagliate come la fonte di un evento, la data, l'utente, la marca temporale, gli indirizzi di origine, gli indirizzi di destinazione e altri elementi utili.
- Di seguito alcuni esempi di registri di eventi:
    - IDS/IPS, Router, Firewall, Web Proxy, Software per l'accesso remoto (VPN), Server di autenticazione, Applicazioni, Registri per database.
    - Login riusciti, tentativi di login falliti (ad esempio ID utente o password sbagliati), creazione, modifica e cancellazione di account utente
    - Registri di modifica della configurazione.
- Servizi Barclays relativi ad applicazioni aziendali e sistemi di infrastrutture tecniche su cui deve essere abilitata la registrazione, in base alle Migliori pratiche di settore applicabili, compresi quelli che sono stati esternalizzati o che risiedono nel cloud.
- Analisi dei registri degli eventi relativi alla sicurezza (compresa la normalizzazione, l'aggregazione e la correlazione).
- Sincronizzazione delle marche temporali nei registri degli eventi con una fonte comune e affidabile
- Protezione dei registri degli eventi relativi alla sicurezza (ad es. tramite cifratura, MFA, controllo degli accessi e backup).
- Adottare le azioni necessarie per risolvere i problemi individuati e rispondere agli Incidenti di Sicurezza Informatica in modo rapido ed efficace.
- Implementazione di Security Information and Event Management (SIEM) o di strumenti di analisi dei registri per la correlazione e l'analisi dei registri.
- Implementazione di strumenti adeguati per eseguire l'aggregazione centrale e la correlazione in tempo reale di attività anomale, allarmi di rete e di sistema, e

	informazioni rilevanti su eventi e minacce informatiche da più fonti, sia interne che esterne, per rilevare e prevenire meglio i molteplici attacchi informatici. • I principali eventi registrati devono includere quelli che rischiano di compromettere la riservatezza, l'integrità e la disponibilità dei Servizi resi a Barclays e che potrebbero contribuire all'identificazione o all'analisi degli incidenti di rilievo e/o delle violazioni dei diritti di accesso subiti dai Sistemi del Fornitore • Verifica periodica del rispetto dei requisiti precedenti da parte del framework. **Indicazioni per il Cliente dei Servizi Cloud (Fornitore) utilizzato per la fornitura dei servizi a Barclays** Il Cliente dei Servizi Cloud (CSC, Cloud Service Customer) deve garantire l'implementazione di controlli appropriati per la Gestione dei registri di sicurezza al fine di salvaguardare il servizio Barclays. • Il Cliente del Servizio Cloud deve definire e documentare i propri requisiti di registrazione degli eventi e verificare che il servizio cloud li soddisfi. • Se al Cliente del Servizio Cloud viene delegata un'operazione con privilegi, è necessario registrare il funzionamento e le prestazioni di tale operazione. Il Cliente del Servizio Cloud deve determinare se le funzionalità di registrazione fornite dal provider di servizi cloud sono appropriate o se deve implementare ulteriori funzionalità di registrazione autonomamente. • Il Cliente del Servizio Cloud deve richiedere informazioni sulla sincronizzazione dell'orologio utilizzata per i sistemi del provider di servizi cloud. • Il Cliente del Servizio Cloud deve richiedere al provider di servizi cloud informazioni sulle funzionalità di monitoraggio dei servizi disponibili per ciascun servizio cloud.	
6. Difese contro i malware	In linea con le Migliori pratiche del settore, il Fornitore deve adottare policy e procedure consolidate, oltre a processi aziendali di supporto e misure tecniche, al fine di prevenire l'esecuzione di malware nell'intero ambiente IT. Il Fornitore deve garantire che la protezione dai malware venga applicata in ogni momento a tutte le risorse IT applicabili per prevenire interruzioni del servizio o violazioni della sicurezza. La protezione dal malware deve includere quanto segue, a titolo di esempio non esaustivo: • Software anti-malware gestito a livello centrale per monitorare e difendere l'ambiente IT dell'organizzazione. • Aggiornamento regolare del motore di scansione del software anti-malware aziendale	Le soluzioni anti-malware sono fondamentali per la protezione dei Patrimoni di dati Barclays contro i Codici Maligni.

	• Aggiornamento regolare del database delle firme • Inviare tutti gli eventi di rilevamento di malware agli strumenti di amministrazione anti-malware aziendali e ai server di registro degli eventi per l'analisi e gli avvisi. • Il Fornitore deve implementare controlli appropriati al fine di proteggere i dispositivi mobili utilizzati per i servizi di Barclays dal malware e da eventuali attacchi. Nota: Anti-malware per includere il rilevamento di (ma non solo) codici mobili non autorizzati, virus, spyware, software key logger, botnet, worm, trojan, ecc.	
7. Standard per la configurazione sicura	Il Fornitore deve disporre di un framework consolidato per garantire che tutti i sistemi/apparecchiature di rete configurabili siano configurati in modo sicuro, conformemente alle Migliori pratiche del settore (ad esempio NIST, SANS, CIS). Il processo standard di configurazione deve coprire, a titolo esemplificativo, le seguenti aree: • Definizione di policy, procedure/misure organizzative e strumenti per consentire l'implementazione degli standard di configurazione della sicurezza secondo le Migliori pratiche del settore per tutti i dispositivi di rete e i sistemi operativi, le applicazioni e i server autorizzati. • Esecuzione di controlli regolari (almeno una volta l'anno) dell'applicazione di quanto sopra al fine di garantire la risoluzione tempestiva dei problemi di conformità agli standard di sicurezza di base. Attuazione di controlli e procedure di monitoraggio appropriate al fine di garantire l'integrità di strutture e dispositivi. • I sistemi e i dispositivi di rete sono configurati in modo da funzionare secondo i principi di sicurezza (ad es. concetto di limitazione dei controlli di porte, protocolli e servizi, nessun software non autorizzato, rimozione e disabilitazione degli account utente non necessari, modifica delle password di default degli account, rimozione del software non necessario, ecc.) • Esecuzione di verifiche periodiche della configurazione, almeno una volta all'anno, per garantire che nell'ambiente di produzione effettivo non siano presenti configurazioni non autorizzate. • Garantire che la gestione della configurazione regoli gli standard di configurazione sicura in tutte le classi di beni e che rilevi, avverta e risponda efficacemente alle modifiche o alle deviazioni della configurazione. **Indicazioni per il Cliente dei Servizi Cloud (Fornitore) utilizzato per la fornitura dei servizi a Barclays**	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

