

Obblighi di controllo dei Fornitori esterni

Sicurezza Informatica e Cibernetica (ICS)

Area di controllo / Titolo	Descrizione del controllo	Perché è importante?
1. Quadro di Governance per la Sicurezza Informatica / Cibernetica	<p>Il Fornitore deve disporre di uno schema di sicurezza standard di settore stabilito e coerente per la governance della Sicurezza Informatica e Cibernetica, al fine di garantire la comprensione del proprio personale, dei processi, dell'ambiente tecnologico e dello stato dei controlli di sicurezza Informatica/Cibernetica, nonché di un programma di sicurezza per proteggere il Fornitore dalle minacce Cibernetiche in conformità con le Principali Prassi del Settore (tra cui NIST, ISO/IEC 27001) o con i requisiti di settore applicabili.</p> <p>Il Quadro di Governance per la Sicurezza deve essere sviluppato, documentato, approvato e implementato, utilizzando misure di sicurezza amministrative, tecniche e fisiche per proteggere i beni e i dati da perdita, uso improprio, accesso non autorizzato, divulgazione, alterazione e distruzione.</p> <p>Il programma di sicurezza deve includere, a titolo esemplificativo, le seguenti aree:</p> <ul style="list-style-type: none"> • Politica, procedure e programma standard per la Sicurezza Informatica e Cibernetica finalizzati alla reale creazione, implementazione e costante misurazione dell'efficacia della politica per la Sicurezza Informatica e Cibernetica e dell'applicazione dei relativi standard. • Un programma di sicurezza completo con una chiara struttura di leadership e una supervisione esecutiva per creare una cultura di responsabilità e consapevolezza per la sicurezza. • Politiche e procedure appropriate in materia di Sicurezza Informatica e Cibernetica che vengono approvate e comunicate in tutta l'organizzazione. • Accertarsi che le politiche e le procedure/gli standard in materia di Sicurezza Informatica e Cibernetica siano rivisti regolarmente (almeno una volta all'anno o in caso di modifiche sostanziali). 	<p>In caso di mancata attuazione di questo principio, Barclays o i propri Fornitori potrebbero non avere e non essere in grado di dimostrare di disporre di una supervisione adeguata in materia di sicurezza Informatica/Cibernetica. Un solido quadro di governance della sicurezza definisce il livello di sicurezza per l'intera organizzazione.</p>

	<ul style="list-style-type: none"> • Il Fornitore deve garantire l'assegnazione della responsabilità individuale per le informazioni e i sistemi, assicurando che esista un'adeguata proprietà degli ambienti aziendali, delle informazioni e dei sistemi critici e che questa sia assegnata a persone capaci. • Il Fornitore coordina e allinea ruoli e responsabilità per il personale, implementando, gestendo e supervisionando l'efficacia della strategia e dello schema di sicurezza con partner interni ed esterni. • Revisioni e valutazioni indipendenti devono essere eseguite almeno una volta all'anno per garantire che l'organizzazione affronti le non conformità delle politiche, degli standard, delle procedure e degli obblighi di conformità stabiliti. <p>Nel caso in cui il Fornitore sia soggetto a fusione, acquisizione o qualsiasi altro cambiamento di proprietà, il Fornitore si impegna a informare Barclays (per iscritto) non appena sia legalmente in grado di farlo.</p>	
<p>2. Gestione dei rischi di sicurezza cibernetica/informatica</p>	<p>Il Fornitore deve stabilire un programma di gestione dei rischi di sicurezza che valuti, attenni e monitori efficacemente i rischi per la sicurezza in tutto l'ambiente controllato dal fornitore.</p> <p>Il programma di gestione dei rischi deve includere, a titolo esemplificativo, le seguenti aree:</p> <ul style="list-style-type: none"> • Il Fornitore deve disporre di un quadro di gestione dei rischi per la Sicurezza Informatica e Cibernetica approvato dall'autorità governativa competente (ad esempio, il Consiglio di amministrazione o uno dei suoi comitati). Il piano di gestione deve essere integrato nella strategia aziendale complessiva e nel quadro di gestione dei rischi. • Allineate al quadro dei rischi, le valutazioni formali dei rischi devono essere eseguite almeno una volta all'anno o a intervalli pianificati, o essere attivate in base agli eventi, ad esempio in risposta a un incidente o alle lezioni apprese ad esso associate (e in combinazione con eventuali modifiche ai sistemi informativi) 	<p>Le procedure e gli standard documentati sono elementi essenziali per la gestione del rischio e la governance. Essi stabiliscono la visibilità sulla gestione dei controlli necessari per gestire il rischio informatico/cibernetico.</p> <p>La mancata implementazione di questo principio potrebbe comportare la divulgazione non idonea dei dati di Barclays e/o potrebbe verificarsi una perdita del servizio che può dare luogo a</p>

	<p>per determinare la probabilità e l'impatto di tutti i rischi identificati utilizzando metodi qualitativi e quantitativi. La probabilità e l'impatto associati al rischio intrinseco e residuo sono determinati in modo indipendente, considerando tutte le categorie di rischio (ad esempio, risultati di audit, analisi delle minacce e delle vulnerabilità e conformità normativa).</p> <ul style="list-style-type: none">• I risultati della valutazione del rischio devono includere aggiornamenti delle politiche, delle procedure, degli standard e dei controlli di sicurezza per garantire che rimangano pertinenti ed efficaci e, se del caso, che siano allineati alle migliori pratiche del settore.• Selezionare le opzioni appropriate per il trattamento dei rischi legati alla sicurezza delle informazioni, tenendo conto dei risultati della valutazione del rischio.• Formulare un piano di trattamento dei rischi legati alla sicurezza delle informazioni e i criteri di accettazione del rischio attraverso persone adeguatamente qualificate e responsabili.• Il Fornitore deve garantire che i rischi identificati nell'ambiente siano minimizzati o eliminati attraverso l'assegnazione delle priorità di rischio e l'implementazione di contromisure.• I rischi dovrebbero essere mitigati a un livello accettabile. I livelli di accettazione basati su criteri di rischio devono essere stabiliti e documentati in base a tempi di risoluzione ragionevoli e all'approvazione delle parti interessate.• Le valutazioni del rischio associate ai requisiti di governance dei dati devono tenere conto di quanto segue:<ul style="list-style-type: none">○ Classificazione e protezione dei dati da uso non autorizzato, accesso, perdita, distruzione e falsificazione.○ Consapevolezza dell'ambiente in cui i dati sensibili vengono memorizzati e trasmessi attraverso applicazioni, database, server e infrastrutture di rete.	<p>provvedimenti legali o normativi o generare danni alla reputazione.</p>
--	--	--

	<ul style="list-style-type: none"> ○ Rispetto dei periodi di conservazione definiti e dei requisiti di smaltimento a fine vita. • Il fornitore deve effettuare almeno una valutazione annuale dei rischi per la sicurezza in relazione alla sicurezza Informatica/Cibernetica e, sulla base degli ambienti specifici, prendere in considerazione una cadenza più frequente. <p>Se il Fornitore non è in grado di rimediare o ridurre le aree di rischio materiali che potrebbero avere un impatto sul servizio fornito a Barclays, deve darne comunicazione a Barclays.</p>	
<p>3. Uso approvato</p>	<p>Il Fornitore è tenuto a redigere e divulgare i Requisiti di uso accettabile, informando i propri dipendenti delle loro responsabilità.</p> <p>È necessario considerare i seguenti aspetti:</p> <ul style="list-style-type: none"> • 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 del Patrimonio di dati di Barclays; e • Elaborazione dei canali di perdita dati <p>Il Fornitore deve adottare misure adeguate atte ad assicurare la conformità ai requisiti di uso accettabile.</p>	<p>I requisiti di uso accettabile aiutano a rafforzare l'ambiente di controllo per la protezione dei Patrimoni di Dati</p>

<p>4. Formazione e consapevolezza</p>	<p>Il Fornitore deve aver istituito un programma di formazione per la sensibilizzazione in materia di sicurezza per tutti i dipendenti, gli appaltatori e gli utenti terzi dei sistemi dell'organizzazione e renderlo obbligatorio, se del caso. Tutti i soggetti che hanno accesso a dati/informazioni Barclays devono ricevere un'adeguata formazione di sensibilizzazione e aggiornamenti periodici sulle procedure organizzative, i processi e le politiche relativi alla loro funzione professionale nell'ambito dell'organizzazione. I livelli di formazione e sensibilizzazione devono essere commisurati ai ruoli svolti e registrati su una piattaforma di gestione dell'apprendimento idonea.</p> <p>Il Fornitore deve garantire che, entro un mese dall'ingresso nell'organizzazione, tutto il personale sotto il proprio controllo intraprenda una formazione obbligatoria sulle informazioni di sicurezza che includa le migliori pratiche di Cyber Security e di protezione dei dati di Barclays, e che tale formazione sia aggiornata almeno una volta all'anno. Ove opportuno, la formazione deve comprendere quanto segue:</p> <p>I gruppi ad alto rischio, come quelli con accesso privilegiato al sistema o che svolgono funzioni aziendali sensibili (compresi gli utenti privilegiati, i dirigenti, il personale addetto alla Sicurezza Informatica e Cibernetica e i terzi interessati), devono ricevere una formazione per la consapevolezza delle situazioni in materia di Sicurezza Informatica e Cibernetica in base ai loro ruoli e alle loro responsabilità.</p>	<p>Formazione e consapevolezza supportano tutti gli altri controlli nell'ambito di questo programma.</p> <p>In caso di mancata attuazione di questo principio, i dipendenti interessati non saranno consapevoli dei rischi cibernetici e dei vettori di attacco e non saranno in grado di rilevare o prevenire gli attacchi.</p>
<p>5. Gestione degli incidenti di sicurezza</p>	<p>Il Fornitore deve stabilire un quadro di gestione degli incidenti di Cyber Security che convalidi, contenga e rimuova/attenui in modo efficace gli incidenti di sicurezza che si verificano nell'ambiente del fornitore.</p> <p>Il Fornitore deve garantire di disporre di piani scritti di risposta agli incidenti che definiscano i ruoli del personale e le fasi di gestione degli incidenti:</p> <ul style="list-style-type: none"> • Convalida degli incidenti - Stabilire un processo di convalida degli incidenti che sfrutti varie fonti di dati e sia integrato in tutta l'azienda per convalidare efficacemente gli incidenti di sicurezza. 	<p>Un processo di risposta e gestione degli incidenti aiuta a garantire che vengano rapidamente circoscritti e che ne venga impedita l'escalation.</p>

