Obblighi di controllo del Fornitore (SCO)

Requisiti di controllo della gestione -

Informazioni, Sicurezza informatica e fisica, Tecnologia, Pianificazione del ripristino, Riservatezza dei dati, Gestione dei dati ed EUDA

MC 1.0 - Governance e responsabilità

Il Fornitore deve disporre di un framework standard di settore consolidato e coerente per la governance di IT, Sicurezza IT, Sicurezza fisica, Pianificazione del ripristino, Gestione dei dati e Gestione delle informazioni personali (riservatezza e protezione dei dati), come NIST, ISO/IEC 27001, COBIT, BS10012, SSAE 18 o ITIL, oppure di un framework standard simile basato sulle migliori pratiche del settore, per garantire che le misure di protezione o le contromisure dei processi, della tecnologia e dell'ambiente fisico utilizzati siano collaudati per un funzionamento efficace. Un programma di governance aziendale ben strutturato deve garantire che i concetti fondamentali di disponibilità, integrità e riservatezza siano supportati da controlli adeguati. I controlli devono essere concepiti per mitigare o ridurre i rischi di perdita, interruzione o danneggiamento delle informazioni e il Fornitore deve garantire che i controlli dei requisiti di Barclays siano applicati e funzionino efficacemente, allo scopo di proteggere i servizi forniti a Barclays.

È necessario istituire un framework di governance, che deve includere misure di sicurezza amministrative, tecniche e fisiche per proteggere gli asset e le Informazioni o i dati da perdita, divulgazione, alterazione o distruzione accidentali e/o deliberate, furto, uso inappropriato o uso improprio, oltre che da accesso, uso o divulgazione non autorizzati.

Il programma di governance e responsabilità deve includere, a titolo di esempio non esaustivo, le aree seguenti:

- Policy di governance - È necessario definire una serie di policy di governance, che deve essere approvata dalla direzione, pubblicata e comunicata ai dipendenti del Fornitore e alle altre parti interessate, oltre che gestita adeguatamente.
    - Policy, procedure e programmi standard finalizzati alla creazione, all'implementazione e alla misurazione continua dell'efficacia delle policy e dell'implementazione degli standard.
    - Un programma di governance completo con una chiara struttura di leadership e una supervisione esecutiva per creare una cultura di responsabilità e sensibilizzazione.
    - Comunicazione continua delle policy e delle procedure approvate in tutta l'organizzazione.
    - Applicazione dei requisiti legali a policy e procedure, protezione dei dati per progettazione e altri controlli con lo scopo di garantire un'implementazione efficace di policy e processi.
- Le policy per tutte le aree del dominio devono essere riviste a intervalli pianificati, o in caso di modifiche significative, al fine di garantirne costantemente l'idoneità, l'adeguatezza e l'efficacia.
    - Verifica della regolare revisione di policy, procedure e standard (almeno una volta l'anno o in caso di cambiamento sostanziale, a seconda dell'evento che si verifica per primo).

- Nomina di una persona, o di persone/un team, in possesso di adeguata esperienza e qualifica professionale, con cui Barclays possa collaborare per quanto riguarda i requisiti SCO, compresi la sicurezza fisica e degli edifici, la sicurezza delle informazioni e dell'ambiente informatico, la gestione delle informazioni personali (privacy dei dati/protezione dei dati), la Pianificazione del ripristino e la Gestione dei dati. A tale persona, o tali persone/tale team verrà assegnata la responsabilità di una corretta implementazione e un efficace monitoraggio dei requisiti di controllo inerenti a Barclays o al Fornitore.
- Il Fornitore deve coordinare e allineare ruoli e responsabilità per il personale che implementa, gestisce e supervisiona l'efficacia dei controlli con i subappaltatori e i subresponsabili interni.

- Il Fornitore è tenuto a implementare un'infrastruttura sicura e un framework di controllo per proteggere l'organizzazione da qualsiasi minaccia (inclusa la Sicurezza Informatica).
- Il Fornitore dovrà istituire uno o più programmi di audit indipendente, per verificare se i controlli ascrivibili al Fornitore risultano di fatto implementati e mantenuti. Tale programma/Tali programmi dovranno essere eseguiti almeno una volta all'anno.

Indicazioni per il Cliente del Servizio Cloud (Fornitore)

È necessario definire una policy sulla sicurezza delle informazioni per il cloud computing, costituita da una policy specifica del Cliente del Servizio Cloud. La policy sulla sicurezza delle informazioni del Cliente del Servizio Cloud per il cloud computing deve essere coerente con i livelli accettabili di rischio per la sicurezza delle informazioni stabiliti dall'organizzazione per le sue informazioni e gli altri asset. Quando definisce i criteri di sicurezza delle informazioni per il cloud computing, il Cliente del Servizio Cloud deve tenere conto di quanto segue:

- Le informazioni memorizzate nell'ambiente di cloud computing sono accessibili e gestibili dal provider di servizi cloud.
- Gli asset, come i programmi applicativi, possono essere gestiti nell'ambiente di cloud computing.
- I processi possono essere eseguiti nell'ambito di un servizio cloud virtualizzato multi-tenant.
- Gli utenti dei servizi cloud e il contesto in cui utilizzano tali servizi.
- Gli amministratori dei servizi cloud che dispongono di accesso con privilegi al cliente del servizio cloud.
- Le ubicazioni geografiche dell'organizzazione del provider di servizi cloud e i Paesi in cui tale provider può archiviare i dati dei clienti del servizio cloud (inclusa la memorizzazione temporanea).

La Policy di sicurezza applicata dal cliente del servizio cloud deve identificare il provider di servizi cloud come tipo di Fornitore e gestirlo conformemente alla policy di sicurezza. nel tentativo di contenere i rischi introdotti dalla gestione e dall'accesso ai dati del Cliente del Servizio Cloud associati al provider di servizi cloud.

Il Cliente del Servizio Cloud deve considerare le leggi e le normative in vigore nelle giurisdizioni a cui è soggetto il provider di servizi cloud, oltre a quelle che disciplinano il Cliente del Servizio Cloud. Il Cliente del Servizio Cloud deve ottenere una prova della conformità del provider

di servizi cloud alle normative e agli standard applicabili richiesti per il business del Cliente del Servizio Cloud. Tali prove possono essere costituite anche da attestati o certificati rilasciati da revisori esterni.

In caso di fusione, acquisizione o qualsiasi altro cambiamento di proprietà dell'azienda del Fornitore, quest'ultimo è tenuto a inviare a Barclays una notifica scritta appena ciò sia legalmente possibile.