	Il Cliente dei Servizi Cloud (CSC, Cloud Service Customer) deve garantire l'implementazione di controlli di Configurazione sicura appropriati per salvaguardare il servizio Barclays. • Quando configurano le macchine virtuali, i clienti dei servizi cloud devono verificare che gli aspetti appropriati siano stati potenziati (ad esempio, vengono utilizzati solo i protocolli, le porte e i servizi necessari) e che siano in vigore misure tecniche adeguate (ad esempio, anti-malware, registrazione) per ogni macchina virtuale utilizzata.	
8. Sicurezza dell'endpoint	Il Fornitore deve adottare un approccio unificato alla gestione degli endpoint, al fine di garantire che gli endpoint utilizzati per accedere alla rete di Barclays o per elaborare e/o accedere ai dati e agli asset informativi di Barclays, siano configurati per la protezione dagli attacchi dannosi. Devono essere utilizzate le Migliori pratiche del settore e la struttura di sicurezza degli endpoint deve includere, a titolo di esempio non esaustivo: • Crittografia completa del disco rigido. • Disattivare tutti i software/servizi/porte non necessari. • Disattivare l'accesso ai diritti di amministrazione per l'utente locale. • I dipendenti del Fornitore non possono modificare le impostazioni di base, come il Service Pack predefinito, la partizione di sistema, i servizi predefiniti, l'antivirus e così via. • Occorre disattivare la funzione per la copia di informazioni/dati di Barclays su supporti USB esterni. • Aggiornato con le ultime firme antivirus e patch di sicurezza. • Prevenzione della perdita di dati limitata al divieto di taglia-copia-incolla e stampa-schermo dei dati Barclays • Occorre disattivare l'accesso alla stampante per impostazione predefinita. • Il Fornitore deve assicurarsi di bloccare l'esfiltrazione dei dati di Barclays a siti di social network, servizi webmail e siti in grado di archiviare informazioni quali, a titolo di esempio non esaustivo, Google Drive, Dropbox e iCloud. • Occorre disattivare il trasferimento/condivisione dei dati di Barclays tramite software o strumenti di messaggistica immediata. • Occorre arrestare, eliminare e rilevare la presenza e/o l'uso di software non autorizzato, incluso il software dannoso.	La mancanza di questo controllo potrebbe esporre Barclays, la rete e gli endpoint dei Fornitori agli attacchi informatici.

	Nota: i supporti rimovibili/dispositivi portatili devono essere disabilitati per impostazione predefinita e abilitati solo per legittimi motivi di lavoro. Il Fornitore deve mantenere immagini o modelli sicuri per tutti i sistemi di un'azienda, sulla base degli standard di configurazione approvati dall'organizzazione. Qualunque sistema esistente o appena implementato che risulti compromesso deve essere configurato utilizzando immagini o modelli approvati. Quando agli endpoint (Laptop/Desktop) viene concesso l'accesso alla rete Barclays tramite le applicazioni Barclays Citrix su Internet, il Fornitore deve installare lo strumento End Point Analysis (EPA) fornito da Barclays per convalidare la sicurezza degli endpoint e la conformità del sistema operativo; solo ai dispositivi che superano i controlli End Point Analysis sarà concesso l'accesso remoto alla rete Barclays tramite l'applicazione Barclays Citrix. Se il Fornitore non è in grado di installare o utilizzare lo strumento EPA, deve informare il Barclays Relationship Manager. Dispositivi mobili utilizzati per i servizi Barclays - • Il Fornitore deve assicurarsi di implementare funzionalità per la gestione unificata degli endpoint (UEM, Unified Endpoint Management) o per la gestione dei dispositivi mobili (MDM, Mobile Device Management) al fine di controllare e gestire in modo sicuro i dispositivi mobili che contengono e/o hanno accesso a informazioni classificate Barclays, durante l'intero ciclo di vita, riducendo il rischio di compromissione dei dati. • Il Fornitore deve garantire l'implementazione e l'utilizzo delle funzionalità di blocco e cancellazione remota dei dispositivi mobili al fine di proteggere le informazioni in caso di smarrimento, furto o compromissione di un dispositivo. • Crittografia dei dati di Barclays archiviati e/o elaborati nei dispositivi mobili	
9. Prevenzione della fuga di dati	Il Fornitore deve utilizzare un framework di gestione efficace approvato per proteggere i dati di Barclays da perdite/esfiltrazione, includendo, a titolo di esempio non esaustivo, i seguenti canali di perdita dei dati: - • Trasferimento non autorizzato di informazioni al di fuori della rete interna/rete del Fornitore. o E-mail o Internet/Web Gateway (inclusi archiviazione on-line e webmail) o DNS	Occorre applicare in modo efficace controlli appropriati al fine di assicurare che l'accesso alle informazioni Barclays sia riservato a coloro che hanno reale necessità di consultarli (riservatezza) e che i dati siano protetti contro le modifiche

	• 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 di informazioni non sicuro con terze parti (subappaltatori, subresponsabili). • Stampa o copia inadeguata di informazioni.	non autorizzate (integrità) e possano essere recuperati e trasmessi quando richiesto (disponibilità). In caso di mancata implementazione dei suddetti requisiti, i dati sensibili Barclays possono essere esposti a modifiche, divulgazioni e accessi non autorizzati e a danni, perdite o distruzione che possono comportare sanzioni legali e normative, danneggiamento della reputazione e perdite o interruzioni dell'attività
10. Sicurezza dei dati	Il Fornitore deve proteggere i dati di Barclays che conserva e/o elabora, mediante una combinazione di tecniche di crittografia, protezione dell'integrità e prevenzione della perdita di dati. L'accesso ai dati di Barclays deve essere limitato esclusivamente ai dipendenti autorizzati del Fornitore e protetto da contaminazione, attacchi di aggregazione, attacchi di inferenza, minacce allo storage, incluse quelle provenienti dagli ambienti di cloud computing, a titolo di esempio non esaustivo. I controlli sulla sicurezza dei dati devono coprire, a titolo esemplificativo ma non esaustivo, le seguenti aree: 1. Il Fornitore è obbligato a rispettare in ogni momento tutte le leggi applicabili alla protezione dei dati. 2. Deve definire policy, processi e procedure a supporto dei processi aziendali e delle misure tecniche. Deve documentare e gestire i flussi di dati per i dati che risiedono all'interno dell'ubicazione geografica del servizio (fisica e virtuale). La documentazione dovrebbe includere la descrizione dettagliata delle applicazioni e dei componenti dei sistemi che fanno parte del flusso di dati. 3. Deve mantenere aggiornato il diagramma di flusso dei dati di Barclays che risiedono all'interno delle ubicazioni geografiche (fisiche e virtuali), nelle applicazioni e nei componenti di sistema. 4. Deve gestire un inventario di tutte le informazioni sensibili/riservate di Barclays memorizzate, elaborate o trasmesse dal Fornitore. 5. Deve garantire che tutti i dati di Barclays siano classificati ed etichettati in base allo standard di classificazione e protezione delle informazioni approvato dal management. 6. Deve proteggere i dati inattivi: a. Applicando una crittografia avanzata per impedire l'esposizione degli asset informativi di Barclays. 7. Monitoraggio delle attività del database;	

	a. Monitorare e registrare l'accesso al database e l'attività per identificare rapidamente ed efficacemente le attività dannose. 8. Deve proteggere i dati in uso: a. Garantendo l'esecuzione di controlli sulle funzionalità di gestione degli accessi utilizzate per l'elaborazione delle informazioni sensibili al fine impedire lo sfruttamento delle informazioni sensibili b. Utilizzare tecnologie di mascheramento e offuscamento dei dati per proteggere efficacemente i dati sensibili in uso dalla divulgazione involontaria e/o dallo sfruttamento malevolo. 9. Deve proteggere i dati in transito: a. Sfruttare le forti capacità di crittografia per garantire la protezione dei dati durante il transito. b. Solitamente la crittografia avanzata dei dati in transito viene ottenuta utilizzando la crittografia di Trasporto o Carico utile (Messaggio o Campo selettivo). I meccanismi di cifratura del trasporto includono, a titolo esemplificativo: 10. Protocollo Transport Layer Security (TLS), seguendo le Migliori pratiche del settore per la crittografia moderna, incluso l'utilizzo o il rifiuto di protocolli e cifrari 11. Tunneling sicuro (Secure Tunneling - IPsec) 12. Guscio di sicurezza (Secure Shell - SSH) a. I protocolli di sicurezza del trasporto devono essere configurati in modo da evitare la negoziazione di algoritmi più deboli e/o lunghezze di chiave più brevi, quando entrambi i punti finali supportano l'opzione più forte.	