	<ul style="list-style-type: none">• Classificazione degli incidenti - Stabilire un processo di classificazione degli incidenti che classifichi in modo efficace e rapido un incidente convalidato in tutti i tipi di evento, consentendo una rapida attività di risposta agli incidenti.• Contenimento degli incidenti - Utilizzare le persone, i processi e le capacità tecnologiche per contenere in modo rapido ed efficace gli incidenti di sicurezza nell'ambiente.• Rimozione/Mitigazione delle minacce - Sfruttare le capacità delle persone, dei processi e della tecnologia per rimuovere/attenuare in modo rapido ed efficace le minacce alla sicurezza e/o i relativi componenti nell'ambiente. <p>Il Fornitore deve cercare di dimostrare che le attività di risposta sono migliorate, ove possibile, incorporando le lezioni apprese dalle attività di rilevamento/risposta attuali e precedenti.</p> <p>Il Fornitore è tenuto a garantire che i team e i processi di risposta agli incidenti sono testati, almeno annualmente, per garantire che il Fornitore sia in grado di reagire agli incidenti di Cyber Security.</p> <ul style="list-style-type: none">• I test devono includere la conferma della capacità di informare Barclays, dimostrando la possibilità di contattare i soggetti incaricati.• Comunicazione - Il Fornitore deve nominare un Punto di Contatto per gli eventuali incidenti di sicurezza che si metta in contatto con Barclays in caso di incidente. Il Fornitore è tenuto a comunicare a Barclays i dati di contatto delle persone e le eventuali modifiche, compresi i contatti fuori orario e i numeri di telefono. <p>I dettagli devono includere: -Nome, responsabilità all'interno dell'organizzazione, ruolo, indirizzo e-mail e/o numero di telefono</p> <p>Il Fornitore informerà Barclays, entro un ragionevole lasso di tempo dal momento in cui viene a conoscenza di qualsiasi incidente che abbia un impatto sul servizio erogato a</p>	
--	--	--

	<p>Barclays o sulle Informazioni/Dati di Barclays e, in ogni caso, non oltre due (2) ore dal momento in cui l'Incidente giunge all'attenzione del Fornitore.</p> <p>In caso di violazione dei dati sospetta o nota, il Fornitore è tenuto a informare Barclays di tali incidenti in linea con i requisiti di protezione dei dati del Paese interessato.</p> <p>Il Fornitore è tenuto a fornire a Barclays un rapporto in relazione a qualsiasi incidente che abbia un impatto sui servizi resi a Barclays o su Dati/Informazioni di Barclays. Il rapporto deve includere i seguenti dettagli:</p> <ul style="list-style-type: none"> • Data e ora • Località • Tipo di incidente • Impatto • Stato • Mitigazione o azioni intraprese <p>Questi incidenti devono essere segnalati al Barclays Supplier Manager e al Barclays Joint Operations Centre all'interno del Barclays Chief Security Office (CSO) Joint Operations Centre (JOC) - gcsojoc@barclays.com.</p>	
<p>6. Classificazione e protezione delle informazioni</p>	<p>Il Fornitore deve disporre di un quadro/schema di classificazione e gestione delle informazioni stabilito e adeguato (allineato ai requisiti delle Buone Pratiche di Settore e/o di Barclays) che copra i seguenti aspetti:</p> <ul style="list-style-type: none"> • Assegnazione del corretto schema di etichette informative. • Gestione delle informazioni in modo sicuro in linea con il livello di classificazione assegnato. • Garantire che tutto il personale sia a conoscenza dei requisiti di etichettatura e gestione del Fornitore/di Barclays e di come applicare in modo appropriato la corretta classificazione delle informazioni. 	<p>Occorre applicare in modo efficace controlli appropriati al fine di assicurare che l'accesso ai dati sensibili Barclays sia riservato a coloro che hanno reale necessità di consultarli (riservatezza) e che i dati siano protetti contro le modifiche non autorizzate (integrità) e possano essere recuperati e</p>

	<p>Il Fornitore deve fare riferimento allo Schema di etichettatura delle informazioni Barclays e ai requisiti di gestione (Appendice B, Tabella B1 e B2) o a uno schema alternativo per garantire che il Fornitore protegga e garantisca le informazioni di Barclays detenute o trattate. Questo requisito si applica a tutti i beni informatici detenuti o trattati per conto di Barclays.</p>	<p>trasmessi quando richiesto (disponibilità).</p> <p>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.</p>
<p>7. Gestione delle risorse (Hardware e Software)</p>	<p>Durante l'intero ciclo di vita dei beni, il Fornitore deve garantire che sia stabilito un programma efficace per la loro gestione. La gestione patrimoniale controlla il ciclo di vita dei beni dall'acquisizione alla dismissione, fornendo visibilità e sicurezza a tutte le classi di beni nell'ambiente.</p> <p>Il Fornitore deve mantenere un inventario completo e accurato dei beni critici per l'azienda situati in tutti i siti e/o luoghi geografici che forniscono servizi a Barclays, incluse le attrezzature Barclays ospitate nei locali del Fornitore, di un subappaltatore del Fornitore o fornite da Barclays, e garantire che sia svolto almeno un test annuale per confermare che l'inventario dei beni informatici sia aggiornato, completo e accurato.</p> <p>Il processo di Gestione delle Risorse deve coprire le seguenti aree:</p> <ul style="list-style-type: none"> • Il patrimonio informatico e le infrastrutture sono protetti in base alla loro classificazione, alla loro criticità e al loro valore commerciale. • Mantenere un inventario accurato e aggiornato di tutti i beni tecnologici che potenzialmente possono memorizzare o elaborare le informazioni. L'inventario deve includere tutti i beni, connessi o meno alla rete dell'organizzazione. (Specifico per i servizi erogati a Barclays). 	<p>Un inventario completo e accurato del patrimonio di dati è essenziale per garantire controlli appropriati.</p> <p>In caso di mancata attuazione di questo principio, le attività di Barclays o le attività di Fornitori al servizio di Barclays potrebbero risultare compromesse e comportare perdite finanziarie, perdite di dati, danni alla reputazione e richiami ufficiali.</p>

	<ul style="list-style-type: none"> • I fornitori con una configurazione di Livello 1, Livello 2 e Livello 3 devono mantenere un inventario aggiornato, completo e accurato dei beni (inclusi desktop, laptop, apparecchiature di rete, token RSA o qualsiasi bene fornito da Barclays). • Assicurarsi che i beni non autorizzati siano rimossi dalla rete, messi in quarantena o che l'inventario sia aggiornato tempestivamente. • Mantenere un elenco aggiornato di tutti i software autorizzati necessari per l'erogazione dei servizi di Barclays. • Assicurarsi che solo le applicazioni software o i sistemi operativi attualmente supportati e che ricevono gli aggiornamenti del fornitore siano aggiunti all'inventario dei software autorizzato dell'organizzazione. Il software non supportato deve essere etichettato come non supportato nel sistema di inventario. <p>Il Fornitore deve garantire l'implementazione di procedure efficaci ed efficienti per la mitigazione delle tecnologie non supportate e la fine del ciclo di vita, la dismissione e la distruzione di beni e dati per eliminare il rischio di compromissione dei dati.</p>	
<p>8. Distruzione/Cancellazione/Disattivazione di Informazioni Fisiche e Logiche</p>	<p>La distruzione o cancellazione del Patrimonio di dati di Barclays archiviato in formato fisico o elettronico deve avvenire in modo sicuro e commisurato ai rischi associati, accertandosi che i dati di Barclays non siano recuperabili.</p> <p>Il Fornitore deve stabilire politiche e procedure con processi aziendali di supporto e misure tecniche implementate per lo smaltimento sicuro e la completa rimozione dei dati Barclays da tutti i supporti di memorizzazione, garantendo che i dati non siano recuperabili con qualsiasi mezzo informatico forense.</p>	<p>La distruzione sicura del Patrimonio di dati aiuta a garantire che tale Patrimonio di dati Barclays non possa essere recuperato per attività di violazione o furto dei dati o per finalità dannose.</p>
<p>9. Sicurezza del perimetro e della rete</p>	<p>Il Fornitore deve garantire che tutti i Sistemi IT gestiti dal Fornitore o dai rispettivi subfornitori che supportano i servizi erogati a Barclays siano protetti da manovre o minacce laterali all'interno della rete del Fornitore (e di qualsiasi subfornitore pertinente).</p> <p>Il Fornitore deve rilevare/prevenire/correggere il flusso di informazioni che si trasferisce</p>	<p>La mancata implementazione di questo principio potrebbe comportare l'attacco delle reti esterne o interne da parte di hacker</p>

	<p>attraverso reti con diversi livelli di fiducia con particolare attenzione ai dati dannosi per la sicurezza.</p> <p>I Meccanismi di integrità della rete devono coprire le seguenti aree:</p> <ul style="list-style-type: none">• 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 o nel caso in cui vi sia un requisito legato ad un evento che causa cambiamenti.• Tutti i collegamenti esterni alla rete del Fornitore devono essere documentati, devono passare attraverso un firewall e devono essere verificati e approvati prima di stabilire la connessione al fine di prevenire violazioni della sicurezza.• Le reti dei Fornitori sono protette mediante l'applicazione di principi di difesa in profondità (ad es. segmentazione della rete, firewall, controlli fisici di accesso alle apparecchiature di rete, ecc.)• Il Fornitore deve disporre di tecnologie di prevenzione delle intrusioni in rete per rilevare e impedire l'ingresso di traffico dannoso nella rete.• Uso di potenti firewall di rete per fornire un livello di difesa perimetrale contro attacchi di rete dolosi.• Tutto il traffico di rete da o verso Internet passa attraverso un proxy con livello di applicazione autenticato che è configurato per filtrare le connessioni non autorizzate.• I dispositivi di rete sono protetti in modo sicuro per prevenire attacchi dolosi.• Separazione logica delle porte/interfacce per la gestione dei dispositivi dal traffico degli utenti; controlli di autenticazione appropriati.• Tutte le regole di configurazione che consentono il flusso del traffico attraverso i dispositivi di rete devono essere documentate in un sistema di gestione della configurazione con una specifica motivazione aziendale per ogni regola.	<p>al fine di ottenere l'accesso ai servizi o ai dati contenuti.</p>
--	--	--

	<ul style="list-style-type: none">• Negare la comunicazione su porte TCP o UDP o il traffico di applicazioni non autorizzati per garantire che solo ai protocolli autorizzati sia consentito attraversare il perimetro di rete in entrata o in uscita tramite le porte di rete dedicate.• Eseguire regolari verifiche tentando l'ingresso nel perimetro di ogni rete protetta per rilevare eventuali connessioni non autorizzate.• Comunicazioni sicure tra i dispositivi e le postazioni di gestione/console.• Configurare i sistemi di monitoraggio per registrare i pacchetti di rete che passano attraverso il perimetro in ciascuno dei perimetri della rete dell'organizzazione.• La connessione di rete tra uffici/fornitore di servizi cloud/data center deve essere crittografata in base a un protocollo sicuro. I dati Barclays in transito all'interno della Wide Area Network (WAN) del Fornitore devono essere criptati.• Il fornitore deve rivedere annualmente le regole del firewall (Firewall esterno e interno).• Tutti gli accessi wireless alla rete sono soggetti a protocolli di autorizzazione, autenticazione, segmentazione e criptazione per prevenire le violazioni della sicurezza.• Il Fornitore deve garantire che l'accesso alla rete interna sia monitorato e consentito esclusivamente ai dispositivi autorizzati, tramite adeguati controlli di accesso alla rete• L'accesso remoto alla rete del fornitore deve utilizzare l'autenticazione a più fattori. <p>Il Fornitore deve garantire che i server utilizzati per fornire il servizio a Barclays non siano distribuiti su reti non affidabili (reti al di fuori del perimetro di sicurezza dell'utente, che sono al di fuori del controllo amministrativo dell'utente, ad esempio, per l'accesso a Internet) senza adeguati controlli di sicurezza.</p>	
--	---	--