MC 2.0 - Gestione del rischio

Il Fornitore deve istituire un programma di gestione dei rischi con lo scopo di valutare, contenere e monitorare efficacemente i rischi in tutto l'ambiente controllato dal Fornitore.

Il programma di gestione dei rischi deve includere, a titolo di esempio non esaustivo, le aree seguenti:

- Il Fornitore deve disporre di un framework di gestione dei rischi opportunamente approvato (ad esempio Dati personali in caso di trattamento di dati PI, Informazioni, Ambiente informatico, Ambiente fisico, Tecnologia, Dati e Pianificazione del ripristino). Deve inoltre essere in grado di dimostrarne l'effettiva integrazione nell'ambito della strategia aziendale.
- In linea con il framework di gestione dei rischi, le valutazioni formali dei rischi devono essere eseguite almeno una volta l'anno o a intervalli pianificati, utilizzando un approccio basato sul rischio, o essere attivate in base agli eventi, ad esempio in risposta a un incidente o in funzione di quanto appreso dallo stesso, e in combinazione con le eventuali modifiche apportate ai sistemi informativi oppure agli spazi fisici o agli immobili, al fine di 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).
- Definizione e gestione di criteri di rischio che includono:
  - Criteri di accettazione del rischio
  - Criteri per l'esecuzione delle valutazioni del rischio
- Identificazione dei rischi:
  - Applicazione del processo di valutazione dei rischi per identificare i rischi associati alle violazioni in materia di riservatezza, integrità e disponibilità delle informazioni nell'ambito del framework di rischio
  - Identificazione dei responsabili dei rischi
- Analisi dei rischi:
  - Valutazione delle potenziali conseguenze dei rischi identificati
  - Valutazione della probabilità di concretizzazione dei rischi identificati
  - Determinazione dei livelli di rischio
- Valutazione dei rischi:
  - Confronto dei risultati dell'analisi dei rischi con i criteri di rischio stabiliti

    - Assegnazione delle priorità di gestione del rischio ai rischi analizzati
- Gestione del rischio:
    - Selezione delle opzioni appropriate per la gestione dei rischi, tenendo conto dei risultati della valutazione dei rischi.
    - Determinazione di tutti i controlli necessari per implementare le opzioni di gestione dei rischi selezionate.
    - Redazione di una Dichiarazione di applicabilità contenente i controlli necessari e la giustificazione per le inclusioni, siano esse implementate o meno.
    - Il Fornitore deve garantire che i rischi identificati nell'ambiente vengano minimizzati o eliminati attraverso l'assegnazione delle giuste priorità e l'implementazione delle contromisure necessarie. Il Fornitore deve monitorare costantemente l'efficacia delle contromisure.
- Il Fornitore deve eseguire come minimo una valutazione annuale dei rischi in relazione a Informazioni, Ambiente informatico, Sicurezza fisica, Gestione dei dati personali (Privacy dei dati/Protezione dei dati) e Pianificazione del ripristino. In caso di minacce attuali ed emergenti in ambienti specifici, il Fornitore deve prendere in considerazione una cadenza più frequente.
    - Valutazione, almeno una volta l'anno, delle sedi critiche per il funzionamento dei processi/servizi forniti a Barclays (inclusi i data center).
- L'organizzazione deve conservare le informazioni documentate sul processo di valutazione dei rischi per la sicurezza delle informazioni.
- Le valutazioni dei rischi associate ai requisiti di governance dei dati (compresi i Dati personali in caso di trattamento di dati PI) devono tenere conto di quanto segue:
    - 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.
    - Rispetto dei periodi di conservazione definiti e dei requisiti di smaltimento a fine vita.
- Il Fornitore, agendo in qualità di titolare o responsabile del trattamento, deve valutare i possibili rischi per la privacy durante l'elaborazione di dati sensibili o di grandi volumi di dati Barclays, al fine di garantire che eventuali modifiche nella gestione/nel trattamento dei dati Barclays non comportino i suddetti rischi.
- Il Fornitore deve sviluppare e implementare la struttura di governance organizzativa al fine di garantire la comprensione costante delle priorità di gestione del rischio per l'organizzazione, in base alle informazioni relative al rischio per la privacy.

MC 3.0 - Ruoli e responsabilità

Il Fornitore è responsabile di garantire che tutti i suoi dipendenti coinvolti nella fornitura di servizi a Barclays inclusi, a titolo di esempio non esaustivo, appaltatori, subappaltatori e subresponsabili, conoscano e rispettino i requisiti di controllo di Barclays. Il Fornitore deve garantire la disponibilità di un team adeguato, formato da specialisti e/o persone dotate competenze commisurate e appropriate, ruoli e responsabilità definiti per supportare e/o gestire i requisiti di controllo di Barclays, che operi per tutelare efficacemente i servizi di Barclays.

Il Fornitore è tenuto a definire e comunicare i ruoli e le responsabilità per il supporto efficace dei requisiti di controllo di Barclays. Tali ruoli le responsabilità devono essere rivisti regolarmente (e in ogni caso almeno una volta l'anno) e dopo ogni modifica rilevante del modello operativo o del business del Fornitore.

Il Fornitore è tenuto a garantire che i propri dipendenti, appaltatori, subappaltatori/subresponsabili conoscano a fondo e rispettino i requisiti di controllo del presente standard, oltre a quelli delle policy e dello standard associati. Il Fornitore deve nominare un Referente per la collaborazione con Barclays in caso di escalation dei problemi di conformità ai requisiti di controllo. I requisiti contrattuali specifici devono essere comunicati per iscritto ai subappaltatori/subresponsabili del Fornitore.

Indicazioni per il Cliente del Servizio Cloud (Fornitore)

Il cliente del servizio cloud deve concordare con il provider di servizi cloud l'assegnazione appropriata dei ruoli e responsabilità per la sicurezza delle informazioni, verificando che sia in grado di adempiere ai suddetti ruoli e responsabilità. I ruoli e le responsabilità di entrambe le parti devono essere indicati in un accordo. Il Cliente del Servizio Cloud deve identificare e gestire il proprio rapporto con la funzione di supporto tecnico e assistenza clienti del provider di servizi cloud.

Il cliente del servizio cloud deve definire o estendere le policy e le procedure esistenti, in funzione della sua modalità di utilizzo dei servizi cloud, e comunicare agli utenti del servizio cloud i propri ruoli e responsabilità in relazione all'uso del servizio cloud.