	13. Backup dei dati – a. Occorre adottare le misure appropriate per garantire l'esecuzione di un backup adeguato per dati e Informazioni, affinché siano recuperabili (e possano essere ripristinati in un tempo ragionevole) conformemente ai requisiti concordati con Barclays. b. Occorre assicurarsi che i backup siano adeguatamente protetti tramite sicurezza fisica e/o crittografia, sia quando vengono memorizzati che quando vengono spostati attraverso la rete. Sono compresi i backup remoti e i servizi cloud. c. Accertarsi che tutti i dati Barclays siano automaticamente e regolarmente sottoposti a backup. d. Se il provider di servizi cloud fornisce funzionalità di backup come parte del servizio cloud, il Cliente del Servizio Cloud deve richiedere le specifiche della funzionalità di backup al provider di servizi cloud. Il Cliente del Servizio Cloud deve inoltre verificare che tale funzionalità soddisfi i propri requisiti di backup. Se il provider di servizi cloud non fornisce funzionalità di backup, il Cliente del Servizio Cloud è responsabile di implementarle.	
11. Sicurezza del software applicativo	Il Fornitore deve sviluppare le applicazioni utilizzando pratiche di codifica sicura e operando in un ambiente sicuro. Se il Fornitore sviluppa applicazioni destinate all'uso da parte di Barclays, o che vengono utilizzate per supportare il servizio fornito a Barclays, deve adottare un framework di sviluppo sicuro del software per integrare la sicurezza nel ciclo di vita dello sviluppo del software. Il Fornitore deve testare e correggere le vulnerabilità del software prima di consegnarlo a Barclays. La sicurezza del software applicativo deve coprire, a titolo esemplificativo ma non esaustivo, le seguenti aree:	I controlli che tutelano lo sviluppo di applicazioni aiutano a garantirne la sicurezza al momento della distribuzione.

	• Stabilire e adottare standard di programmazione sicuri approvati dal management, in linea con le Migliori pratiche del settore, al fine di prevenire vulnerabilità e interruzioni del servizio. • Stabilire pratiche di codifica sicure e adeguate al linguaggio di programmazione. • Tutte le attività di sviluppo devono essere svolte in un ambiente non produttivo. • Mantenere ambienti separati per i sistemi di produzione e non. Gli sviluppatori non devono avere un accesso non monitorato agli ambienti di produzione. • Separare le mansioni per gli ambienti di produzione e non. • I sistemi devono essere sviluppati in linea con le Migliori pratiche del settore (ad esempio OWASP). • Il codice deve essere conservato in modo sicuro e soggetto ai controlli della Garanzia di Qualità. • Il codice deve essere adeguatamente protetto da modifiche non autorizzate una volta che il test è stato confermato e consegnato in produzione. • Per il software sviluppato dal Fornitore utilizzare solo componenti aggiornati di terze parti di fiducia. • Applicare strumenti di analisi statica e dinamica per verificare il rispetto delle pratiche di codifica sicura. • Il Fornitore deve garantire che i dati attivi (compresi i Dati personali) non vengano utilizzati in ambienti diversi da quello di produzione. • Le applicazioni e le interfacce di programmazione (API) devono essere progettate, sviluppate, implementate e testate conformemente alle Migliori pratiche di settore (ad esempio OWASP, per le applicazioni web). • Vietare l'uso dei repository di codice pubblici Il Fornitore è tenuto a proteggere le applicazioni web distribuendo firewall per applicazioni web (WAF) che esaminano tutto il traffico verso l'applicazione web per verificare che non vi siano attacchi di applicazioni web esistenti e comuni. Per le applicazioni che non sono basate sul web, devono essere implementati specifici firewall applicativi, se tali strumenti sono disponibili per il tipo di applicazioni in uso. Se il traffico è criptato, il dispositivo dovrebbe trovarsi 'dietro' la criptazione o essere in grado di decriptare il traffico prima dell'analisi. Se nessuna delle due opzioni è applicabile, dovrebbe essere implementato un firewall per applicazioni web basate su host.	
12. Logical Access Management (LAM)	L'accesso alle Informazioni deve essere basato su restrizioni, tenendo in debita considerazione i principi dell'Esigenza di conoscere (need-to-know), del Privilegio minimo e	Controlli LAM appropriati aiutano a garantire la

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

	• Ogni account deve essere associato in modo univoco a una singola persona, che sarà responsabile di tutte le attività svolte utilizzando tale account. • Ricertificazione dell'accesso - Occorre provvedere ai controlli atti ad assicurare che i permessi di accesso siano riesaminati almeno ogni 12 mesi, al fine di verificare che siano commisurati allo scopo. • Tutte le autorizzazioni di accesso con privilegi devono essere esaminate almeno ogni sei (6) mesi. La gestione dei privilegi deve essere conforme alle procedure efficaci per la gestione degli accessi con privilegi (PAM, Privilege Access Management). • Le credenziali non personali (ad esempio password e segreti) devono essere inserite in uno strumento idoneo, in linea con i migliori standard del settore, che garantisce riservatezza, integrità e disponibilità (CIA, Confidentiality, Integrity and Availability) per le credenziali e le capacità break-glass. Laddove ciò non sia possibile, le credenziali devono essere protette in modo che nessuno possa mai utilizzarle. Se l'account deve essere utilizzato da un essere umano, l'accesso deve essere temporaneo, limitato nel tempo e seguito da una reimpostazione delle credenziali (una procedura comunemente denominata "break-glass"). In informatica, l'espressione "break-glass" viene utilizzata per descrivere l'atto di estrarre la password di un account di sistema per l'uso da parte di un essere umano. Questa funzione viene solitamente utilizzata per gli account di sistema di livello più elevato, come root per Unix o SYS/SA per i database. Questi account sono altamente privilegiati e non vengono assegnati a una persona specifica. La funzione di "break-glass" ne limita l'utilizzo in base alla durata della password, allo scopo di controllare e ridurre l'utilizzo dell'account allo stretto necessario. • Controlli Mover - Consentono di rimuovere l'accesso per assicurarsi che non sia più disponibile dalla fine dell'operazione, dello spostamento o del giorno del trasferimento. • Controlli Leaver - Consentono di revocare tutti gli accessi logici utilizzati per accedere alle risorse informative di Barclays e/o per fornire servizi a Barclays dalla data di uscita o dell'ultimo giorno lavorativo del Fornitore.	