	<p>Il Fornitore che ospita le informazioni Barclays (incluso il subappaltatore) in un data center o spazio cloud deve possedere una certificazione ISO/IEC 27001 e/o SOC 1 o 2 valida per la gestione della sicurezza (o certificazioni che dimostrino controlli equivalenti, supportate da un rapporto di audit indipendente).</p> <p>Rete T2 e T3 -</p> <ul style="list-style-type: none"> • La rete T2 deve essere separata in modo logico dalla rete aziendale del Fornitore da un Firewall e tutto il traffico in entrata e in uscita deve essere limitato e monitorato. • La configurazione del percorso deve garantire solo le connessioni alla rete Barclays e non deve condurre ad altre reti del Fornitore. • Il router Supplier Edge che si collega ai gateway extranet di Barclays deve essere configurato in modo sicuro con un concetto di limitazione dei controlli di porte, protocolli e servizi; <ul style="list-style-type: none"> ○ Assicurarsi che la registrazione e il monitoraggio siano abilitati. <p><i>N.B. Il termine "rete" come utilizzato in questo controllo si riferisce a qualsiasi rete non-Barclays per cui il Fornitore è responsabile, dell'inclusione delle reti del subfornitore.</i></p>	
<p>10. Rifiuto di rilevamento del servizio (Denial of Service Detection)</p>	<p>Il Fornitore deve mantenere la capacità di rilevare e proteggere dagli attacchi Rifiuto di servizio (Denial of Service - DoS) e Rifiuto di servizio diffuso (Distributed Denial of Services - DDoS).</p> <p>Il Fornitore deve accertarsi che i servizi di supporto per i canali Internet o esterni erogati a Barclays godano di un'adeguata protezione DoS per garantire la disponibilità.</p>	<p>In caso di mancata attuazione di questo principio, Barclays e i suoi Fornitori potrebbero non essere in grado di impedire che un attacco di tipo Denial of Service vada a buon fine.</p>
<p>11. Accesso remoto</p>	<p>L'accesso remoto alla rete Barclays tramite l'applicazione Barclays Citrix e/o i dati Barclays presenti/archiviati all'interno dell'ambiente gestito dal Fornitore non sono forniti di default e non forniscono la connessione da luoghi non approvati/fuori ufficio/da casa, e</p>	<p>I controlli di accesso remoto aiutano a garantire che i dispositivi non autorizzati e non sicuri non siano</p>

	<p>qualsiasi accesso remoto deve essere approvato e autorizzato da Barclays (Chief Security Office - ECAM Team).</p> <p>Il Fornitore deve garantire che i seguenti componenti siano istituiti per l'accesso remoto:</p> <ul style="list-style-type: none">• L'accesso remoto alla rete del Fornitore deve essere criptato durante il trasferimento dei dati e utilizzare l'autenticazione a più fattori.• L'accesso alla rete Barclays deve avvenire tramite l'applicazione Barclays Citrix con Token RSA (Hard & Soft) fornito da Barclays• Il Fornitore deve mantenere un inventario di tutti i token RSA (Hard & Soft) forniti da Barclays e un processo di gestione che includa la revisione e il monitoraggio dell'assegnazione, dell'utilizzo e della restituzione dei token (Hard token).• Il Fornitore deve conservare le registrazioni delle persone a cui è stato chiesto di lavorare da remoto e le motivazioni di tale richiesta• Il Fornitore deve eseguire la riconciliazione di tutti gli utenti remoti su base trimestrale e fornire un'attestazione a Barclays (Chief Security Office - team ECAM).• Barclays disattiverà 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).• Il fornitore deve garantire che il punto finale utilizzato per il collegamento da remoto ai sistemi informativi di Barclays sia configurato in modo sicuro (ad es. livello delle patch, stato dell'anti-malware, ecc.)• I servizi che hanno accesso alla stampa remota tramite l'applicazione Barclays Citrix devono essere approvati e autorizzati da Barclays (Chief Security Office -	<p>collegati all'ambiente Barclays da remoto.</p>
--	--	---

	<p>ECAM Team). Il fornitore deve mantenere i registri ed eseguire la riconciliazione trimestrale.</p> <ul style="list-style-type: none"> • 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 del fornitore, i consulenti, gli operatori di emergenza, gli appaltatori e i partner di servizi gestiti). <p>Nota: l'accesso remoto alla rete e ai dati di Barclays non è consentito se non specificamente approvato e autorizzato da Barclays.</p>									
<p>12. Gestione dei registri di sicurezza</p>	<p>Il Fornitore deve garantire l'esistenza di un quadro di audit e di gestione dei registri consolidato e di supporto che confermi che i sistemi IT chiave, comprese le applicazioni, le apparecchiature di rete, i dispositivi di sicurezza e i server, siano impostati per registrare gli eventi chiave e i registri devono essere centralizzati, adeguatamente protetti e conservati dal Fornitore per un periodo minimo di 12 mesi.</p> <table border="1" data-bbox="478 878 1465 1089"> <thead> <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> </thead> <tbody> <tr> <td>Conservazione dei registri</td> <td>3 mesi</td> <td>6 mesi</td> <td>12 mesi</td> </tr> </tbody> </table> <p>Il processo di Gestione dei Registri di Sicurezza deve coprire le seguenti aree:</p> <ul style="list-style-type: none"> • 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. 	Categoria	Sistemi a impatto basso / Servizio	Sistemi a impatto medio / Servizio	Sistemi a impatto elevato / Servizio	Conservazione dei registri	3 mesi	6 mesi	12 mesi	<p>La mancata implementazione di questo controllo potrebbe comportare l'impossibilità da parte dei Fornitori di rilevare e rispondere all'uso improprio o dannoso dei loro servizi o dei dati forniti entro periodi di tempo ragionevoli.</p>
Categoria	Sistemi a impatto basso / Servizio	Sistemi a impatto medio / Servizio	Sistemi a impatto elevato / Servizio							
Conservazione dei registri	3 mesi	6 mesi	12 mesi							

	<ul style="list-style-type: none">• Raccogliere, gestire e analizzare i registri di audit degli eventi che potrebbero aiutare a rilevare, comprendere o recuperare da 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.• Esempi di registri di eventi:<ul style="list-style-type: none">○ 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 degli eventi, compresi quelli che sono stati esternalizzati o che sono "in clouding".• Analisi dei registri degli eventi relativi alla sicurezza (compresa la normalizzazione, l'aggregazione e la correlazione).• Sincronizzazione delle marche temporali nei registri degli eventi con una fonte comune e affidabile• Protezione dei registri degli eventi relativi alla sicurezza (ad es. tramite cifratura, 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.	
--	---	--

	<p>Gli eventi principali registrati devono comprendere quelli che potrebbero compromettere la riservatezza, l'integrità e la disponibilità dei Servizi resi a Barclays e potrebbero contribuire all'identificazione o alla ricerca di incidenti di rilievo e/o violazioni dei diritti di accesso che si verificano in relazione ai Sistemi del Fornitore</p>	
<p>13. Difese contro i malware</p>	<p>Il Fornitore deve far sì che vengano stabilite politiche e procedure e che siano implementati processi aziendali e misure tecniche di supporto per prevenire l'esecuzione di malware su dispositivi di proprietà dell'organizzazione o gestiti dall'utente finale (ad esempio, workstation, laptop e dispositivi mobili distribuiti) e componenti di rete e di sistema dell'infrastruttura IT.</p> <p>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.</p> <p>La protezione dai malware deve avere o includere quanto segue:</p> <ul style="list-style-type: none"> • Software anti-malware gestito a livello centrale per monitorare e difendere costantemente ogni postazione di lavoro e server dell'organizzazione. • Garanzia che il software anti-malware dell'organizzazione aggiorni regolarmente il proprio motore di scansione e il database delle firme. • Inviare tutti gli eventi di rilevamento di malware agli strumenti di amministrazione anti-malware aziendali e ai server di registro degli eventi per l'analisi e gli avvisi. • Il Fornitore deve implementare controlli appropriati per la protezione contro il malware mobile e gli attacchi ai dispositivi mobili che si connettono a Barclays o alle reti del Fornitore e che accedono ai dati di Barclays. <p>Nota: Anti-malware per includere il rilevamento di (ma non solo) codici mobili non autorizzati, virus, spyware, software key logger, botnet, worm, trojan, ecc.</p>	<p>Le soluzioni anti-malware sono fondamentali per la protezione dei Patrimoni di dati Barclays contro i Codici Maligni.</p>

<p>14. Standard per la configurazione sicura</p>	<p>Il Fornitore deve disporre di un quadro di riferimento consolidato per garantire che tutti i sistemi/apparecchiature di rete configurabili siano configurati in modo sicuro conformemente agli standard di settore (ad es. NIST, SANS, CIS).</p> <p>Il processo standard di configurazione deve coprire le seguenti aree:</p> <ul style="list-style-type: none"> • Stabilisce politiche, procedure e strumenti per gli standard di configurazione della sicurezza per tutti i dispositivi di rete e i sistemi operativi autorizzati. • Esegue controlli regolari (annuali) sull'applicazione delle norme per garantire che il mancato rispetto degli standard di sicurezza di base sia prontamente corretto. Sono in atto controlli e monitoraggi adeguati per garantire che sia mantenuta l'integrità delle costruzioni/apparecchiature. • I sistemi e i dispositivi di rete sono configurati in modo da funzionare secondo i principi di sicurezza (ad es. concetto di limitazione dei controlli di porte, protocolli e servizi e nessun software non autorizzato). <p>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.</p>	<p>I controlli delle norme della struttura aiutano a proteggere il Patrimonio di dati da accesso non autorizzato</p> <p>La conformità alle strutture e ai controlli standard che garantiscono l'autorizzazione delle modifiche aiuta a garantire la protezione del Patrimonio di dati Barclays</p>
<p>15. Sicurezza dell'endpoint</p>	<p>Il Fornitore deve garantire che gli endpoint utilizzati per accedere alla rete di Barclays o per accedere/elaborare i Dati di Barclays siano configurati per la protezione dagli attacchi.</p> <p>La costruzione di sicurezza dell'endpoint deve avere: -</p> <ul style="list-style-type: none"> • Crittografia del disco. • Disattivare tutti i software/servizi/porte non necessari. • Disattivare l'accesso ai diritti di amministrazione per l'utente locale. • Il personale del Fornitore non potrà modificare le impostazioni di base come il Service Pack predefinito, la partizione di sistema e i servizi predefiniti, ecc. • La porta USB deve essere disabilitata per vietare la copia dei dati Barclays su supporti esterni 	<p>La mancata attuazione di questo controllo potrebbe rendere Barclays, la rete e gli endpoint dei Fornitori vulnerabili agli attacchi Cibernetici.</p>