MC 4.0 - Educazione e sensibilizzazione

Il Fornitore deve implementare un programma continuativo di sensibilizzazione per tutti i suoi dipendenti, inclusi appaltatori, dipendenti a tempo determinato e consulenti. Tutti i dipendenti del Fornitore che lavorano per i servizi di Barclays e/o che hanno accesso a dati/informazioni o altri asset fisici di Barclays devono ricevere una formazione adeguata, oltre ad aggiornamenti periodici sulla sensibilizzazione in relazione alle procedure organizzative, alle policy e ai processi correlati alla rispettiva funzione professionale nell'ambito dell'organizzazione. I livelli di formazione e sensibilizzazione devono preparare i dipendenti del Fornitore a svolgere il proprio ruolo in modo sicuro, e garantire che questi ultimi comprendano le loro responsabilità durante l'accesso o il trattamento dei dati appartenenti a Barclays, compresi gli eventuali dati personali. I verbali del programma in corso devono essere registrati in una piattaforma appropriata per la gestione della formazione o tramite un processo manuale.

Il Fornitore deve garantire che tutti i suoi dipendenti completino i corsi di formazione e sensibilizzazione obbligatori, che devono includere Sicurezza informatica, Sicurezza fisica, Pianificazione del ripristino, Gestione delle informazioni personali (riservatezza e protezione dei dati), Gestione dei dati, Gestione dei servizi IT, EUDA e protezione dei dati Barclays, entro un mese dall'inserimento nell'organizzazione e/o dall'inizio della partecipazione ai servizi Barclays. Oltre ad aggiornare annualmente la formazione, il Fornitore deve assicurarsi di verificare che i propri dipendenti comprendano le proprie responsabilità e siano consapevoli dei rischi associati ai dati di Barclays, alle leggi e ai regolamenti applicabili, nonché di altri fattori che potrebbero influire sulla performance o mettere a rischio la banca. Tutta la formazione

erogata deve essere registrata e gestita per tutti i dipendenti del Fornitore che partecipano alla fornitura dei servizi Barclays. Deve essere inoltre disponibile per la consultazione da parte di Barclays quando richiesto.

Il Fornitore deve garantire che il suo programma di formazione sulla sensibilizzazione includa il rispetto degli argomenti relativi alla sicurezza informatica, come ingegneria sociale e minacce interne. Si consiglia al Fornitore di eseguire test di simulazione sugli attacchi di ingegneria sociale, utilizzando tecniche come le simulazioni di phishing, per tutti i dipendenti a livello aziendale, implementare un monitoraggio continuo per assicurarsi che la minaccia associata a tali rischi sia stata chiaramente compresa e mitigare i problemi identificati.

I gruppi ad alto rischio, come quelli che dispongono di accesso con privilegi al sistema, che accedono ad aree critiche o ad alto rischio oppure che svolgono funzioni aziendali sensibili (inclusi gli utenti con privilegi, come sviluppatori e tecnici di supporto, alti dirigenti, addetti alla sicurezza delle Informazioni e stakeholder esterni), devono ricevere una formazione supplementare sulla sensibilizzazione ai problemi di sicurezza delle Informazioni e sicurezza fisica, a seconda del proprio ruolo o responsabilità.

Tutto il Personale addetto alla sicurezza fisica (dipendenti del Fornitore, titolari di proprietà o Fornitori esterni) deve essere ingaggiato o impegnato contrattualmente tramite un fornitore di servizi accreditato e autorizzato ai sensi della legislazione locale e, ove richiesto dalla giurisdizione, essere personalmente autorizzato ad assumere obblighi di sicurezza. Il Personale addetto alla sicurezza fisica deve ricevere una formazione sulla sicurezza commisurata al proprio ruolo e alle proprie responsabilità. Tutta la formazione erogata deve essere documentata e, su richiesta, deve essere conservato un verbale della formazione per tutto il personale addetto alla sicurezza, che deve rimanere a disposizione per l'ispezione da parte di Barclays.

Il Fornitore deve garantire che il personale di terze parti avente accesso a dati contenenti informazioni personali sia a conoscenza dei rischi legati alla privacy e adempia ai propri doveri e alle proprie responsabilità in conformità con i numerosi elementi a ciò correlati: policy, processi, procedure, accordi e valori aziendali in termini di privacy. Tutta la formazione erogata deve essere documentata e, su richiesta, deve essere conservato un verbale della formazione per tutto il personale, che deve rimanere a disposizione per l'ispezione da parte di Barclays.

Il Fornitore deve formare i dipendenti in modo che siano in grado di svolgere efficacemente le proprie mansioni di gestione dei dati (gestione di dati critici o applicazioni gestite da terze parti).

Il titolare di EUDA presso il Fornitore deve identificare i dipendenti del Fornitore con responsabilità relative alle EUDA e assicurarsi che completino i corsi di formazione e sensibilizzazione adeguati al proprio ruolo almeno una volta l'anno, conservando le prove che dimostrano la conformità al controllo.

Indicazioni per il Cliente del Servizio Cloud (Fornitore)

Il Cliente del Servizio Cloud deve aggiungere gli argomenti che seguono ai programmi di sensibilizzazione, istruzione e formazione per i manager aziendali dei servizi cloud, gli amministratori dei servizi cloud, gli integratori di servizi cloud e gli utenti dei servizi cloud, inclusi i dipendenti e gli appaltatori interessati:

- Standard e procedure per l'uso dei servizi cloud.
- Rischi per la sicurezza delle informazioni associati ai servizi cloud e modalità di gestione dei suddetti rischi.
- Rischi associati all'ambiente di rete e ai sistemi utilizzati per i servizi cloud.
- Considerazioni legali e normative applicabili

I programmi di sensibilizzazione, istruzione e formazione sulla sicurezza delle Informazioni associati ai servizi cloud devono essere forniti al management e ai responsabili della supervisione, inclusi quelli delle Business Unit. Queste iniziative contribuiscono al coordinamento efficace delle attività di sicurezza delle Informazioni.

MC 5.0 - Gestione degli incidenti

Il Fornitore deve implementare un framework di gestione degli incidenti che consenta di gestire, contenere e rimuovere/mitigare efficacemente gli incidenti e le relative causa alla radice nell'ambiente del Fornitore.

Il Fornitore deve adottare una procedura per la Gestione di Incidenti e Crisi, che preveda un processo di escalation a Barclays per gli Incidenti e le Crisi. Il Fornitore deve garantire che i team e i processi di risposta a Incidenti e Crisi vengano testati, almeno una volta l'anno, per dimostrare la propria capacità di reagire in modo efficace ed efficiente in caso di Incidente. Il Fornitore deve inoltre verificare la propria capacità di informare, entro i tempi stabiliti, i contatti interessati da un incidente e dimostrarlo a Barclays quando richiesto.