	• Autenticazione - I controlli di lunghezza e complessità delle password, frequenza di modifica delle password, autenticazione a più fattori, gestione sicura delle credenziali delle password o di altro tipo devono essere seguiti secondo le Migliori pratiche del settore • Gli account inattivi non utilizzati da almeno 60 giorni consecutivi devono essere sospesi/disabilitati (conservando le registrazioni pertinenti). • Le password di account interattivi devono essere cambiate almeno ogni 90 giorni e devono essere diverse dalle dodici (12) precedenti. • Le password degli account con privilegi devono essere cambiati dopo ogni utilizzo e almeno ogni 90 giorni. • Gli account interattivi devono essere disabilitati dopo un massimo di cinque (5) tentativi consecutivi di accesso non riusciti, o un numero di tentativi inferiore, se imposto dalle Migliori pratiche del settore. Indicazioni per il Cliente dei Servizi Cloud (Fornitore) utilizzato per la fornitura dei servizi a Barclays Il Cliente dei Servizi Cloud (CSC, Cloud Service Customer) deve garantire l'implementazione di controlli appropriati per la gestione degli accessi logici, al fine di salvaguardare il servizio Barclays. • Il Cliente del Servizio Cloud deve utilizzare tecniche di autenticazione sufficienti (ad esempio l'autenticazione a più fattori) per autenticare i propri amministratori dei servizi cloud che accedono alle funzionalità amministrative di un servizio cloud, in base ai rischi identificati. • Il Cliente del Servizio Cloud deve garantire che l'accesso alle informazioni nel servizio cloud possa essere limitato, come previsto dalla policy di controllo degli accessi, e che tali restrizioni vengano applicate. Ciò include la limitazione dell'accesso ai servizi cloud, alle funzioni dei servizi cloud e ai dati dei clienti dei servizi cloud gestiti nel servizio. • Se è consentito l'uso di programmi di utilità, il Cliente del Servizio Cloud deve identificare i programmi di utilità da utilizzare nel proprio ambiente di cloud computing e assicurarsi che non interferiscano con i controlli del servizio cloud.	
13. Gestione della vulnerabilità	Il Fornitore deve implementare un efficace programma di gestione delle vulnerabilità, tramite policy e procedure consolidate, a supporto dei processi e delle misure tecniche e organizzative, per garantire il monitoraggio efficace, il rilevamento tempestivo e la correzione delle vulnerabilità all'interno delle applicazioni gestite da, o appartenenti al, Fornitore, della	La mancata attuazione di questo controllo potrebbe comportare l'utilizzo di queste vulnerabilità dei sistemi per

<table>
<tr>
<td></td>
<td>
rete dell'infrastruttura e dei componenti di sistema, al fine di garantire l'efficacia dei controlli di sicurezza implementati.

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

Definizione dei ruoli, delle responsabilità e delle competenze per il monitoraggio, il reporting, l'escalation e la correzione.
Strumenti e infrastrutture adeguati per la scansione delle vulnerabilità.
Il Provider di servizi deve eseguire scansioni regolari delle vulnerabilità utilizzando le firme delle vulnerabilità aggiornate (con la cadenza indicata dalle Migliori pratiche del settore), per identificare efficacemente le vulnerabilità note e sconosciute in tutte le categorie di asset dell'ambiente.
Utilizzare un processo di valutazione del rischio per dare priorità al rimedio delle vulnerabilità scoperte.
Occorre assicurarsi che le vulnerabilità vengano eliminate efficacemente tramite affidabili attività di correzione e gestione delle patch, al fine di ridurre il rischio che vengano sfruttate (la correzione deve avvenire in modo tempestivo e conformemente alle Migliori pratiche del settore o al programma di gestione delle patch).
Stabilire un processo di validazione per il rimedio delle vulnerabilità che verifichi in modo rapido ed efficace tale rimedio in tutte le classi di attività nell'ambiente.
Confrontare regolarmente i risultati di scansioni consecutive delle vulnerabilità per verificare che queste ultime siano state corrette in modo tempestivo.

Per i servizi del Fornitore correlati alle infrastrutture/applicazioni di hosting per conto di Barclays (compresi i terzi ad alto rischio segnalati)

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

<table>
<tr><th>Priorità</th><th>Classificazione</th><th>Giorni di chiusura (massimo)</th></tr>
<tr><td>P1</td><td>Critica</td><td>15</td></tr>
</table>
</td>
<td>condurre attacchi informatici che possono dare luogo a danni a livello normativo e reputazionale.</td>
</tr>
</table>

	<table><tr><td>P2</td><td>Alta</td><td>30</td></tr><tr><td>P3</td><td>Media</td><td>60</td></tr><tr><td>P4</td><td>Bassa</td><td>180</td></tr><tr><td>P5</td><td>A titolo informativo</td><td>360</td></tr></table> Tutti i problemi di sicurezza e le vulnerabilità che potrebbero produrre gravi conseguenze sulle applicazioni o l'infrastruttura di hosting di Barclays fornita dal Fornitore, e di cui il Fornitore ha deciso di accettare il rischio, devono essere tempestivamente comunicati o segnalati a Barclays e concordati per iscritto con Barclays (Chief Security Office - Team ECAM externalcyberassurance@barclayscorp.com). **Indicazioni per il Cliente dei Servizi Cloud (Fornitore) utilizzato per la fornitura dei servizi a Barclays** Il Cliente dei Servizi Cloud (CSC, Cloud Service Customer) deve garantire l'implementazione di controlli appropriati sulla Gestione delle vulnerabilità, al fine di salvaguardare il servizio Barclays. • Il Cliente del Servizio Cloud deve richiedere al provider di servizi cloud informazioni sulla gestione delle vulnerabilità tecniche che possono influire sui servizi cloud forniti. Il Cliente del Servizio Cloud deve identificare le vulnerabilità tecniche di cui sarà responsabile e definire chiaramente un processo di gestione.	
14. Gestione degli aggiornamenti	Il Fornitore deve implementare un programma di Gestione delle patch supportato da policy e procedure consolidate, processi aziendali/misure organizzative e misure tecniche, al fine di monitorare/tracciare le patch necessarie e distribuire le patch di sicurezza in modo da gestire l'intero ambiente/infrastruttura del Fornitore. Il Fornitore deve garantire che i server, i dispositivi di rete, le applicazioni e i dispositivi endpoint siano aggiornati con le patch di sicurezza più recenti e conformemente alle migliori Pratiche del settore, garantendo che: • Il Fornitore valuta e verifica tutte le patch su sistemi che riproducono accuratamente la configurazione dei sistemi di produzione target prima di implementarle in tali	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.

<table>
<tr>
<td></td>
<td>sistemi, verificando la corretta applicazione delle patch dopo ogni ciclo di correzione. Se in un sistema non può essere installata una patch, adottare le contromisure appropriate.
• Tutte le modifiche fondamentali all'ambiente IT devono essere registrate, verificate e approvate prima di essere implementate tramite un'affidabile procedura di gestione delle modifiche approvata, al fine di rispondere alle eventuali esigenze di audit, indagine, risoluzione dei problemi e analisi future.
• Il Fornitore deve verificare l'applicazione delle patch negli ambienti di produzione e di disaster recovery (DR).</td>
<td></td>
</tr>
<tr>
<td>15. Simulazione di minaccia/ Test di penetrazione/ Valutazione della sicurezza IT</td>
<td>Il Fornitore deve coinvolgere un provider indipendente di servizi di sicurezza specializzato per eseguire una valutazione della sicurezza IT o una simulazione delle minacce alle infrastrutture IT, compreso il disaster recovery, e alle applicazioni web correlate ai servizi che eroga a Barclays.