	<ul style="list-style-type: none">• Aggiornato con le ultime firme antivirus e patch di sicurezza.• Prevenzione della perdita di dati limitata al divieto di taglia-copia-incolla e stampa-schermo dei dati Barclays• Come impostazione predefinita, l'accesso alla stampante deve essere disabilitato.• Il Fornitore deve limitare la capacità di accedere a siti di social network, servizi di webmail e siti con la possibilità di memorizzare informazioni su Internet come google drive, Dropbox, iCloud.• La condivisione/il trasferimento dei dati di Barclays durante l'utilizzo di strumenti/software di messaggistica istantanea devono essere disabilitati.• Capacità e processi per rilevare software non autorizzati identificati come dannosi e impedire l'installazione di software non autorizzati. <p>Nota: I supporti rimovibili/dispositivi portatili devono essere disabilitati per impostazione predefinita e abilitati solo per legittimi motivi di lavoro.</p> <p>Il Fornitore deve mantenere immagini o modelli sicuri per tutti i sistemi dell'azienda sulla base degli standard di configurazione approvati dall'organizzazione. Qualsiasi nuova implementazione del sistema o sistema esistente che venga compromesso deve essere raffigurato utilizzando una di queste immagini o modelli.</p> <p>Dispositivi mobili utilizzati per i servizi Barclays -</p> <ol style="list-style-type: none">1. Il Fornitore deve assicurarsi di implementare le funzionalità di gestione dei dispositivi mobili (MDM) per controllare e gestire in modo sicuro durante l'intero ciclo di vita i dispositivi mobili che hanno accesso e/o contengono informazioni classificate Barclays, riducendo il rischio di compromissione dei dati.2. Il Fornitore deve garantire l'implementazione delle funzionalità di blocco e cancellazione remota dei dispositivi mobili per proteggere le informazioni in caso di smarrimento, furto o compromissione di un dispositivo.3. Crittografare i dati dei dispositivi mobili (Dati di Barclays).	
--	--	--

	<p>4. Per impostazione predefinita, sui dispositivi mobili forniti dal Fornitore non deve essere consentito l'utilizzo di servizi basati sul cloud.</p>	
<p>16. Prevenzione della fuga di dati</p>	<p>Il Fornitore deve disporre di un quadro di riferimento consolidato per garantire che sia in atto la protezione contro la fuga di dati inopportuna garantendo una protezione che include i seguenti canali di fuga di dati (a titolo esemplificativo):</p> <ul style="list-style-type: none"> • Trasferimento non autorizzato di informazioni al di fuori della rete interna/rete del Fornitore. <ul style="list-style-type: none"> ○ E-mail ○ Internet/Web Gateway (inclusi archiviazione on-line e webmail) • Perdita o furto del Patrimonio di dati di Barclays da supporti elettronici portatili (comprese le informazioni elettroniche su laptop, dispositivi mobili e supporti portatili). • Trasferimento non autorizzato di informazioni a supporti portatili. • Scambio non sicuro di informazioni con terze parti (subfornitori). • Stampa o copia inadeguata di informazioni. 	<p>Occorre applicare in modo efficace controlli appropriati al fine di assicurare che l'accesso alle informazioni Barclays sia riservato a coloro che hanno reale necessità di consultarli (riservatezza) e che i dati siano protetti contro le modifiche non autorizzate (integrità) e possano essere recuperati e trasmessi quando richiesto (disponibilità).</p> <p>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</p>
<p>17. Protezione dei dati</p>	<p>Il Fornitore deve garantire che i dati di Barclays affidati/presenti nella rete del Fornitore ricevano una protezione adeguata ottenuta attraverso una combinazione di crittografia, protezione dell'integrità e tecniche di prevenzione della perdita di dati. È importante prestare la dovuta attenzione a limitare l'accesso ai dati di Barclays.</p> <p>I controlli per la protezione dei dati devono coprire le seguenti aree:</p> <ol style="list-style-type: none"> 1. Devono essere stabilite politiche e procedure, e implementati processi aziendali e misure tecniche di supporto, in modo da inventariare, documentare e mantenere i flussi di dati per i dati presenti (permanentemente o temporaneamente) nelle applicazioni del servizio (fisiche e virtuali) geograficamente distribuite e dei componenti di rete e di sistema dell'infrastruttura e/o condivisi con terze parti diverse. 	

	<ol style="list-style-type: none">2. Mantenere un inventario di tutte le informazioni sensibili (Dati di Barclays) memorizzate, elaborate o trasmesse dal Fornitore.3. Stabilire uno standard di classificazione dei dati per garantire che le informazioni sensibili (Dati di Barclays) siano classificate e protette in modo appropriato.4. Assicurarsi che tutti i dati all'interno dell'organizzazione siano etichettati in base allo standard di classificazione dei dati.5. Politica di utilizzo dei dati - accesso ai dati6. Protezione dei dati archiviati;<ol style="list-style-type: none">a. Crittografare i dati archiviati per impedire lo sfruttamento di informazioni sensibili tramite l'accesso non autorizzato.7. Monitoraggio delle attività del database;<ol style="list-style-type: none">a. Monitorare l'accesso al database e l'attività per identificare rapidamente ed efficacemente le attività dannose.8. Protezione dei dati in uso;<ol style="list-style-type: none">a. Garantire che la visualizzazione e l'uso delle informazioni sensibili sia controllato attraverso le capacità di gestione degli accessi per proteggere dallo sfruttamento le informazioni sensibili.b. Utilizzare tecnologie di mascheramento e offuscamento dei dati per proteggere efficacemente i dati sensibili in uso dalla divulgazione involontaria e/o dallo sfruttamento malevolo.9. Protezione dei dati in transito;<ol style="list-style-type: none">a. Sfruttare le forti capacità di crittografia per garantire la protezione dei dati durante il transito.b. Solitamente la crittografia dei dati in transito è ottenuta utilizzando la crittografia Trasporto o Carico utile (Messaggio o Campo selettivo). I meccanismi di cifratura del trasporto includono, a titolo esemplificativo:<ul style="list-style-type: none">• Sicurezza del livello di trasporto (Transport Layer Security - TLS)• Tunneling sicuro (Secure Tunneling - IPsec)• Guscio di sicurezza (Secure Shell - SSH)	
--	--	--

	<p>c. I protocolli di sicurezza del trasporto devono essere configurati in modo da evitare la negoziazione di algoritmi più deboli e/o lunghezze di chiave più brevi, quando entrambi i punti finali supportano l'opzione più forte.</p> <p>10. Backup dei dati –</p> <p>a. Si devono prendere i dovuti provvedimenti per garantire che le Informazioni ricevano un adeguato back-up e siano recuperabili conformemente ai requisiti concordati con Barclays.</p> <p>b. Assicurarsi che i backup siano adeguatamente protetti tramite sicurezza fisica o crittografia quando vengono memorizzati, così come quando vengono spostati attraverso la rete. Sono compresi i backup remoti e i servizi cloud.</p> <p>c. Accertarsi che tutti i dati Barclays siano automaticamente e regolarmente sottoposti a backup.</p>	
<p>18. Sicurezza del software applicativo</p>	<p>Il Fornitore deve sviluppare le applicazioni utilizzando pratiche di codifica sicura e operando in un ambiente sicuro. Se il Fornitore sviluppa delle applicazioni per l'utilizzo da parte di Barclays o che sono utilizzate a supporto dei servizi resi a Barclays, il Fornitore deve stabilire un quadro di sviluppo sicuro per prevenire violazioni della sicurezza e per individuare e rimediare alle vulnerabilità nel codice durante il processo di sviluppo.</p> <p>La sicurezza del software applicativo deve coprire le seguenti aree:</p>	<p>I controlli che tutelano lo sviluppo di applicazioni aiutano a garantirne la sicurezza al momento della distribuzione.</p>

	<ul style="list-style-type: none">• Gli standard di codifica sicura devono essere in vigore e adottati conformemente alle migliori prassi del settore per prevenire le vulnerabilità di sicurezza e le interruzioni del servizio che, allo stesso tempo, difendono da possibili vulnerabilità ben note.• Stabilire pratiche di codifica sicure e adeguate al linguaggio di programmazione.• Tutte le attività di sviluppo devono essere svolte in un ambiente non produttivo.• Mantenere ambienti separati per i sistemi di produzione e non. Gli sviluppatori non devono avere un accesso non monitorato agli ambienti di produzione.• Separazione dei compiti per gli ambienti di produzione e non.• I sistemi sono sviluppati in linea con le migliori pratiche di Secure Development (ad esempio OWASP).• Il codice deve essere conservato in modo sicuro e soggetto ai controlli della Garanzia di Qualità.• Il codice deve essere adeguatamente protetto da modifiche non autorizzate una volta che il test è stato confermato e consegnato in produzione.• Per il software sviluppato dal Fornitore utilizzare solo componenti aggiornati di terze parti di fiducia.• Applicare strumenti di analisi statica e dinamica per verificare il rispetto delle pratiche di codifica sicura.• Il Fornitore deve garantire che i dati attuali (compresi i Dati Personali) non saranno utilizzati in ambienti non produttivi.• Le applicazioni e le interfacce di programmazione (API) devono essere progettate, sviluppate, implementate e testate conformemente ai principali standard di settore (ad es. OWASP per le applicazioni web). <p>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 comuni. Per le applicazioni che non sono basate sul web, devono essere implementati firewall specifici per le applicazioni, se tali strumenti sono disponibili per il tipo di applicazione dato. Se il traffico è criptato, il dispositivo dovrebbe trovarsi 'dietro' la criptazione o essere in grado di decriptare il</p>	
--	---	--

	traffico prima dell'analisi. Se nessuna delle due opzioni è appropriata, dovrebbe essere implementato un firewall per applicazioni web basate su host.	
--	--	--

<p>19. Logical Access Management (LAM)</p>	<p>L'accesso alle Informazioni deve essere limitato, tenendo in debita considerazione l'esigenza di conoscere (need-to-know), il Privilegio minimo e i principi di segregazione delle mansioni. Spetta al titolare del Patrimonio di dati decidere chi ha necessità di accedere e il tipo di accesso.</p> <ul style="list-style-type: none"> • 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. <p>I processi di gestione dell'accesso devono essere definiti secondo le migliori prassi del settore e devono includere quanto segue:</p> <ul style="list-style-type: none"> • Il fornitore è tenuto a garantire che le procedure di gestione degli accessi siano documentate e si applichino a tutti i sistemi IT (che memorizzano o elaborano patrimoni di dati Barclays); una volta implementate, inoltre, devono fornire controlli appropriati per quanto riguarda: Joiner / Mover / Leaver / Accesso remoto. • Occorre provvedere ai controlli ai fini dell'autorizzazione per assicurare che la procedura relativa alla concessione, alla modifica e alla revoca dell'accesso 	<p>Controlli LAM appropriati aiutano a garantire la protezione dei Patrimoni di dati da un uso improprio.</p> <p>Occorre applicare in modo efficace controlli appropriati al fine di assicurare che l'accesso alle informazioni Barclays sia riservato a coloro che hanno reale necessità di consultarli (riservatezza) e che i dati siano protetti contro le modifiche non autorizzate (integrità) e possano essere recuperati e trasmessi quando richiesto (disponibilità).</p> <p>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.</p>
--	--	--