Il Fornitore deve disporre di un piano ben documentato per la risposta agli Incidenti, che definisca i ruoli dei suoi dipendenti e le fasi di gestione degli incidenti:

- Responsabilità e procedure - Occorre definire responsabilità e procedure di gestione, al fine di garantire una risposta rapida, efficace e ordinata agli incidenti.
- Segnalazione degli incidenti - Gli incidenti devono essere segnalati al più presto possibile tramite i canali di gestione appropriati. Inoltre, il meccanismo di segnalazione deve essere semplice e accessibile a tutti i dipendenti e appaltatori del Fornitore.
- Valutazione degli incidenti - Gli incidenti devono essere valutati per determinarne la criticità, la classificazione e la risposta appropriate.
    - Classificazione degli incidenti - Occorre stabilire una scala di classificazione degli incidenti e decidere se un determinato evento deve essere classificato come incidente o meno. La classificazione e la definizione delle priorità degli incidenti possono contribuire a determinare l'impatto e l'entità di un incidente.

- Risposta agli incidenti - Gli incidenti devono ricevere una risposta conforme alle procedure di Gestione degli incidenti documentate del Fornitore.
    - Contenimento degli incidenti - Occorre utilizzare persone, processi e capacità tecnologiche per contenere in modo rapido ed efficace gli incidenti che si verificano nell'ambiente.
    - Rimozione/Mitigazione delle minacce - È necessario sfruttare le capacità di persone, processi e tecnologie al fine di rimuovere/mitigare in modo rapido ed efficace le minacce alla sicurezza e/o i relativi componenti nell'ambiente.
- Nozioni apprese dagli incidenti - Le informazioni acquisite durante l'analisi e la risoluzione degli incidenti devono essere utilizzate per ridurre la probabilità o l'impatto degli incidenti futuri.
- Raccolta di prove - Il Fornitore deve definire e applicare procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni utilizzabili come prova.

Attività successive agli incidenti - In caso di interruzione dei servizi Barclays, è necessario inviare a Barclays una **Relazione a posteriori sull'Incidente** entro massimo quattro **settimane di calendario** dal ripristino dei normali livelli operativi. Requisito minimo della Relazione a posteriori sull'Incidente:

- Eventi che hanno dato origine alla situazione.
- Modalità di gestione dell'Incidente o della Crisi.
- Analisi delle cause alla radice.
- Se il Fornitore o Barclays hanno classificato l'evento come "Evento a rischio" (vale a dire, se è stato giudicato sufficientemente rilevante e, di conseguenza, deve essere comunicato/inoltrato ai soggetti interessati conformemente alle policy applicabili note al Fornitore).
- Se costituisce un "Rischio comportamentale" (ad esempio se il Fornitore interagisce direttamente con i clienti di Barclays).
- Gli eventuali rimedi noti al Fornitore e applicati dai clienti di Barclays
- Il miglioramento continuo necessario per evitare che la situazione si ripresenti
- 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

Per quanto riguarda la Comunicazione, il Fornitore deve nominare un Referente responsabile di contattare Barclays in caso di incidente. Il Fornitore è tenuto a comunicare a Barclays i recapiti delle persone incaricate, e le eventuali variazioni, compresi i numeri di telefono e le persone da contattare al di fuori dell'orario di lavoro.

I dettagli devono includere: - Nome, responsabilità all'interno dell'organizzazione, ruolo, indirizzo e-mail e numero di telefono

Se, in qualsiasi momento, il Fornitore determina che un incidente influisce negativamente sui servizi, sui sistemi o sui dati di Barclays, dovrà comunicarlo immediatamente a Barclays.

Quando il Fornitore viene a conoscenza di un incidente informatico, anche mediante notifica da parte di un'entità Barclays, deve intervenire al più presto possibile, e in ogni caso entro il tempo massimo imposto dalla Legge applicabile o, in assenza di tale requisito, entro 48 ore dal momento in cui viene inizialmente a conoscenza dell'incidente informatico. In tale evenienza, deve informare Barclays inviando un'e-mail all'indirizzo gcsojoc@barclays.com e fornire tutte le informazioni pertinenti, tra cui, se possibile, (a) le categorie e il numero approssimativo dei record di dati Barclays interessati e, se applicabile, le categorie e il numero approssimativo dei soggetti interessati, (b) l'impatto e le probabili conseguenze dell'incidente informatico per Barclays e, se applicabile, per gli interessati e (c) le misure correttive e di contenimento che il Fornitore ha adottato o intende adottare.

In caso di furto, divulgazione o utilizzo non autorizzato di Dati personali protetti, sia esso effettivo, sospetto o presunto, dovuto a una protezione inefficace da parte delle misure di sicurezza del Fornitore (o di un suo Dipendente) oppure all'accesso non autorizzato ai Dati personali protetti da parte del, o tramite il, Fornitore (o il Personale del Fornitore), così come alla perdita di possesso o controllo, al danneggiamento o alla distruzione dei Dati personali protetti da parte del Fornitore o di un suo dipendente, o a qualsiasi altro trattamento non autorizzato dei Dati personali protetti, il Fornitore è tenuto a informare Barclays non appena possibile e, in ogni caso, entro 24 ore dal momento in cui viene a conoscenza dell'evento in questione, inviando un'e-mail all'indirizzo gcsojoc@barclays.com e fornendo a Barclays tutta la cooperazione e l'assistenza necessarie in relazione a tale evento, compresa la fornitura di tutte le informazioni rilevanti quali dati, orari, luogo, tipo di incidente, impatto, stato e misure di contenimento adottate.

Se per fornire il servizio viene utilizzato un subappaltatore o un subresponsabile del trattamento dei dati che dovrà trattare o entrare in possesso dei Dati, delle Informazioni o degli asset di Barclays, il Fornitore deve ottenere il consenso di Barclays. Il Fornitore deve stabilire un rapporto contrattuale con il subappaltatore/subresponsabile e garantire che quest'ultimo sia accreditato in base a un analogo framework di Migliori pratiche del settore basate sugli standard, al fine di garantire che opera in modo efficace per proteggere i dati e le informazioni di Barclays che deve elaborare e/o conservare. In caso di incidente con il subappaltatore/subresponsabile, è necessario garantire la segnalazione dell'incidente con le modalità sopra riportate.

Indicazioni per il Cliente del Servizio Cloud (Fornitore)

Il Cliente del Servizio Cloud deve verificare l'assegnazione delle responsabilità relative alla gestione degli incidenti, assicurandosi che soddisfi i proprio requisiti. Il Cliente del Servizio Cloud deve richiedere al provider di servizi cloud le informazioni relative ai meccanismi da utilizzare nei casi seguenti:
- Segnalazione di un incidente/evento rilevato dal Cliente del Servizio Cloud al provider di servizi cloud.
- Segnalazione di un incidente/evento rilevato dal provider di servizi cloud al Cliente del Servizio Cloud.
- Monitoraggio dello stato di un evento di sicurezza delle informazioni segnalato, da parte del Cliente del Servizio Cloud.