Questa procedura deve essere eseguita almeno una volta l'anno, al fine di identificare le vulnerabilità sfruttabili per violare la sicurezza informatica dei dati di Barclays. Tutte le vulnerabilità devono ottenere la massima priorità e devono essere tracciate fino alla risoluzione. Il test deve essere eseguito conformemente alle Migliori pratiche del settore.

Per i servizi del Fornitore correlati alle infrastrutture/applicazioni di hosting per conto di Barclays (compresi i terzi ad alto rischio segnalati)

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

<table><tr><th>Priorità</th><th>Classificazione</th><th>Giorni di chiusura (massimo)</th></tr></table></td>
<td>Se questo controllo non viene implementato, il Fornitore potrebbero non essere in grado di valutare le minacce informatiche a cui è soggetto, né l'idoneità e la solidità delle proprie difese.

Le informazioni di Barclays possono essere divulgate e/o può verificarsi una perdita del servizio che può dare luogo a danni a livello normativo o reputazionale.</td>
</tr>
</table>

<table>
<tr><td></td><td></td><td><table>
<tr><td>P1</td><td>Critica</td><td>15</td></tr>
<tr><td>P2</td><td>Alta</td><td>30</td></tr>
<tr><td>P3</td><td>Media</td><td>60</td></tr>
<tr><td>P4</td><td>Bassa</td><td>180</td></tr>
<tr><td>P5</td><td>A titolo informativo</td><td>360</td></tr>
</table></td><td></td><td></td></tr>
<tr><td>16. Crittografia</td><td colspan="3">
Motivazione della crittografia - Il Fornitore deve documentare la motivazione per l'utilizzo della tecnologia crittografica ed esaminarla per assicurarsi che sia ancora adatta allo scopo.
Procedure del ciclo di vita della crittografia - Il Fornitore deve porre in essere e mantenere una serie documentata di procedure di gestione del ciclo di vita della crittografia che descrivano in dettaglio i processi end-to-end per la gestione delle chiavi dalla generazione, al caricamento, alla distribuzione fino alla distruzione. Il Fornitore deve ritirare le proprie chiavi al termine del periodo di servizio o impostare un programma di rotazione chiavi obbligatorio.
Approvazione delle operazioni manuali - Il Fornitore deve garantire che tutti gli eventi gestiti dall'uomo per le chiavi e i certificati digitali, compresa la registrazione e la generazione di nuove chiavi e certificati, siano approvati ad un livello appropriato e che sia conservata una registrazione dell'approvazione.
Certificati digitali - Il Fornitore deve garantire che tutti i certificati siano ottenuti da una serie di Autorità di Certificazione (CA) approvate e controllate che dispongono di servizi di revoca e di politiche di gestione dei certificati e deve accertarsi che i certificati autofirmati siano utilizzati solo se tecnicamente non esiste la possibilità di supportare una soluzione basata su CA e deve disporre di controlli manuali per garantire l'integrità, l'autenticità delle chiavi e il raggiungimento tempestivo della revoca e del rinnovo.
Generazione di chiavi e criptoperiodo - Il Fornitore deve garantire che tutte le chiavi siano generate in modo casuale da un hardware certificato o da un CSPRNG (Cryptographically Secure Pseudo Random Number Generator - Generatore di numeri pseudo casuali crittograficamente sicuro) presente nel software.

Il Fornitore deve garantire che tutte le chiavi siano soggette ad un criptoperiodo di tempo limitato e definito per la loro sostituzione o disattivazione. Ciò deve

</td><td>Una protezione e algoritmi criptati aggiornati e adeguati garantiscono la protezione costante dei Patrimoni di dati di Barclays.</td></tr>
</table>

	essere in linea anche con le procedure NIST (National Institute of Standards and Technology) e con le Migliori pratiche del settore. • Protezione della conservazione delle chiavi - Il Fornitore deve garantire che le chiavi crittografiche segrete/private esistano solo nelle seguenti forme: o nel confine crittografico di un dispositivo/modulo hardware di sicurezza certificato. o In forma criptata sotto un'altra chiave stabilita o derivata da una password. o In componenti separati suddivisi tra gruppi di custodi distinti. o Cancellare nella memoria dell'host per il periodo dell'operazione di crittografia, a meno che non sia richiesta la protezione HSM. • Il Fornitore deve garantire che le chiavi siano generate e conservate entro i confini della memoria degli HSM per le chiavi ad alto rischio. Sono compresi: o Chiavi per i servizi regolamentati in cui la protezione HSM è obbligatoria. o Certificati che rappresentano Barclays da parte delle CA. o Certificati Root, Issuing, OCSP e RA (autorità di registrazione) utilizzati per l'emissione di Certificati a protezione dei servizi Barclays. o Chiavi che proteggono i repository aggregati memorizzati di chiavi, credenziali di autenticazione o dati PII. • Backup e conservazione delle chiavi - Il Fornitore mantiene un backup di tutte le chiavi per evitare l'interruzione del servizio nel caso in cui le chiavi si danneggino o richiedano il ripristino. L'accesso ai back-up è limitato a postazioni sicure che applicano il principio di 'split knowledge' e il doppio controllo. I backup delle chiavi devono avere una protezione crittografica almeno pari a quella delle chiavi in uso. • Inventario - Il Fornitore mantiene un inventario completo e aggiornato dell'uso della crittografia nei servizi che fornisce a Barclays, che descrive in dettaglio tutte le chiavi crittografiche, i certificati digitali e il software e l'hardware di crittografia gestiti dal Fornitore per prevenire danni in caso di incidente. Per dimostrare ciò, l'inventario revisionato viene firmato almeno ogni trimestre e fornito a Barclays. Gli inventari devono comprendere, se del caso: o Il Team di supporto IT o Le attività collegate o Algoritmi, lunghezza delle chiavi, ambiente, gerarchia delle chiavi, autorità di certificazione, impronte digitali, protezione dell'archiviazione delle chiavi e scopo tecnico e operativo. • Scopo funzionale e operativo - Le chiavi devono avere un unico scopo funzionale e operativo e non devono essere condivise tra più servizi o al di fuori dei servizi Barclays.	