	<p>comprenda un livello di autorizzazione commisurato ai privilegi in corso di concessione.</p> <ul style="list-style-type: none">• Occorre provvedere ai controlli atti ad assicurare che le procedure di gestione degli accessi comprendano processi appropriati di verifica dell'identità.• Ogni account deve essere associato a una singola persona, che sarà responsabile di tutte le attività svolte utilizzando l'account.• Ricertificazione dell'accesso - Occorre provvedere ai controlli atti ad assicurare che i permessi di accesso siano riesaminati almeno ogni 12 mesi, al fine di verificare che siano commisurati allo scopo.• Tutti i permessi di accesso privilegiato devono essere riesaminati almeno ogni sei (6) mesi; inoltre, occorre implementare controlli adeguati per quanto riguarda le richieste di accesso privilegiato.• Controlli sui trasferimenti – Accesso modificato entro ventiquattro (24) ore dalla data di trasferimento;• Controlli sui congedi – Tutti gli accessi logici utilizzati per fornire a Barclays i servizi, rimossi entro ventiquattro (24) ore dalla data del congedo;• Accesso remoto - I controlli sugli accessi remoti devono essere autorizzati esclusivamente tramite procedure approvate da Barclays (Chief Security Office - ECAM team) e gli accessi remoti devono utilizzare l'autenticazione a più fattori.• Autenticazione - Lunghezza e complessità delle password adeguate, frequenza delle modifiche delle password, autenticazione a più fattori, gestione sicura delle credenziali delle password o altri controlli devono essere seguiti secondo le Best Practices del settore• Gli account inattivi non utilizzati da almeno 60 giorni consecutivi devono essere sospesi/disabilitati.• Le password di account interattivi devono essere cambiate almeno ogni 90 giorni e devono essere diverse dalle dodici (12) precedenti.• Gli Account privilegiati devono essere cambiati dopo ogni uso e almeno ogni 90 giorni.	
--	--	--

	<ul style="list-style-type: none"> • Gli account interattivi devono essere disabilitati dopo un massimo di cinque (5) tentativi consecutivi di accesso non riusciti. 	
<p>20. Gestione della vulnerabilità</p>	<p>Il Fornitore deve far sì che vengano stabilite politiche e procedure e che siano implementati processi e misure tecniche di supporto per il rilevamento tempestivo delle vulnerabilità all'interno di applicazioni gestite o di proprietà dell'organizzazione, della rete infrastrutturale e dei componenti di sistema per garantire l'efficienza dei controlli di sicurezza implementati.</p> <p>Gestione delle Vulnerabilità deve coprire le seguenti aree:</p> <ul style="list-style-type: none"> • Devono essere stabilite politiche e procedure e implementati processi e misure tecniche di supporto per il rilevamento tempestivo delle vulnerabilità all'interno di applicazioni gestite o di proprietà dell'organizzazione, della rete infrastrutturale e dei componenti di sistema per garantire l'efficienza dei controlli di sicurezza implementati. • Ruoli e responsabilità definiti. • Strumenti e infrastrutture adeguati per la scansione delle vulnerabilità. • Svolgere regolarmente scansioni delle vulnerabilità che identifichino efficacemente le vulnerabilità note e sconosciute in tutte le classi di attività dell'ambiente. • Utilizzare un processo di valutazione del rischio per dare priorità al rimedio delle vulnerabilità scoperte. • Stabilire un processo di validazione per il rimedio delle vulnerabilità che verifichi in modo rapido ed efficace tale rimedio in tutte le classi di attività nell'ambiente. • Accertarsi che le vulnerabilità siano affrontate in modo efficace attraverso robuste attività di bonifica e gestione delle patch per ridurre il rischio di sfruttamento delle vulnerabilità. • Confrontare regolarmente i risultati di scansioni consecutive delle vulnerabilità per verificare che queste ultime siano state corrette in modo tempestivo. 	<p>La mancata attuazione di questo controllo potrebbe comportare l'utilizzo di queste vulnerabilità dei sistemi per condurre attacchi Cibernetici contro Barclays e i suoi Fornitori.</p>

	<p>Tutti i problemi di sicurezza e le vulnerabilità che potrebbero avere un impatto concreto sull'infrastruttura di hosting di Barclays/le applicazioni web fornite dal Fornitore, che il Fornitore ha deciso di accettare a rischio, devono essere comunicati/notificati a Barclays tempestivamente e concordate per iscritto con Barclays (Chief Security Office - team ECAM).</p>	
21. Gestione degli aggiornamenti	<p>Il Fornitore deve far sì che vengano stabilite politiche e procedure e che siano implementati processi aziendali e misure tecniche di supporto per l'implementazione di patch di sicurezza per i dispositivi end-point gestiti dagli utenti (ad es. workstation, laptop e dispositivi mobili) e per i componenti di rete e di sistema dell'infrastruttura IT.</p> <p>Il Fornitore deve garantire che le più recenti patch di sicurezza siano applicate ai sistemi/attività/reti/applicazioni in modo tempestivo, accertandosi che:</p> <ul style="list-style-type: none"> • il Fornitore controlli tutte le patch su sistemi che rappresentano accuratamente la configurazione dei sistemi di produzione target prima dell'implementazione della patch nei sistemi di produzione e che il corretto funzionamento del servizio di patch sia verificato dopo ogni attività di patch. Se in un sistema non può essere installata una patch, adottare le contromisure appropriate. • Tutte le modifiche IT fondamentali devono essere registrate, verificate e approvate prima dell'implementazione tramite una procedura di gestione delle modifiche solida e approvata al fine di prevenire qualsiasi interruzione del servizio o violazione della sicurezza. • Il Fornitore deve garantire che le patch si riflettano negli ambienti di produzione e di DR. 	<p>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.</p>
22. Simulazione di minaccia/ Test di penetrazione/	<p>Il Fornitore deve coinvolgere un provider indipendente specializzato in servizi di sicurezza per eseguire una valutazione della sicurezza IT/simulazione della minaccia alle infrastrutture IT, compreso il disaster recovery, e alle applicazioni web relative ai servizi che il Fornitore eroga a Barclays.</p>	<p>In caso di mancata attuazione di questo controllo, i Fornitori potrebbero non essere in grado di valutare le Minacce Cibernetiche a</p>

<p>Valutazione della sicurezza IT</p>	<p>Questa procedura deve essere ripetuta almeno una volta all'anno per individuare le vulnerabilità che potrebbero essere sfruttate per violare la riservatezza dei dati di Barclays tramite Attacchi Cibernetici. Tutte le vulnerabilità devono ottenere la massima priorità e devono essere tracciate fino alla risoluzione. Il test deve essere svolto in linea con le Migliori Prassi del settore.</p> <p>Per i servizi erogati dai Fornitori relativamente all'infrastruttura/applicazione di Hosting per conto di Barclays.</p> <ul style="list-style-type: none"> • 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). 	<p>cui sono soggetti e l'idoneità e solidità delle proprie difese.</p> <p>Le informazioni di Barclays possono essere divulgate e/o può verificarsi una perdita del servizio che può dare luogo a provvedimenti legali o normativi o generare danni alla reputazione.</p>
<p>23. Crittografia</p>	<ul style="list-style-type: none"> • 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. • 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 	<p>La mancata implementazione di questo controllo impedisce di attivare gli adeguati controlli fisici e tecnici provocando ritardi o interruzione dell'erogazione del servizio o Violazioni della Sicurezza Cibernetica.</p>

	<p>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.</p> <ul style="list-style-type: none">• 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.<ul style="list-style-type: none">○ Il Fornitore deve garantire che tutte le chiavi siano soggette ad un criptoperiodo di tempo limitato e definito per la loro sostituzione o disattivazione. Ciò deve essere in linea anche con il National Institute of Standards and Technology (NIST) e con i requisiti di settore applicabili• Protezione della conservazione delle chiavi - Il Fornitore deve garantire che le chiavi crittografiche segrete/private esistano solo nelle seguenti forme:<ul style="list-style-type: none">○ nel confine crittografico di un dispositivo/modulo hardware di sicurezza certificato.○ In forma criptata sotto un'altra chiave stabilita o derivata da una password.○ In componenti separati suddivisi tra gruppi di custodi distinti.○ 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:<ul style="list-style-type: none">○ Chiavi per i servizi regolamentati in cui la protezione HSM è obbligatoria.○ Certificati che rappresentano Barclays da parte delle CA.○ Certificati Root, Issuing, OCSP e RA (autorità di registrazione) utilizzati per l'emissione di Certificati a protezione dei servizi Barclays.○ 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	
--	---	--

	<p>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.</p> <ul style="list-style-type: none">• 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:<ul style="list-style-type: none">○ Il Team di supporto IT○ Le attività collegate○ 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.<ul style="list-style-type: none">○ 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	
--	--	--

	<p>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.</p> <ul style="list-style-type: none"> • Chiave compromessa - Il Fornitore mantiene e monitora un piano per le chiavi compromesse per garantire che le chiavi di ricambio siano generate indipendentemente dalla chiave compromessa per evitare che quest'ultima fornisca informazioni sulla sua sostituzione. Se si verifica un incidente di compromesso, Barclays deve essere notificato al Barclays Chief Security Office (CSO) Joint Operations Centre (JOC) - gcsojoc@barclays.com. • Solidità degli algoritmi e delle chiavi - Il Fornitore garantisce che gli algoritmi e la lunghezza delle chiavi in uso sono conformi al National Institute of Standards and Technology (NIST) e ai requisiti di settore applicabili. <ul style="list-style-type: none"> ○ La solidità degli algoritmi e la lunghezza delle chiavi riducono al minimo il rischio che i dati sensibili vengano persi o compromessi da hacker con sofisticate capacità di elaborazione. ○ L'efficacia della crittazione utilizzata deve essere commisurata alla propensione al rischio, poiché può avere un impatto operativo o sulle prestazioni. 	
<p>24. Cloud Computing</p>	<p>Il Fornitore deve essere certificato ISO/IEC 27017 o 27001 o SOC 1 o 2 avendo stabilito e supportato processi aziendali e implementato misure tecniche per garantire che ogni utilizzo della tecnologia Cloud sia soggetto ad adeguati controlli di sicurezza applicati.</p> <p>I dati Barclays memorizzati nel Cloud come parte del servizio reso a Barclays devono essere approvati da Barclays (Chief Security Office - team ECAM).</p> <p>I controlli cloud devono coprire i seguenti modelli di distribuzione (IaaS/PaaS/SaaS):</p> <ul style="list-style-type: none"> • Gestione dell'identità e degli accessi/Controllo degli accessi • Connettività di rete 	<p>La mancata implementazione di questo controllo potrebbe compromettere i Dati Barclays protetti in modo non idoneo; tale condizione può dare luogo a provvedimenti normativi o generare danni alla reputazione.</p>

	<ul style="list-style-type: none"> • Protezione dei dati (Transito/Sosta/Archiviazione) • Registrazione e monitoraggio della sicurezza • Crittografia e gestione delle chiavi • Sicurezza delle applicazioni e delle interfacce • Sicurezza delle infrastrutture e della virtualizzazione • Separazione dei servizi 	
25. Spazio dedicato alla banca (Bank Dedicated Space - BDS)	<p>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.)</p> <p>I diversi tipi di BDS sono:</p> <p>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.</p> <p>Livello 2 (Business class) - L'intera infrastruttura IT è gestita dal Fornitore e si collega ai gateway Barclays - i dispositivi LAN, WAN & Desktop sono di proprietà e gestiti dal Fornitore.</p> <p>Livello 3 (Classe Economy) - L'intera infrastruttura IT è gestita dal Fornitore e si collega ai gateway Internet Barclays - i dispositivi LAN, WAN & Desktop sono di proprietà e gestiti dal Fornitore.</p>	La mancata implementazione di questo controllo impedisce di attivare gli adeguati controlli fisici e tecnici provocando ritardi o interruzione dell'erogazione del servizio o violazioni della sicurezza cibernetica.
25.1 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.	
25.2 BDS - Controllo dell'accesso fisico	<ul style="list-style-type: none"> • Il Fornitore deve porre in essere un processo di accesso fisico che copra i metodi di accesso e l'autorizzazione al BDS nel luogo in cui vengono erogati i servizi. • L'ingresso e l'uscita verso le aree BDS devono essere limitati e monitorati da meccanismi di controllo dell'accesso fisico per garantire che l'accesso sia consentito solo al personale autorizzato. 	