MC 6.0 – Gestione degli asset IT (Hardware e Software)

Il Fornitore deve implementare e gestire un efficace programma di gestione degli asset per l'intero ciclo di vita degli stessi. La gestione degli asset deve controllarne il ciclo di vita dall'acquisizione alla dismissione e/o allo smaltimento sicuro, garantendo visibilità e sicurezza per tutte le categorie di asset presenti nell'ambiente.

Il Fornitore deve mantenere un inventario completo, accurato e aggiornato degli asset business-critical disponibili in tutte le sedi e/o ubicazioni geografiche che forniscono servizi a Barclays, incluse tutte le apparecchiature di Barclays ospitate nei locali del Fornitore, o di un suo subappaltatore/subresponsabile, o fornite da Barclays. Deve inoltre garantire lo svolgimento di almeno un test annuale con lo scopo di verificare che l'inventario degli asset informatici sia aggiornato, completo e accurato, quindi trasmettere i risultati a Barclays quando richiesto.

Il processo di Gestione degli asset deve coprire le aree seguenti:

- Inventario degli asset - Il Fornitore deve identificare tutti gli asset associati alle informazioni e alle strutture di trattamento, quindi redigere e conservare un inventario di tali asset.
    - Il Fornitore deve mantenere un inventario accurato e aggiornato di tutti gli asset hardware IT utilizzabili per memorizzare o elaborare le informazioni.
    - Il Fornitore deve disporre di un inventario degli asset informativi accurato e aggiornato per le apparecchiature Barclays ospitate nei propri asset IT e/o in quelli che fornisce a Barclays.
    - Se il Fornitore utilizza una configurazione di Livello 1, Livello 2 o Livello 3, deve mantenere un inventario aggiornato, completo e accurato degli asset (inclusi desktop, laptop, apparecchiature di rete, token RSA o qualsiasi altro asset fornito da Barclays).
    - Il Fornitore deve eseguire annualmente la riconciliazione di tutti gli asset di Barclays (Hardware e Software) e comunicare i risultati a Barclays (Chief Security Office - Team TPSecM).
    - Il Fornitore deve mantenere un inventario aggiornato di tutti i prodotti software implementati e autorizzati necessari per la fornitura dei servizi Barclays, rispettando i termini e le condizioni delle relative licenze.
    - L'inventario degli asset del Cliente del Servizio Cloud deve tenere conto delle informazioni e degli asset associati memorizzati nell'ambiente di cloud computing. I record dell'inventario devono indicare la posizione di conservazione degli asset, ad esempio identificando il servizio cloud.
- Uso accettabile degli asset - Il Fornitore deve identificare, documentare e implementare le regole per l'uso accettabile delle informazioni e degli asset associati alle strutture di trattamento de dati.
    - Occorre assicurarsi che gli asset non autorizzati vengano rimossi dalla rete.
    - Il Fornitore deve garantire l'implementazione di procedure efficaci ed efficienti per il contenimento delle tecnologie non supportate e per la fine del ciclo di vita, la dismissione e lo smaltimento sicuro di asset e dati, allo scopo di eliminare il rischio.
    - Occorre contrassegnare i Componenti hardware e software non supportati nel sistema dell'inventario.

- Restituzione degli asset - Tutti i dipendenti e i subappaltatori/subresponsabili del Fornitore (nell'ambito dei servizi Barclays) devono restituire tutti gli asset di Barclays in loro possesso al termine del loro rapporto di lavoro, contratto o accordo.
    - Gli asset di Barclays "smarriti o rubati" devono essere adeguatamente ricercati e segnalati a Barclays, come previsto dal controllo della gestione degli incidenti.
    - Lo "smarrimento o furto" di asset del Fornitore che contengono Informazioni di Barclays deve essere comunicato a Barclays come previsto dal controllo della gestione degli incidenti.

Il Fornitore deve tempestivamente avvisare Barclays quando viene a conoscenza di cambiamenti nella propria capacità di supporto, diretta o indiretta, per gli asset IT utilizzati ai fini della fornitura di servizi a Barclays, anche nel caso in cui tali prodotti presentino vulnerabilità di sicurezza, ed è tenuto a garantire l'upgrade o il ritiro tempestivo di tali asset IT.

Trasporto degli asset di Barclays - Il Fornitore deve assicurarsi che tutti gli asset e i Dati di Barclays vengano trasportati in modo sicuro, con controlli commisurati al valore degli asset e dei dati movimentati (considerando sia i potenziali danni economici che i danni alla reputazione), tenendo conto degli effetti del contesto di rischio in cui vengono trasportati.

Gestione del supporto (Fornitore)

Il Fornitore deve tempestivamente avvisare Barclays quando viene a conoscenza di cambiamenti nella propria capacità di supporto, diretta o indiretta, per gli asset IT utilizzati ai fini della fornitura di servizi a Barclays, anche nel caso in cui tali prodotti presentino vulnerabilità di sicurezza, ed è tenuto a garantire l'upgrade o il ritiro tempestivo di tali asset IT.

Il Fornitore deve assicurare che eventuali cambiamenti potenziali a livello di disposizioni chiave relative al supporto di terze parti siano identificati e comunicati a Barclays per gli asset interessati, al fine di garantire che le informazioni sul Prodotto siano mantenute perfettamente aggiornate.

Indicazioni per il Cliente del Servizio Cloud (Fornitore)

L'inventario degli asset del Cliente del Servizio Cloud deve tenere conto delle informazioni memorizzate nell'ambiente di cloud computing, così come degli asset associati. I record dell'inventario devono indicare la posizione di conservazione degli asset, ad esempio identificando il servizio cloud.

L'installazione di software commerciale su licenza in un servizio cloud può determinare una violazione delle condizioni di licenza del software. Il Cliente del Servizio Cloud deve disporre di una procedura che consenta di identificare i requisiti di licenza specifici per il cloud, prima di consentire l'installazione di qualunque software su licenza in un servizio cloud. È necessario prestare particolare attenzione ai casi in cui il servizio cloud è elastico e scalabile, poiché il software potrebbe essere eseguito su un numero di sistemi o core di processore superiore a quello consentito dalle condizioni di licenza.

MC 7.0 - Distruzione/smaltimento sicuro degli asset fisici e delle tracce residue delle informazioni elettroniche

La distruzione o la cancellazione sicura degli asset informativi di Barclays, comprese le immagini utilizzate per la manutenzione che vengono conservate in forma fisica e/o elettronica, devono essere eseguite con un metodo sicuro appropriato, verificando che i dati di Barclays non siano recuperabili.