	• Processo di verifica - Il Fornitore deve eseguire e conservare la prova della revisione dei registri verificabili ogni trimestre almeno per tutti gli eventi di gestione del ciclo di vita delle chiavi e dei certificati che dimostrino una catena di custodia completa per tutte le chiavi, compresa la generazione, la distribuzione, il carico e la distruzione per rilevare qualsiasi uso non autorizzato. • Hardware - Il Fornitore conserva i dispositivi hardware in aree sicure e mantiene un processo di verifica per tutto il ciclo di vita della chiave per garantire che la catena di custodia dei dispositivi crittografici non sia compromessa. Questo processo viene rivisto su base trimestrale. o Il Fornitore deve garantire che l'hardware crittografico sia certificato almeno per il livello 2 di FIPS140-2 e che raggiunga il livello 3 nella Sicurezza Fisica e Gestione delle chiavi crittografiche o PCI HSM. Il Fornitore può scegliere di consentire l'utilizzo di smartcard basate su chip o di e-Token certificati FIPS come hardware accettabile per la memorizzazione di chiavi che rappresentano e sono detenute da singole persone o clienti quando si trovano fuori sede. • Chiave compromessa - Il Fornitore mantiene e monitora un piano per le chiavi compromesse per garantire che le chiavi di ricambio siano generate indipendentemente dalla chiave compromessa per evitare che quest'ultima fornisca informazioni sulla sua sostituzione. Se si verifica un incidente di compromesso, Barclays deve essere notificato al **Barclays Chief Security Office (CSO) Joint Operations Centre (JOC) - gcsojoc@barclays.com.** • Affidabilità degli algoritmi e delle chiavi - Il Fornitore garantisce che gli algoritmi e la lunghezza delle chiavi in uso sono conformi ai requisiti NIST (National Institute of Standards and Technology) e alle Migliori pratiche del settore.	
17. Cloud Computing	Il Fornitore, o Cliente dei Servizi Cloud (CSC, Cloud Service Customer), deve garantire che il servizio cloud utilizzato per i servizi Barclays utilizza un framework di controlli di sicurezza ben definito al fine di raggiungere gli obiettivi di riservatezza, integrità e disponibilità, oltre che di garantire che i controlli di sicurezza siano in atto e funzionino efficacemente per proteggere i servizi Barclays. Per garantire la sicurezza di tutta la tecnologia cloud utilizzata, il Fornitore deve disporre della certificazione ISO/IEC 27017, 27001 o SOC 2, oppure utilizzare le Migliori pratiche del settore o un framework di sicurezza simile per il cloud, al fine di garantire l'implementazione di misure di sicurezza consolidate. Occorre assicurarsi che il provider di servizi cloud sia certificato in base alle Migliori pratiche del settore, compresi i controlli appropriati equivalenti all'ultima versione della Cloud Controls Matrix (CCM) della Cloud Security Alliance.	La mancata implementazione di questo controllo cloud potrebbe compromettere i Dati Barclays e tale condizione può dare luogo a danni a livello normativo o reputazionale.

	Il Fornitore deve richiedere una prova documentata che l'implementazione dei controlli e delle linee guida per la sicurezza delle informazioni per il servizio cloud sia in linea con qualsiasi dichiarazione rilasciata dal provider di servizi cloud. Il Fornitore è responsabile di garantire i controlli di sicurezza dei dati correlati agli Asset di informazioni e ai Dati di Barclays, compresi i Dati personali all'interno del cloud, mentre il CSP del provider di servizi cloud è responsabile della sicurezza dell'ambiente di cloud computing. Il Fornitore rimane responsabile della configurazione e del monitoraggio dell'implementazione dei controlli di sicurezza per una protezione attiva da qualsiasi incidente di sicurezza, comprese le violazioni dei dati. Il Fornitore deve implementare misure di sicurezza in tutti gli aspetti del servizio fornito, compreso il modello di responsabilità condivisa del cloud, in modo tale da salvaguardare la riservatezza, l'integrità, la disponibilità e l'accessibilità, riducendo al minimo la possibilità che persone non autorizzate abbiano accesso alle informazioni di Barclays e ai servizi utilizzati da Barclays. I controlli di sicurezza in cloud devono coprire, a titolo esemplificativo ma non esaustivo, i seguenti domini per i modelli di distribuzione (IaaS/PaaS/SaaS): • Meccanismi di governance e responsabilità • Gestione delle identità e degli accessi • Sicurezza della rete (compresa la connettività) • Sicurezza dei dati (Transito/Sosta/Archiviazione) • Eliminazione/cancellazione sicura dei dati • Crittografia, criptazione e gestione delle chiavi - CEK • Registrazione e monitoraggio • Virtualizzazione • Separazione dei servizi Gli asset informativi e i Dati di Barclays, compresi i Dati personali memorizzati nel cloud come parte del servizio reso a Barclays, devono essere approvati da Barclays (Chief Security Office - Team ECAM). Il Fornitore deve indicare a Barclays le sedi delle zone dati e le zone dati di failover in cui verranno archiviati o conservati i suoi dati. Il Fornitore deve confermare i ruoli di sicurezza delle informazioni e le responsabilità correlate al servizio cloud, come indicato nel contratto di servizio, che possono includere i seguenti processi: • Protezione dal malware • Backup	

	• Controlli crittografici • Gestione della vulnerabilità • Gestione degli incidenti • Test di sicurezza • Audit • Raccolta, gestione e protezione delle prove, inclusi registri e tracce di audit • Protezione delle informazioni alla scadenza del contratto di servizio • Gestione di identità e accessi	
18. Spazio dedicato alla banca (Bank Dedicated Space - BDS)	Per i servizi forniti che richiedono uno Spazio Bancario Dedicato (Bank Dedicated Space - BDS) ufficiale, devono essere attivati requisiti fisici e tecnici BDS specifici. (Se BDS è un requisito per il servizio, saranno applicabili i requisiti di controllo.) I diversi tipi di BDS sono: Livello 1 (Prima classe) - L'intera infrastruttura IT è gestita da **Barclays** attraverso la fornitura di una LAN, WAN & Desktop gestita da **Barclays** ad un sito Fornitore con uno spazio dedicato Barclays. Livello 2 (Classe Business) - L'intera infrastruttura IT viene gestita dal **Fornitore** e si connette ai gateway Extranet di **Barclays** (i dispositivi LAN, WAN e Desktop appartengono al, e sono gestiti dal, Fornitore). Livello 3 (Classe Economica) - L'intera infrastruttura IT viene gestita dal **Fornitore** e si connette ai gateway Internet di **Barclays** (i dispositivi LAN, WAN e Desktop appartengono al, e sono gestiti dal, Fornitore).	La mancata implementazione di questo controllo impedisce di attivare gli adeguati controlli fisici e tecnici provocando ritardi o interruzione dell'erogazione del servizio o violazioni della sicurezza informatica / incidenti di sicurezza.
18.1 BDS - Separazione fisica	L'area fisica occupata deve essere dedicata a Barclays e non condivisa con altre società / altri venditori. Deve essere logicamente e fisicamente separata.	
18.2 BDS - Controllo dell'accesso fisico	• Il Fornitore deve porre in essere un processo di accesso fisico che copra i metodi di accesso e l'autorizzazione al BDS nel luogo in cui vengono erogati i servizi. • L'ingresso alle e l'uscita verso le aree BDS devono essere regolamentati e monitorati da meccanismi di controllo dell'accesso fisico, per garantire che l'accesso sia consentito solo ai dipendenti autorizzati. • Una carta d'accesso elettronica autorizzata per accedere alle aree BDS degli uffici. • Il Fornitore deve effettuare controlli trimestrali per garantire che solo le persone autorizzate abbiano accesso alle aree BDS. Le eccezioni vengono studiate a fondo fino alla risoluzione.	