	<ul style="list-style-type: none"> • Una carta d'accesso elettronica autorizzata per accedere alle aree BDS degli uffici. • Il Fornitore deve effettuare controlli trimestrali per garantire che solo le persone autorizzate abbiano accesso alle aree BDS. Le eccezioni vengono studiate a fondo fino alla risoluzione. • I diritti di accesso vengono rimossi entro 24 ore per tutti gli utenti soggetti a spostamenti o dimissioni. • Utilizzare i guardiani per pattugliare abitualmente l'interno delle aree BDS per identificare efficacemente gli accessi non autorizzati o le attività potenzialmente dannose. • Per l'accesso a BDS devono essere svolti controlli automatici di sicurezza, tra cui: In caso di personale autorizzato: <ul style="list-style-type: none"> ○ Tesserino identificativo con foto sempre visibile ○ Sono utilizzati lettori ottici di card ○ Sono attivi dispositivi anti-pass back • Il Fornitore deve disporre di processi e procedure per il controllo e il monitoraggio di persone esterne, comprese le terze parti con accesso fisico alle aree BDS a scopo di manutenzione e pulizia.
<p>25.3 BDS - Videosorveglianza</p>	<ul style="list-style-type: none"> • Implementare la videosorveglianza per le aree BDS per individuare efficacemente gli accessi non autorizzati o le attività dannose e contribuire alle indagini. • Tutti i punti di entrata e uscita dell'area BDS devono essere videosorvegliati. • Le telecamere di sicurezza sono posizionate in modo appropriato e forniscono immagini chiare e identificabili in ogni momento per catturare attività dannose e contribuire alle indagini. <p>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.</p>
<p>25.4 BDS - Accesso alla rete Barclays e ai token di autenticazione Barclays</p>	<ul style="list-style-type: none"> • 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.).

	<ul style="list-style-type: none"> • 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. <p>Fare riferimento alla Sezione11 - Sicurezza dell'accesso remoto</p>
25.5 BDS - Supporto di Out of Office	L'accesso remoto all'area BDS non è fornito di default per il supporto di out of office/out of business/work from home. Qualsiasi accesso remoto deve essere approvato dalle funzioni di Barclays pertinenti (compreso il Chief Security Office – ECAM team)
25.6 BDS - Sicurezza della rete	<ul style="list-style-type: none"> • Mantenere un inventario aggiornato di tutti i perimetri della rete dell'organizzazione (attraverso un'Architettura di Rete/Diagramma). • La progettazione e l'implementazione della rete deve essere rivista almeno una volta all'anno. • La rete BDS deve essere separata in modo logico dalla rete aziendale del Fornitore da un Firewall e tutto il traffico in entrata e in uscita deve essere limitato e monitorato. • La configurazione del percorso deve garantire solo le connessioni alla rete Barclays e non deve condurre ad altre reti del Fornitore. • Il router Supplier Edge che si collega ai gateway extranet di Barclays deve essere configurato in modo sicuro con un concetto di limitazione dei controlli di porte, protocolli e servizi; <ul style="list-style-type: none"> ◦ 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 <p>Fare riferimento alla Sezione 9 - Sicurezza del perimetro e della rete</p>
25.7 BDS - Rete wireless	Le reti wireless devono essere disabilitate per il segmento delle reti Barclays in cui si erogano i servizi di Barclays.
25.8 BDS - Sicurezza dell'endpoint	<p>È necessario configurare in modo sicuro e secondo le Migliori Prassi del settore la struttura dei desktop dei computer che utilizzano la rete BDS</p> <p>Costruzione di sicurezza dei dispositivi endpoint BDS:</p>

	<ul style="list-style-type: none"> • crittografia del disco; • avvio da altri dispositivi attivi deve essere disabilitato; • disattivare tutti i software/servizi/porte non necessari; • disattivare l'accesso ai diritti di amministrazione per l'utente locale • Il personale del Fornitore non potrà modificare le impostazioni di base come il Service Pack predefinito e i servizi predefiniti, ecc.; • la porta USB deve essere disabilitata per vietare la copia dei dati Barclays su supporti esterni; • aggiornata con le ultime firme antivirus e patch di sicurezza; • prevenzione della perdita di dati limitata al divieto di taglia-copia-incolla e stampa-schermo o strumento di cattura della stampa dei dati Barclays; • come impostazione predefinita, l'accesso alla stampante deve essere disabilitato; • la condivisione / il trasferimento dei dati di Barclays durante l'utilizzo di strumenti/software di messaggistica istantanea devono essere disabilitati; • capacità e processi per rilevare software non autorizzati identificati come dannosi e impedire l'installazione di software non autorizzati; <p>fare riferimento alla Sezione 15 - Controllo di sicurezza degli endpoint</p>
<p>25.9 BDS - E-mail e Internet</p>	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

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

Appendice A: Glossario

Account	Serie di credenziali (per esempio, ID utente e password) che consentono di gestire gli accessi ai sistemi IT tramite controlli sugli accessi logici.
Backup, Back-up	Un backup o la procedura di esecuzione del backup si riferisce alla realizzazione di copie dei dati che possono essere utilizzate per ripristinare gli originali dopo un evento di perdita dati.
Spazio dedicato alla banca	BDS (Bank Dedicated Space - Spazio Bancario Dedicato) indica i locali posseduti o controllati dai Membri del Gruppo del Fornitore o dai Subfornitori che sono dedicati in esclusiva a Barclays in cui sono realizzati o erogati i Servizi.
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.
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. O 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.
Autenticazione a più fattori	Autenticazione che utilizza due o più diverse tecniche di autenticazione. Un esempio è l'uso di un token di sicurezza, dove il successo dell'autenticazione dipende da qualcosa che è in possesso della persona (cioè il token di sicurezza) e da qualcosa che l'utente conosce (cioè il PIN del token di sicurezza).
Account privilegiato	<p>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.</p> <p>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.</p>
Account condiviso	Un account concesso a uno o più dipendenti, a consulenti, collaboratori esterni o personale temporaneo che siano stati autorizzati ad accedere quando non è possibile usare account individuali a causa della natura del sistema a cui si accede.
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 prima di scegliere un'altra opzione.
Incidente di sicurezza	<p>Sono definiti incidenti di sicurezza gli eventi che violano una politica di sicurezza esplicita o implicita.</p> <ul style="list-style-type: none"> • Tentativi (falliti o riusciti) di accesso non autorizzato ad un sistema o ai rispettivi dati. • Interruzione indesiderata o rifiuto di servizio. • Uso non autorizzato di un sistema per l'elaborazione o la memorizzazione dei dati.

- Modifiche alle caratteristiche hardware, firmware o software del sistema senza che il proprietario ne sia a conoscenza o fornisca istruzioni o consenso.
- Vulnerabilità dell'applicazione che comporta un accesso non autorizzato ai dati.

Appendice B: Schema di Etichettatura delle informazioni di Barclays

Tabella B1: Schema di Etichettatura delle informazioni di Barclays

Etichetta	Definizione	Esempi
Segrete	<p>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).</p> <p>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.</p>	<ul style="list-style-type: none"> • Informazioni su potenziali fusioni e acquisizioni • Informazioni di pianificazione strategica, a livello aziendale e organizzativo • Determinate informazioni sulla configurazione di sicurezza • Determinati risultati di audit e rapporti • Verbali dei comitati esecutivi • Dettagli di Autenticazione o Identificazione e verifica (ID&V) – cliente e collega • Grandi volumi di informazioni sui titolari di carte • Previsioni di profitto e risultati finanziari annuali (prima della divulgazione pubblica) • Qualsiasi punto che rientri nell'ambito di un Non-Disclosure Agreement (NDA - Accordo di non divulgazione) ufficiale
Riservata – Interna	<p>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</p>	<ul style="list-style-type: none"> • Strategie e budget • Stime delle performance • Remunerazione dei dipendenti e dati personali • Valutazioni di vulnerabilità

	<p>un target specifico.</p> <p>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).</p> <p>Queste informazioni non sono destinate alla diffusione generale ma possono essere inoltrate o condivise dai destinatari secondo il principio need-to-know.</p>	
Riservata – Esterna	<p>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.</p> <p>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).</p> <p>Queste informazioni non sono destinate alla diffusione generale ma possono essere inoltrate o condivise dai destinatari secondo il principio need-to-know.</p>	<ul style="list-style-type: none"> • Nuovi piani di prodotto • Contratti con i clienti • Contratti legali • Informazioni relative a clienti singoli/a basso volume da inviare all'esterno • Comunicazioni relative ai clienti. • Nuovi materiali per offerte (ad es. prospetti, promemoria per offerte) • Documenti di ricerca definitivi • Informazioni essenziali non pubbliche (Material Non-Public Information - MNPI) esterne a Barclays • Tutti i report di ricerca • Alcuni materiali di marketing • Commenti del mercato • Risultati di audit e rapporti
Non riservate	<p>Le informazioni destinate alla diffusione generale o la cui divulgazione non avrebbe un impatto negativo sull'organizzazione devono essere classificate come Non riservate.</p>	<ul style="list-style-type: none"> • Materiali di marketing • Pubblicazioni • Annunci pubblici • Annunci di lavoro

		• Informazioni che non influiscono su Barclays
--	--	--

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

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

Fase del ciclo di vita	Segrete	Riservata – Interna	Riservata – Esterna
Creazione e introduzione	<ul style="list-style-type: none"> • Ai patrimoni di dati deve essere assegnato un proprietario delle informazioni. 	<ul style="list-style-type: none"> • Ai patrimoni di dati deve essere assegnato un proprietario delle informazioni. 	<ul style="list-style-type: none"> • Ai patrimoni di dati deve essere assegnato un proprietario delle informazioni.
Conservazione	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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.