Il Fornitore deve adottare procedure che supportino processi aziendali e misure tecniche finalizzati allo smaltimento sicuro, utilizzando metodi di sanificazione appropriati come, a titolo di esempio non esaustivo, la cancellazione, l'eliminazione e la distruzione per la rimozione/cancellazione sicura e il recupero dei dati di Barclays da tutti i supporti di archiviazione, in modo che i dati di Barclays risultino irrecuperabili con mezzi legali noti.

I dati di Barclays memorizzati nei supporti devono essere cancellati in modo da risultare irrecuperabili, utilizzando tecniche appropriate di cancellazione dei dati, come eliminazione, rimozione e cancellazione sicura dei dati, distruzione degli asset o un metodo software per la sovrascrittura dei dati. In alternativa è possibile utilizzare il framework standard di settore per lo smaltimento dei dati (NIST). Tutte le apparecchiature (asset informativi) devono essere smaltite al termine del loro ciclo di vita e/o della loro vita operativa (perché difettose, dismesse a causa della fine del supporto o non più necessarie, oppure utilizzate a scopo di valutazione o per una prova di concetto). Per le apparecchiature che devono essere riutilizzate e così via, è possibile utilizzare servizi di cancellazione dei dati.

I requisiti di smaltimento si applicano anche ai subappaltatori/subresponsabili del Fornitore utilizzati per fornire il servizio a Barclays.

Le informazioni cartacee devono essere smaltite tramite distruzione almeno secondo lo standard P4 DIN66399, utilizzando un tritadocumenti a taglio trasversale (incluse le informazioni sulle Carte di pagamento), oppure essere incenerite conformemente allo standard BS EN15713:2009.

Barclays richiede la conservazione delle prove dell'eliminazione dei dati, così come la fornitura di tracce di audit, evidenze e dati di tracciamento, che devono includere:

- Prova della distruzione e/o dello smaltimento (inclusa la data in cui sono stati eseguiti e il metodo utilizzato).
- Registri di controllo del sistema per la cancellazione.
- Certificati di smaltimento dati.
- Entità che ha effettuato lo smaltimento (compresi eventuali partner di smaltimento, terzi o appaltatori).
- Il Fornitore deve generare un report di distruzione e verifica che attesti l'esito positivo o negativo di qualsiasi procedimento di distruzione/eliminazione (ad esempio, un processo di sovrascrittura deve generare un report che fornisce informazioni dettagliate sui settori che non possono essere cancellati).

Al termine della fornitura dei servizi a Barclays, il Fornitore deve garantire che i dati di Barclays sono stati distrutti in modo sicuro, su richiesta e autorizzazione di Barclays.

Indicazioni per il Cliente del Servizio Cloud (Fornitore)

Il Cliente del Servizio Cloud deve richiedere al provider di servizi cloud di dimostrare l'applicazione delle policy e procedure per lo smaltimento o il riutilizzo sicuro delle risorse. Il Cliente del Servizio Cloud deve richiedere una descrizione documentata del processo di cessazione del servizio, che include la restituzione e la rimozione degli asset del Cliente del Servizio Cloud, seguita dall'eliminazione di tutte le copie di tali asset dai sistemi del provider di servizi cloud. La descrizione deve elencare tutti gli asset e documentare il programma di cessazione del servizio, che dovrebbe avvenire in modo tempestivo.

MC 8.0 - Classificazione delle informazioni e trattamento dei dati

Il Fornitore deve disporre di un framework o schema di classificazione delle informazioni e trattamento dei dati consolidato e appropriato (in linea con i requisiti delle Buone pratiche di settore e/o di Barclays), che copra gli aspetti seguenti:

- Classificazione delle informazioni - Le informazioni devono essere classificate in termini di criticità e sensibilità alla divulgazione o modifica non autorizzata.
- Etichettatura delle informazioni - Deve essere sviluppata e implementata una serie appropriata di procedure per l'etichettatura delle informazioni, conformemente allo schema di classificazione delle informazioni adottato dal Fornitore.
- Gestione degli asset - Devono essere sviluppate e implementate procedure di gestione degli asset, conformemente allo schema di classificazione delle informazioni adottato dal Fornitore.

Il Fornitore deve ugualmente garantire che tutto il personale sia a conoscenza dei requisiti di Etichettatura e trattamento applicati dal Fornitore e da Barclays, così come delle corrette modalità di classificazione delle informazioni.

Il Fornitore deve fare riferimento allo Schema di etichettatura delle informazioni di Barclays e ai requisiti di trattamento (Appendice A, Tabelle A1 e A2), o a uno schema alternativo, al fine di garantire la protezione e la sicurezza le informazioni di Barclays che elabora e/o conserva. Questo requisito si applica a tutti gli Asset informativi conservati o elaborati per conto di Barclays, anche tramite subappaltatori e subresponsabili.

Indicazioni per il Cliente del Servizio Cloud (Fornitore)

Il Cliente del Servizio Cloud deve etichettare le informazioni e gli asset associati che vengono gestiti nell'ambiente di cloud computing, conformemente alle procedure di etichettatura adottate dal Cliente del Servizio Cloud. Ove applicabile, è possibile adottare le funzionalità di supporto dell'etichettatura fornite dal provider di servizi cloud.

MC 9.0 - Backup dei dati/delle informazioni

Il Fornitore deve disporre di un adeguato processo di Backup dei dati, per garantire che l'infrastruttura venga regolarmente sottoposta ad accurate procedure di backup, al fine di prevenire la perdita di dati. Le informazioni memorizzate in formato elettronico vengono sottoposte a backup per essere mantenute al sicuro in caso di guasti del sistema, disastri o incidenti. I piani di backup devono essere sviluppati, testati e implementati in modo da risultare pienamente conformi alla policy specifica applicata in materia di backup.

Nel piano di backup si devono tenere in debita considerazione i seguenti elementi:

- Definizione dei requisiti di backup - I requisiti inerenti al backup dei dati vengono chiaramente definiti, registrati e concordati con l'azienda
- Creazione di record accurati e completi in relazione alle copie di backup effettuate, con opportuna documentazione inerente alle procedure di ripristino.
- Frequenza di backup (ad esempio, backup completo o differenziale)
- Archiviazione sicura dei backup
    - archiviazione in un luogo remoto, sicuro e protetto, a una distanza sufficiente per evitare eventuali danni causati da un evento disastroso nel sito principale.
- Test regolari dei dispositivi di backup, per garantire la loro affidabilità e il conseguente utilizzo in caso di emergenza, quando necessario. Test relativo alla capacità di ripristinare i dati di backup su un apposito sistema di test, senza sovrascrivere il dispositivo di archiviazione originale nel caso in cui il processo di backup o ripristino fallisca e causi danni o perdite irreparabili dei dati.
- Prima dell'esecuzione del backup occorre assicurarsi che vengano rilevate eventuali perdite accidentali di dati.
- Verificare che il backup sia adatto allo scopo

Assicurarsi che i backup siano adeguatamente protetti tramite sicurezza fisica e/o crittografia, sia quando vengono archiviati, sia durante il loro trasferimento attraverso la rete o le varie sedi. Sono compresi i backup remoti e i servizi cloud.