	• I diritti di accesso vengono rimossi entro 24 ore per tutti i dipendenti che cambiano sede, si dimettono o si rendono irreperibili (conservando le registrazioni pertinenti). • Utilizzare i guardiani per pattugliare abitualmente l'interno delle aree BDS per identificare efficacemente gli accessi non autorizzati o le attività potenzialmente dannose. • Per l'accesso a BDS devono essere svolti controlli automatici di sicurezza, tra cui: Per i dipendente autorizzati: o Tesserino identificativo con foto sempre visibile o Sono utilizzati lettori ottici di card o I dispositivi anti-pass back devono essere attivi e monitorati • Il Fornitore deve disporre di processi e procedure per il controllo e il monitoraggio delle persone esterne, inclusi i subappaltatori e i subresponsabili che accedono fisicamente alle aree BDS per le attività di manutenzione e pulizia.
18.3 BDS - Videosorveglianza	• Occorre implementare la videosorveglianza per le aree BDS allo scopo di individuare efficacemente gli accessi non autorizzati o le attività dannose, in modo da semplificare le indagini. • Tutti i punti di entrata e uscita dell'area BDS devono essere videosorvegliati. • Le telecamere di sicurezza sono posizionate in modo appropriato e forniscono immagini chiare e identificabili in ogni momento per catturare attività dannose e contribuire alle indagini. Il Fornitore deve conservare le riprese TVCC catturate per 30 giorni e tutte le registrazioni TVCC e i registratori devono essere posizionati in modo sicuro per evitare la modifica, la cancellazione o la visione "casuale" di eventuali schermi TVCC associati e l'accesso alle registrazioni deve essere controllato e limitato solo alle persone autorizzate.
18.4 BDS - Accesso alla rete Barclays e ai token di autenticazione Barclays	• Ciascun utente che vuole autenticarsi sulla rete Barclays dall'area BDS, può utilizzare esclusivamente un dispositivo di autenticazione a più fattori fornito da Barclays. • Il Fornitore deve conservare i registri delle persone a cui sono stati forniti i token di autenticazione Barclays e deve eseguire una riconciliazione su base trimestrale. • Barclays disattiverà entro ventiquattro (24) ore le credenziali di autenticazione non appena sarà notificato che l'accesso non è più necessario (ad es. licenziamento di un dipendente, riassegnazione di un progetto, ecc.). • Barclays disattiverà prontamente le credenziali di autenticazione nel caso in cui tali credenziali non siano state utilizzate per un periodo di tempo (tale periodo di non utilizzo non deve superare un mese). • I servizi che hanno accesso alla stampa remota tramite l'applicazione Barclays Citrix devono essere approvati e autorizzati da Barclays (Chief Security Office - ECAM Team). Il Fornitore deve mantenere i registri ed eseguire la riconciliazione trimestrale. Fare riferimento al Controllo 4. Lavoro a distanza (accesso remoto)

18.5 BDS - Supporto dei dipendenti in trasferta	L'accesso remoto all'area BDS non è fornito di default per il supporto di out of office/out of business/work from home. Qualsiasi Accesso Remoto deve essere approvato dalle funzioni di Barclays pertinenti (compreso il Chief Security Office – ECAM team)
18.6 BDS - Sicurezza della rete	• Mantenere un inventario aggiornato di tutti i perimetri della rete dell'organizzazione (attraverso un'Architettura di Rete/Diagramma). • La progettazione e l'implementazione della rete deve essere rivista almeno una volta all'anno. • La rete BDS deve essere separata in modo logico dalla rete aziendale del Fornitore, tramite un Firewall, e tutto il traffico in entrata e in uscita deve essere monitorato e soggetto a restrizioni. • La configurazione del percorso deve garantire solo le connessioni alla rete Barclays e non deve condurre ad altre reti del Fornitore. • Il router Supplier Edge che si collega ai gateway extranet di Barclays deve essere configurato in modo sicuro con un concetto di limitazione dei controlli di porte, protocolli e servizi; o Assicurarsi che la registrazione e il monitoraggio siano abilitati. • La rete BDS deve essere monitorata e consentita esclusivamente ai dispositivi autorizzati, tramite adeguati controlli di accesso alla rete Fare riferimento al Controllo 2. Sicurezza del perimetro e della rete
18.7 BDS - Rete wireless	Disattivare la rete wireless per il provisioning della rete BDS per i servizi Barclays.
18.8 BDS - Sicurezza degli endpoint	La struttura desktop dei computer all'interno della rete BDS deve essere configurata in modo sicuro e conformemente alle Migliori pratiche del settore. Devono essere applicate le Migliori pratiche del settore e la struttura di sicurezza dei dispositivi endpoint deve includere, a titolo di esempio non esaustivo: • Crittografia completa del disco rigido. • disattivare tutti i software/servizi/porte non necessari; • disattivare l'accesso ai diritti di amministrazione per l'utente locale • I dipendenti del Fornitore non possono modificare le impostazioni di base come il Service Pack predefinito, i servizi predefiniti e così via. • Occorre disattivare la funzione per la copia di informazioni/dati di Barclays su supporti USB esterni. • Occorre aggiornare i dispositivi con le ultime firme anti-malware e patch di sicurezza. • prevenzione della perdita di dati limitata al divieto di taglia-copia-incolla e stampa-schermo o stampa schermo dei dati Barclays;

	• Occorre disattivare l'accesso alla stampante per impostazione predefinita • la condivisione / il trasferimento del Patrimonio informatico / dei Dati di Barclays durante l'utilizzo di strumenti/software di messaggistica istantanea devono essere disabilitati; • Occorre arrestare, eliminare e rilevare la presenza e/o l'uso di software non autorizzato, incluso il software dannoso. Fare riferimento al Controllo 8. Sicurezza dell'endpoint	

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

18.10 BDS - BYOD/Dispositivi personali	I dispositivi personali/BYOD non devono essere autorizzati ad accedere all'ambiente Barclays e/o ai dati Barclays	
Diritto di ispezione	Il Fornitore deve consentire a Barclays, su preavviso scritto di Barclays con almeno dieci (10) giorni lavorativi di anticipo, di verificare la sicurezza di qualsiasi luogo o tecnologia utilizzati dal Fornitore o dai Subappaltatori per sviluppare, testare, migliorare, eseguire la manutenzione o gestire i sistemi del Fornitore che vengono utilizzati per i Servizi, al fine di verificare il rispetto degli obblighi da parte del Fornitore. Il Fornitore deve inoltre consentire a Barclays di svolgere un'ispezione almeno una volta l'anno, o subito dopo un incidente di sicurezza. Eventuali non-conformità individuate da Barclays durante un'ispezione devono essere sottoposte a valutazione dei rischi da parte di Barclays, che specificherà una tempistica per la relativa correzione. Il Fornitore è quindi tenuto a completare eventuali interventi correttivi entro tale periodo. Il Fornitore deve fornire tutta l'assistenza ragionevolmente richiesta da Barclays in relazione alle ispezioni effettuate e la documentazione presentata durante l'ispezione deve essere completata e restituita a Barclays.	In mancanza di un accordo, il Fornitore non sarà in grado di garantire il pieno rispetto di tali obblighi di sicurezza.

Appendice A: Glossario

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

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

	NOTA - Una macchina virtuale incapsula completamente l'hardware virtuale, i dischi virtuali e i metadati associati. Le macchine virtuali consentono il multiplexing del sistema fisico sottostante attraverso un livello software denominato hypervisor.