	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Non si deve lavorare su patrimoni di dati (sia fisici sia elettronici), né lasciarli incustoditi in luoghi in cui persone non autorizzate possano visualizzarli o accedervi. È possibile lavorare su patrimoni di dati se sussistono controlli adeguati (per esempio schermi per la privacy). I patrimoni di dati stampati devono essere recuperati immediatamente dalla stampante. Ove ciò non sia possibile, occorre usare strumenti di stampa sicuri. I dati elettronici devono essere protetti mediante controlli Logical Access Management appropriati
Condivisione	<ul style="list-style-type: none"> Le copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile su ciascuna pagina. 	<ul style="list-style-type: none"> Le copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile. L'etichetta deve essere apposta per lo meno sulla copertina. 	<ul style="list-style-type: none"> Le copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile. L'etichetta deve essere apposta per lo meno sulla copertina.

	<ul style="list-style-type: none">• Le buste contenenti copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile sul lato frontale ed essere chiuse con un sigillo che riveli eventuali tentativi di manomissione. Prima della distribuzione, inoltre, devono essere inserite in una seconda busta priva di etichetta.• I patrimoni di dati elettronici devono essere corredate di chiara etichetta informativa. Le copie elettroniche dei documenti di più pagine devono essere corredate di etichetta informativa visibile su ciascuna pagina.• I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione.• I patrimoni di dati devono essere distribuiti esclusivamente ai dipendenti dell'organizzazione o a individui vincolati a quest'ultima da un obbligo contrattuale appropriato o per assolvere a un'esigenza aziendale chiaramente riconosciuta, come una negoziazione contrattuale.	<ul style="list-style-type: none">• I patrimoni di dati elettronici devono essere corredate di chiara etichetta informativa.• I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione.• I patrimoni di dati devono essere distribuiti esclusivamente ai dipendenti dell'organizzazione o a individui vincolati a quest'ultima da un obbligo contrattuale appropriato o per assolvere a un'esigenza aziendale chiaramente riconosciuta, come una negoziazione contrattuale.	<ul style="list-style-type: none">• Le buste contenenti copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile sul lato frontale.• I patrimoni di dati elettronici devono essere corredate di chiara etichetta informativa. Le copie elettroniche dei documenti di più pagine devono essere corredate di etichetta informativa visibile su ciascuna pagina.• I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione.• I patrimoni di dati devono essere distribuiti esclusivamente ai dipendenti dell'organizzazione o a individui vincolati a quest'ultima da un obbligo contrattuale appropriato o per assolvere a un'esigenza aziendale chiaramente riconosciuta, come una negoziazione contrattuale.• I patrimoni di dati devono essere distribuiti esclusivamente alle persone che hanno necessità di riceverli per motivi connessi alla loro attività.
--	--	---	--

	<ul style="list-style-type: none"> • I patrimoni di dati devono essere distribuiti esclusivamente alle persone specificamente autorizzate a riceverli dal proprietario delle informazioni. • I patrimoni di dati non devono essere inviati via fax. • Durante il transito al di fuori della rete interna, i patrimoni di dati elettronici devono essere criptati tramite un dispositivo di protezione crittografica approvato. • Occorre implementare una catena di custodia dei patrimoni di dati elettronici. 		<ul style="list-style-type: none"> • I patrimoni di dati non devono essere inviati via fax, a meno che il mittente non abbia verificato che i destinatari sono pronti a ritirare il fax. • Durante il transito al di fuori della rete interna, i patrimoni di dati elettronici devono essere criptati tramite un dispositivo di protezione crittografica approvato.
Archiviazione ed eliminazione	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Le copie cartacee dei patrimoni di dati devono essere eliminate tramite un servizio di eliminazione riservato. • Le copie dei patrimoni di dati elettronici devono essere cancellate in modo tempestivo anche dai "cestini" del sistema o da dispositivi analoghi.

Segreto bancario

Ulteriori controlli solo per
giurisdizioni che prevedono il

segreto bancario
(Svizzera/Monaco)

Area di controllo / Titolo	Descrizione del controllo	Perché è importante?
1. Ruoli e responsabilità	<p>Il Fornitore deve definire e comunicare i ruoli e le responsabilità per la gestione dei Dati identificativi del cliente (Client Identifying Data - CID). Il Fornitore deve rivedere i documenti che specificano ruoli e responsabilità per i CID dopo qualsiasi modifica sostanziale al modello operativo (o alle attività) del Fornitore o almeno una volta all'anno e consegnarli alla pertinente giurisdizione che prevede il segreto bancario.</p> <p>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.</p>	La chiara definizione dei ruoli e delle responsabilità supporta l'attuazione del Programma sugli Obblighi di controllo dei Fornitori esterni.

<p>2. Segnalazione di violazione dei CID</p>	<p>Occorre implementare controlli e processi documentati per assicurare che qualsiasi violazione che ha ripercussioni sui CID sia segnalata e gestita.</p> <p>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 una procedura di risposta agli incidenti per la tempestiva gestione e regolare segnalazione degli eventi che riguardano i CID.</p> <p>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.</p> <p>Nel caso in cui il Fornitore esterno eroghi servizi di consulenza, e un dipendente di tale Fornitore abbia innescato incidenti per la prevenzione della perdita di dati, la Banca notificherà l'incidente al Fornitore e, se del caso, la Banca ha il diritto di richiedere la sostituzione del dipendente.</p>	<p>Un processo di risposta agli incidenti aiuta a garantire che vengano rapidamente circoscritti e che ne venga impedita l'escalation.</p> <p>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</p>
--	---	--

<p>3. Formazione e consapevolezza</p>	<p>I dipendenti del Fornitore che accedono ai CID e/o li gestiscono devono ricevere un'adeguata formazione* che copra i Requisiti di Segretezza bancaria dei CID dopo ogni modifica dei regolamenti o almeno una volta all'anno.</p> <p>Il Fornitore deve garantire che tutto il nuovo personale alle proprie dipendenze (che ha accesso ai CID e/o li gestisce), entro un periodo di tempo ragionevole (circa 3 mesi), completi un corso di formazione che garantisca la comprensione delle rispettive responsabilità rispetto ai CID.</p> <p>Il Fornitore deve tenere traccia dei dipendenti che completano la formazione.</p> <p>* le giurisdizioni che prevedono il segreto bancario forniscono le linee guida sui contenuti previsti per il corso di formazione.</p>	<p>Formazione e consapevolezza supportano tutti gli altri controlli nell'ambito di questo programma.</p>
<p>4. Schema di Etichettatura delle informazioni</p>	<p><i>Laddove appropriato*</i>, 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.</p> <p>I requisiti di gestione per i dati CID sono esposti nella Tabella E2 dell'Appendice E.</p> <p>* "<i>laddove appropriato</i>" fa riferimento al vantaggio derivante dall'etichettatura in rapporto al costo che comporta. Per esempio, non sarebbe appropriato etichettare un documento se, così facendo, si violassero i requisiti normativi antimanomissione.</p>	<p>Un inventario completo e accurato del patrimonio di dati è essenziale per garantire controlli appropriati.</p>

<p>5. Cloud Computing/Archiviazione esterna</p>	<p>L'uso del cloud computing e/o dell'archiviazione esterna dei CID (in server non ubicati nella giurisdizione che prevede il segreto bancario o esterni alle infrastrutture del Fornitore) nell'ambito di servizi resi per tale giurisdizione deve essere approvato dai corrispondenti team locali pertinenti (tra cui il Chief Security Office, Conformità e Legal); inoltre devono essere implementati i necessari controlli conformemente alle indicazioni della giurisdizione che prevede il segreto bancario pertinente per proteggere i CID rispetto al profilo ad alto rischio che presentano.</p>	<p>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</p>
---	--	---

Appendice C: Glossario

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

Termine	Definizione
CID	Client Identifying Data (Dati identificativi del cliente)
CIS	Cyber and Information Security (Sicurezza cibernetica e informatica)

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

Appendice D: DEFINIZIONE DI DATI IDENTIFICATIVI DEL CLIENTE

ICID Diretti (DCID) possono essere definiti come identificatori unici (di proprietà del cliente), che consentono, in quanto tali e di per sé, di identificare un cliente senza accedere ai dati contenuti nelle applicazioni bancarie di Barclays. Tali dati devono essere inequivocabili,

non soggetti a interpretazione e possono comprendere informazioni come nome, cognome, nome dell'azienda, firma, ID dei social network, ecc. I CID diretti si riferiscono a dati del cliente che non sono di proprietà della banca o creati da quest'ultima.

I CID Indiretti (ICID) sono suddivisi in 3 livelli

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

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

Gli L1 ICID Diretti e Indiretti non devono essere condivisi con persone esterne alla Banca e devono rispettare in qualsiasi momento il principio need-to-know. Gli L2 ICID possono essere condivisi sulla base del principio need-to-know ma non possono essere condivisi unitamente a qualsiasi altra parte di CID. Condividendo più parti di CID esiste la possibilità di creare una 'combinazione tossica' che potenzialmente potrebbe rivelare l'identità del cliente. Si crea una combinazione tossica con la combinazione di almeno due L2 ICID. Gli

L3 ICID possono essere condivisi poiché non sono classificati come informazioni a livello di Segreto Bancario a meno che l'uso ripetuto dello stesso identificatore possa dare luogo all'ottenimento di dati L2 ICID sufficienti a rivelare l'identità del cliente.