Assicurarsi che il backup di tutti i dati Barclays venga regolarmente eseguito in base agli specifici requisiti del servizio.

Se il provider di servizi cloud fornisce funzionalità di backup come parte del servizio cloud, il Cliente del Servizio Cloud deve richiedere le specifiche della funzionalità di backup al provider di servizi cloud. Il Cliente del Servizio Cloud deve inoltre verificare che tale funzionalità soddisfi i propri requisiti di backup. Se il provider di servizi cloud non fornisce funzionalità di backup, il Cliente del Servizio Cloud è responsabile di implementarle.

Il Fornitore deve garantire che tutti i sistemi e servizi IT utilizzati per la fornitura di servizi a Barclays dispongano di processi di backup e ripristino adeguati e funzionanti, in linea con le esigenze di Barclays, la cui efficienza deve essere comprovata periodicamente.

Il Fornitore deve garantire che tutti i dispositivi di backup associati alla fornitura di servizi a Barclays, così come le disposizioni per la gestione e la conservazione di tali dispositivi, siano sempre sicuri e affidabili.

MC 10.0 - Gestione delle configurazioni

Il Fornitore deve definire e implementare appositi processi e strumenti per applicare le configurazioni stabilite (comprese le configurazioni di sicurezza) per hardware, software, servizi (inclusi i servizi cloud) e reti, sia per i sistemi appena installati che per i sistemi già operativi, durante il loro ciclo di vita.

Gestione delle configurazioni - Il Fornitore deve disporre di una serie di configurazioni approvate e testate per hardware, software e reti. Le stesse devono essere opportunamente registrate; occorre inoltre mantenere un registro di tutte le modifiche apportate alle configurazioni. Tali record devono essere conservati in modo sicuro. Ciò può essere realizzato in vari modi, ad esempio tramite database di configurazione o modelli di configurazione.

Monitoraggio delle configurazioni - Le configurazioni devono essere monitorate attraverso un set completo di strumenti di gestione del sistema (ad esempio, utility di manutenzione, supporto remoto, strumenti di gestione aziendale, software di backup e ripristino) e devono essere riviste regolarmente per verificare le impostazioni di configurazione, valutare la robustezza delle password e le attività eseguite. Le configurazioni effettive possono essere confrontate con i modelli target definiti in precedenza. Le eventuali discordanze devono essere risolte mediante l'applicazione automatica della configurazione target predefinita o attraverso l'analisi manuale della difformità rilevata, seguita da opportune azioni correttive.

Mantenimento di un registro dei Componenti della configurazione - Il Fornitore deve mantenere un registro completo e accurato di tutti i Componenti della configurazione che influiscono sull'erogazione dei servizi a Barclays (comprese la titolarità e le dipendenze/mappature upstream e downstream). Il Fornitore deve provvedere a controlli atti a garantire il mantenimento costante dell'accuratezza e della completezza dei dati.

Isolamento dell'ambiente di produzione - Il Fornitore deve garantire che i servizi di produzione erogati a Barclays non dipendano da eventuali componenti non produttivi, al fine di evitare la realizzazione di servizi inaffidabili o non sicuri.

Configurazione sicura - Il Fornitore deve disporre di un framework consolidato per garantire che tutti i sistemi/apparecchiature di rete configurabili siano configurati in modo sicuro, conformemente alle Migliori pratiche del settore (ad esempio NIST, SANS, CIS).

- Definizione di policy, procedure/misure organizzative e strumenti per consentire l'implementazione degli standard di configurazione della sicurezza secondo le Migliori pratiche del settore per tutti i dispositivi di rete e i sistemi operativi, le applicazioni e i server autorizzati.
- Esecuzione di controlli regolari (almeno una volta l'anno) dell'applicazione di quanto sopra al fine di garantire la risoluzione tempestiva dei problemi di conformità agli standard di sicurezza di base. Attuazione di controlli e procedure di monitoraggio appropriate al fine di garantire l'integrità di strutture e dispositivi.
- I sistemi e i dispositivi di rete sono configurati in modo da funzionare secondo i principi di sicurezza (ad esempio il concetto di limitazione dei controlli di porte, protocolli e servizi, nessun software non autorizzato, rimozione e disabilitazione degli account utente non necessari, modifica delle password di default degli account, rimozione del software non necessario, ecc.).
- Esecuzione di verifiche periodiche della configurazione, almeno una volta all'anno, per garantire che nell'ambiente di produzione effettivo non siano presenti configurazioni non autorizzate.
- Garantire che la gestione della configurazione regoli gli standard di configurazione sicura in tutte le classi di beni e che rilevi, avverta e risponda efficacemente alle modifiche o alle deviazioni della configurazione.

Indicazioni per il Cliente dei Servizi Cloud (Fornitore) utilizzato per la fornitura dei servizi a Barclays

Il Cliente dei Servizi Cloud (CSC, Cloud Service Customer) deve garantire l'implementazione di controlli di Configurazione sicura appropriati per salvaguardare il servizio Barclays.

- Quando configurano le macchine virtuali, i clienti dei servizi cloud devono verificare che gli aspetti appropriati siano stati potenziati (ad esempio, vengono utilizzati solo i protocolli, le porte e i servizi necessari) e che siano in vigore misure tecniche adeguate (ad esempio, anti-malware, registrazione) per ogni macchina virtuale utilizzata.

MC 11.0 Requisiti di sicurezza dell'Intelligenza Artificiale (IA)

Il Fornitore deve consultarsi con Barclays (Chief Security Office - Team TPSecM (externalcyberassurance@barclayscorp.com) qualora utilizzi strumenti di intelligenza artificiale per qualsiasi parte del ciclo di vita dei servizi e/o trattamento dei dati di Barclays.