Segreto bancario

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

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

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

Appendice B: Glossario

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

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

Appendice C: DEFINIZIONE DI DATI IDENTIFICATIVI DEL CLIENTE

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

I CID Indiretti (ICID) sono suddivisi in 3 livelli

- L1 ICID possono essere definiti come identificatori unici (di proprietà della Banca) che permettono di identificare in modo univoco un cliente nel caso in cui sia disposto l'accesso alle applicazioni bancarie o ad altre applicazioni di terze parti. L'identificatore deve essere inequivocabile, non soggetto a interpretazioni e può includere identificatori come numero di conto, codice IBAN, numero di carta di credito, ecc.
- L2 ICID possono essere definite come informazioni (di proprietà del cliente) che, unitamente ad altre, forniscono conclusioni sull'identità di un cliente. Mentre queste informazioni non possono essere utilizzate per identificare un cliente di per sé, possono essere usate insieme ad altre informazioni per identificare un cliente. L2 ICID devono essere protetti e gestiti con la stessa diligenza utilizzata per i 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 acquisito o potenziale	Numero contenitore / ID contenitore	Luogo di nascita	Qualsiasi identificatore strettamente interno dell'applicazione di hosting/elaborazione del CID
	Nome della società	Numero MACC (conto liquidità soggetto a ID Contenitore Avaloq)	Data di nascita	Identificatore dinamico
	Estratto conto	ID SDS	Nazionalità	ID Party Role CRM
	Firma	IBAN	Titolo	ID contenitore esterno
	ID social network	Dettagli di registrazione eBanking	Situazione familiare	
	Numero passaporto	Numero cassetta di sicurezza	Codice postale	
	Numero telefonico	Numero carta di credito	Condizioni di salute	
	Indirizzo e-mail	Messaggio SWIFT	Maggior valore di posizione/transazione	
	Qualifica lavorativa o PEP (Persona esposta politicamente)	ID Business Partner interno	Ultima visita cliente	
	Pseudonimo		Lingua	
	Indirizzo IP		Sesso	
	Numero fax		Data di scadenza CC	
			Contatto principale	
			Luogo di nascita	
			Data di apertura del conto	

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

1. Nome del cliente

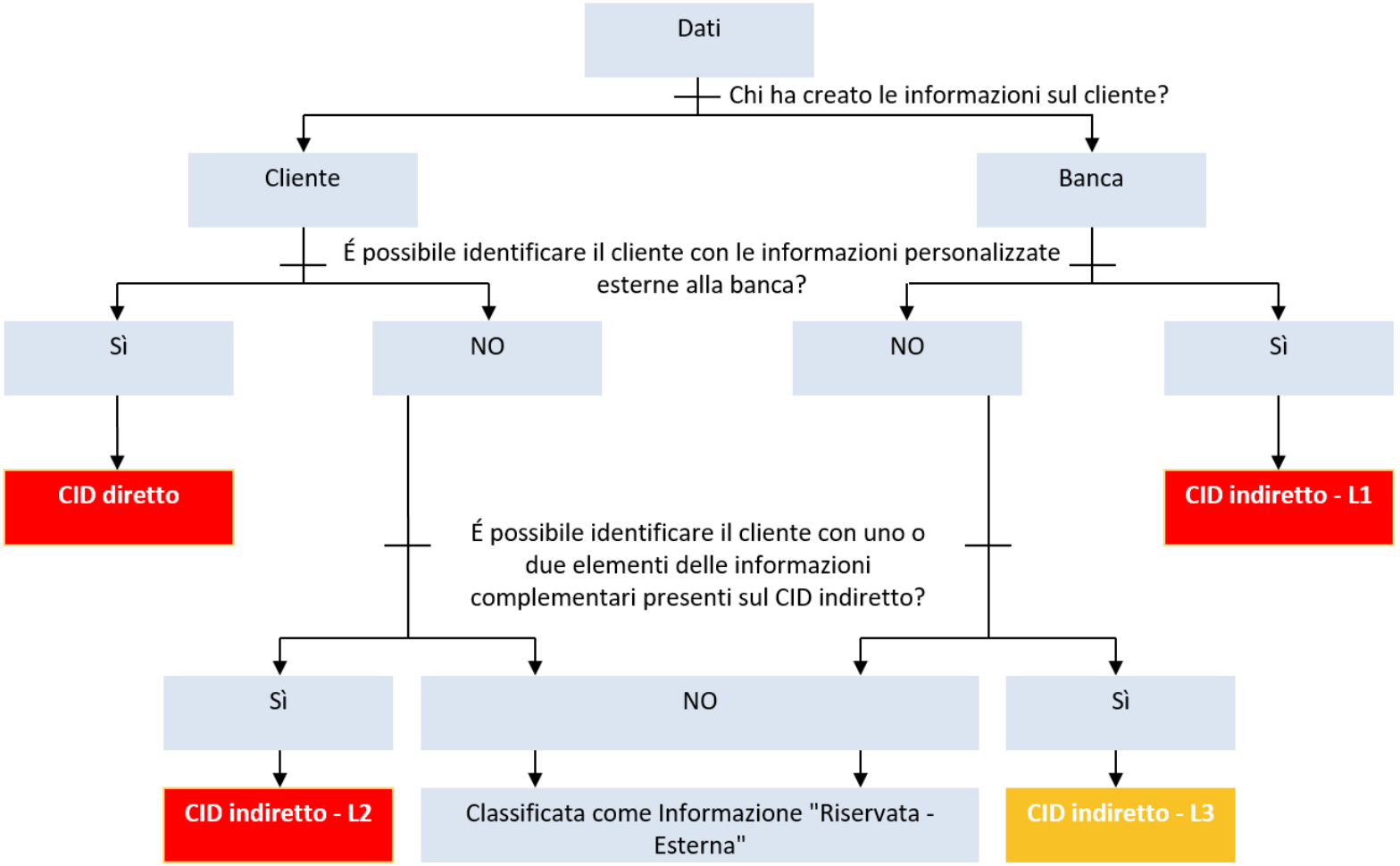
   (DCID) = Violazione del segreto bancario

2. ID contenitore

   (L1 ICID) = Violazione del segreto bancario

3. Condizioni di salute + Nazionalità

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



Appendice D: Schema di Etichettatura delle informazioni di Barclays

Tabella D1: Schema di Etichettatura delle informazioni di Barclays

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

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

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

	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.	• 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. • Retribuzione e informazioni personali dei dipendenti • Valutazioni di vulnerabilità. • Risultati di audit e rapporti.
Riservata – Esterna	Le informazioni devono essere classificate come Riservata - Esterna se i destinatari previsti sono dipendenti Barclays autenticati e MSP in possesso di un contratto attivo che riguarda un target specifico o parti esterne autorizzate dal titolare delle informazioni. La divulgazione non autorizzata potrebbe avere un impatto negativo su Barclays, valutato nell'ambito dell'ERMF come "Principale" o "Limitato" (a livello finanziario o non finanziario).	• Nuovi piani di prodotto. • Contratti con i clienti. • Contratti legali. • Informazioni relative a clienti singoli/a basso volume da inviare all'esterno. • Comunicazioni relative ai clienti. • Nuovi materiali per offerte (ad es. prospetti, promemoria per offerte). • Documenti di ricerca definitivi.

	Queste informazioni non sono destinate alla diffusione generale ma possono essere inoltrate o condivise dai destinatari secondo il principio need-to-know.	• Informazioni essenziali non pubbliche (Material Non-Public Information - MNPI) esterne a Barclays. • Tutti i report di ricerca • Alcuni materiali di marketing. • Commenti del mercato.
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 D2: Schema di Etichettatura delle informazioni - Requisiti di gestione

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

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

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

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

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

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

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

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