Classificazione delle informazioni	Segreto bancario			Riservata – Interna
Classificazione	CID diretto (DCID)	CID indiretto (ICID)		
		Indiretto (L1)	Potenzialmente indiretto (L2)	Identificatore impersonale (L3)
Tipo di informazione	Nome del cliente	Numero contenitore / ID contenitore	Luogo di nascita	Qualsiasi identificatore strettamente interno dell'applicazione di hosting/elaborazione del CID
	Nome della società	Numero MACC (conto liquidità soggetto a ID Contenitore Avaloq)	Data di nascita	Identificatore dinamico
	Estratto conto	ID SDS	Nazionalità	ID Party Role CRM
	Firma	IBAN	Carica in azienda	ID contenitore esterno
	ID social network	Dettagli di registrazione eBanking	Situazione familiare	

	Numero passaporto	Numero cassetta di sicurezza	Codice postale	
	Numero telefonico	Numero carta di credito	Condizioni di salute	
	Indirizzo e-mail	Messaggio SWIFT	Maggior valore di posizione/transazione	
	Qualifica lavorativa o PEP (Persona esposta politicamente)	ID Business Partner interno	Ultima visita cliente	
	Pseudonimo		Lingua	
	Indirizzo IP		Sesso	
	Numero fax		Data di scadenza CC	
			Contatto principale	
			Luogo di nascita	
			Data di apertura del conto	

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

1. Nome del cliente

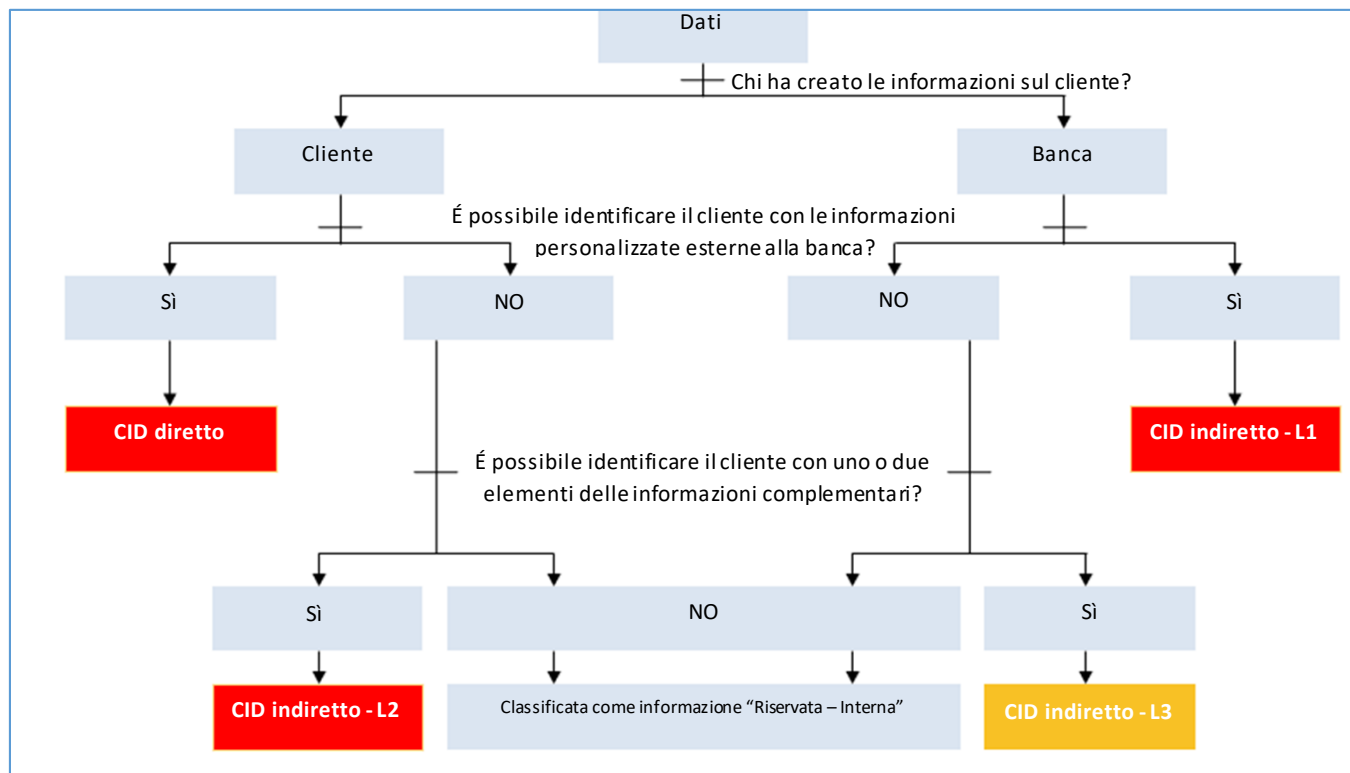
(DCID) = Violazione del segreto bancario

2. ID contenitore

(L1 ICID) = Violazione del segreto bancario

3. Condizioni di salute + Nazionalità

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



Appendice E: Schema di Etichettatura delle informazioni di Barclays

Tabella E1: Schema di Etichettatura delle informazioni di Barclays

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

Etichetta	Definizione	Esempi
Segreto bancario	<p>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.</p>	<ul style="list-style-type: none"> • Nome del cliente • Indirizzo del cliente • Firma • Indirizzo IP del cliente (altri esempi nell'Appendice D)

Etichetta	Definizione	Esempi
Segrete	<p>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).</p> <p>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.</p>	<ul style="list-style-type: none"> • Informazioni su potenziali fusioni e acquisizioni. • Informazioni di pianificazione strategica, a livello aziendale e organizzativo. • Determinate informazioni sulla configurazione di sicurezza. • Determinati risultati di audit e rapporti • Verbali dei comitati esecutivi • Dettagli di Autenticazione o Identificazione e verifica (ID&V) – cliente e collega. • Grandi volumi di informazioni sui titolari di carte. • Previsioni di profitto e risultati finanziari annuali (prima della divulgazione pubblica). • Qualsiasi punto che rientri nell'ambito di un Non-Disclosure Agreement (NDA) ufficiale.
Riservata – Interna	<p>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.</p> <p>La divulgazione non autorizzata potrebbe avere un impatto negativo su Barclays, valutato nell'ambito</p>	<ul style="list-style-type: none"> • Strategie e budget. • Stime delle performance. • Remunerazione dei dipendenti e dati personali. • Valutazioni di vulnerabilità. • Risultati di audit e rapporti.

	<p>dell'ERMF come "Principale" o "Limitato" (a livello finanziario o non finanziario).</p> <p>Queste informazioni non sono destinate alla diffusione generale ma possono essere inoltrate o condivise dai destinatari secondo il principio need-to-know.</p>	
Riservata – Esterna	<p>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.</p> <p>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).</p> <p>Queste informazioni non sono destinate alla diffusione generale ma possono essere inoltrate o condivise dai destinatari secondo il principio need-to-know.</p>	<ul style="list-style-type: none"> • Nuovi piani di prodotto. • Contratti con i clienti. • Contratti legali. • Informazioni relative a clienti singoli/a basso volume da inviare all'esterno. • Comunicazioni relative ai clienti. • Nuovi materiali per offerte (ad es. prospetti, promemoria per offerte). • Documenti di ricerca definitivi. • Informazioni essenziali non pubbliche (Material Non-Public Information - MNPI) esterne a Barclays. • Tutti i report di ricerca • Alcuni materiali di marketing. • Commenti del mercato.

Non riservate	Informazioni destinate alla diffusione generale o la cui divulgazione non avrebbe un impatto sull'organizzazione.	<ul style="list-style-type: none"> • Materiali di marketing. • Pubblicazioni. • Annunci pubblici. • Annunci di lavoro. • Informazioni che non influiscono su Barclays.
---------------	---	---

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

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

Fase del ciclo di vita	Requisiti del Segreto bancario
Creazione e Etichettatura	Come per "Riservata – Interna" e: <ul style="list-style-type: none"> • Ai patrimoni di dati deve essere assegnato un proprietario CID.
Conservazione	Come per "Riservata – Esterna" e: <ul style="list-style-type: none"> • 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.

	<ul style="list-style-type: none"> • 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	<p>Come per "Riservata – Esterna" e:</p> <ul style="list-style-type: none"> • 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.
	<ul style="list-style-type: none"> • 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	<p>Come per "Riservata – Esterna" e:</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Ai patrimoni di dati deve essere assegnato un proprietario delle informazioni. 	<ul style="list-style-type: none"> • Ai patrimoni di dati deve essere assegnato un proprietario delle informazioni. 	<ul style="list-style-type: none"> • Ai patrimoni di dati deve essere assegnato un proprietario delle informazioni.
Conservazione	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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.

			<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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.

		<ul style="list-style-type: none"> • I dati elettronici devono essere protetti mediante controlli Logical Access Management appropriati 	<ul style="list-style-type: none"> • I patrimoni di dati elettronici devono essere protetti mediante controlli Logical Access Management appropriati
Condivisione	<ul style="list-style-type: none"> • Le copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile. L'etichetta deve essere apposta per lo meno sulla copertina. • I patrimoni di dati elettronici devono essere corredati di chiara etichetta informativa. • I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione. 	<ul style="list-style-type: none"> • Le copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile. L'etichetta deve essere apposta per lo meno sulla copertina. • Le buste contenenti copie cartacee dei patrimoni di dati devono essere corredate di etichetta informativa visibile sul lato frontale. • I patrimoni di dati elettronici devono essere corredati di chiara etichetta informativa. Le copie elettroniche dei documenti di più pagine devono essere corredate di etichetta informativa visibile su ciascuna pagina. 	<ul style="list-style-type: none"> • 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.

	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione.• I patrimoni di dati devono essere distribuiti esclusivamente ai dipendenti dell'organizzazione o a individui vincolati a quest'ultima da un obbligo contrattuale appropriato o per assolvere a un'esigenza aziendale chiaramente riconosciuta, come una negoziazione contrattuale.• I patrimoni di dati devono essere distribuiti esclusivamente alle persone che hanno necessità di riceverli per motivi connessi alla loro attività.	<ul style="list-style-type: none">• I patrimoni di dati elettronici devono essere corredati di chiara etichetta informativa. Le copie elettroniche dei documenti di più pagine devono essere corredate di etichetta informativa visibile su ciascuna pagina.• I patrimoni di dati devono essere distribuiti esclusivamente tramite sistemi, metodi o fornitori approvati dall'organizzazione.• I patrimoni di dati devono essere distribuiti esclusivamente ai dipendenti dell'organizzazione o a individui vincolati a quest'ultima da un obbligo contrattuale appropriato o per assolvere a un'esigenza aziendale chiaramente riconosciuta, come una negoziazione contrattuale.
--	--	---	---

		<ul style="list-style-type: none"> • I patrimoni di dati non devono essere inviati via fax, a meno che il mittente non abbia verificato che i destinatari sono pronti a ritirare il fax. • Durante il transito al di fuori della rete interna, i patrimoni di dati elettronici devono essere criptati tramite un dispositivo di protezione crittografica approvato. 	<ul style="list-style-type: none"> • I patrimoni di dati devono essere distribuiti esclusivamente alle persone specificamente autorizzate a riceverli dal proprietario delle informazioni. • I patrimoni di dati non devono essere inviati via fax. • Durante il transito al di fuori della rete interna, i patrimoni di dati elettronici devono essere criptati tramite un dispositivo di protezione crittografica approvato. • Occorre implementare una catena di custodia dei patrimoni di dati elettronici.
Archiviazione ed eliminazione	<ul style="list-style-type: none"> • Le copie cartacee dei patrimoni di dati devono essere eliminate tramite un servizio di eliminazione riservato. 	<ul style="list-style-type: none"> • Le copie cartacee dei patrimoni di dati devono essere eliminate tramite un servizio di eliminazione riservato. 	<ul style="list-style-type: none"> • Le copie cartacee dei patrimoni di dati devono essere eliminate tramite un servizio di eliminazione riservato.

	<ul style="list-style-type: none">• Le copie dei patrimoni di dati elettronici devono essere cancellate in modo tempestivo anche dai "cestini" del sistema o da dispositivi analoghi.	<ul style="list-style-type: none">• Le copie dei patrimoni di dati elettronici devono essere cancellate in modo tempestivo anche dai "cestini" del sistema o da dispositivi analoghi.	<ul style="list-style-type: none">• 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.
--	---	---	---