Il Fornitore deve, qualora utilizzi l'intelligenza artificiale per qualsiasi parte del ciclo di vita dei servizi e/o tratti i dati di Barclays, gestire un sistema di gestione dell'intelligenza artificiale, finalizzato a documentare i processi/le procedure in base ai seguenti punti:

- Governance dell'IA - Il Fornitore deve definire e stabilire un quadro di governance per l'utilizzo degli strumenti di IA (compresi quelli di terze parti). Questo framework di governance deve garantire che gli strumenti di intelligenza artificiale siano progettati/implementati o integrati nei processi esistenti in modo da proteggersi da perdita di dati, danni al sistema, interruzioni del servizio e conseguenze normative. Un programma di governance ben strutturato deve garantire che i concetti fondamentali di disponibilità, integrità e riservatezza siano supportati da controlli adeguati. I controlli devono essere concepiti per mitigare o ridurre

i rischi di perdita, interruzione o danneggiamento delle informazioni attraverso il Sistema di IA e il Fornitore deve garantire che i controlli di sicurezza di Barclays siano applicati e funzionino efficacemente, allo scopo di proteggere i dati e i servizi forniti a Barclays quando interagiscono con tale Sistema di IA.

- Sicurezza dell'IA - Il Fornitore deve definire e stabilire un quadro di sicurezza dell'IA che deve includere, a titolo esemplificativo ma non esaustivo, le seguenti aree:
  - Politiche in materia di Intelligenza Artificiale - Il Fornitore deve documentare una politica di Intelligenza Artificiale che descrive i requisiti per l'uso o lo sviluppo sicuro e responsabile di Sistemi di IA
  - Organizzazione interna - Il Fornitore deve assicurarsi di stabilire la responsabilità all'interno dell'organizzazione per sostenere un approccio responsabile all'implementazione, al funzionamento e alla gestione dei sistemi di IA.
  - Risorse per i sistemi di IA - Il Fornitore deve garantire che l'organizzazione tenga conto delle risorse (compresi i componenti e gli asset del sistema di IA) del sistema di IA al fine di comprendere e affrontare pienamente i rischi e gli impatti.
  - Dati per i sistemi di IA - Il Fornitore deve garantire che l'organizzazione comprenda il ruolo e gli impatti dei dati (compresi i dati di Barclays) nei sistemi di IA nell'applicazione e nello sviluppo, nella fornitura o nell'utilizzo dei sistemi di IA durante il loro ciclo di vita.
  - Informazioni per le parti interessate ai sistemi di IA - Il Fornitore deve garantire che tutte le parti interessate (compresa Barclays) dispongano delle informazioni necessarie per comprendere e valutare i rischi del Sistema di IA e i relativi impatti (sia positivi che negativi).
  - Rapporti con terzi e con i clienti - Il Fornitore deve garantire che l'organizzazione comprenda le proprie responsabilità e rimanga responsabile rispetto al Sistema di IA e che i rischi siano adeguatamente ripartiti quando sono coinvolti terzi in qualsiasi fase del ciclo di vita del sistema di IA.

EUDA - Laddove i servizi del Fornitore o la capacità o funzionalità dei prodotti del Fornitore forniti a Barclays utilizzino EUDA e l'IA sia implementata o impiegata per implementare o supportare tali EUDA, il Fornitore deve informare Barclays e garantire che l'utilizzo dell'IA non sia in conflitto con i requisiti EUDA SCO di Barclays.

Nota: Il requisito di controllo della sicurezza di cui sopra non è applicabile solo all'Intelligenza Artificiale (AI), ma anche all'apprendimento automatico (ML), poiché l'Intelligenza Artificiale e l'apprendimento automatico sono strettamente correlati e collegati. Il Fornitore deve implementare tutti i requisiti di controllo di cui sopra per l'utilizzo di strumenti di ML per qualsiasi parte del ciclo di vita dei servizi e/o per il trattamento dei dati di Barclays.

Definizione di IA/ML: L'Intelligenza Artificiale (IA) indica un sistema basato su macchine che è progettato per operare con un livello di autonomia e in grado, per una determinata serie di obiettivi, di generare output come previsioni, raccomandazioni o decisioni che influenzano ambienti fisici o virtuali. L'apprendimento automatico (ML) è un sottoinsieme dell'Intelligenza Artificiale (AI), che si riferisce alla capacità di una macchina di migliorare la propria prestazione attraverso l'esperienza e le iterazioni senza essere esplicitamente programmata con regole.

Un metodo, applicazione o strumento che rientra nella definizione di cui sopra viene definito come IA/ML se presenta caratteristiche dell'IA/ML[1] oppure utilizza un algoritmo IA/ML elencato[2].

1. Un metodo/applicazione/strumento ha caratteristiche di IA/ML se contiene parametri che vengono formati sui dati e l'adeguatezza di tali parametri non può essere valutata individualmente da un esperto in materia. Questo può essere dovuto all'elevato numero di parametri, alla complessità del calcolo o alla frequenza con cui vengono aggiornati. Ai fini di questa definizione, per "parametri" si intendono variabili numeriche nell'algoritmo che possono essere modificate per influenzarne il risultato; per "appropriatezza" si intende che il risultato del modello è adatto allo scopo dato il suo utilizzo; per "esperto in materia" si intende il proprietario del modello o lo sviluppatore del modello (se agisce come delegato per lo sviluppo del modello).

2. Gli algoritmi di IA/ML includono Bagging (random forest, ecc.), Boosting (GBM, XGBoost, ecc.), Clustering (K-means, DBSCAN, ecc.), Deep learning/neural network, Instance-based learning (KNN, ecc.), Regularized regression (ad esempio, Lasso, ridge), Reinforcement learning, Support vector machine.

Diritto di ispezione

Il Fornitore deve consentire a Barclays, su preavviso scritto di Barclays con almeno dieci (10) Giorni lavorativi di anticipo, di effettuare una verifica della sicurezza di qualsiasi tecnologia o sede utilizzata dal Fornitore o dai subappaltatori/subresponsabili per sviluppare, testare, migliorare, gestire o eseguire la manutenzione dei sistemi del Fornitore utilizzati per i Servizi, al fine di verificare il rispetto degli obblighi da parte del Fornitore nei confronti di Barclays. Il Fornitore deve inoltre consentire a Barclays di condurre un'ispezione almeno una volta l'anno, o subito dopo un incidente di sicurezza.

I rischi associati agli eventuali problemi di conformità individuati da Barclays durante l'ispezione devono essere valutati da Barclays, che indicherà le tempistiche per la relativa correzione. Il Fornitore è quindi tenuto a completare gli eventuali interventi correttivi entro tale periodo di tempo.

Il Fornitore deve fornire tutta l'assistenza ragionevolmente richiesta da Barclays in relazione all'ispezione e alla documentazione presentata durante l'ispezione. La documentazione deve essere compilata e restituita tempestivamente a Barclays. Il Fornitore deve inoltre fornire supporto a Barclays, tramite il responsabile della valutazione, e fornire le prove richieste durante qualsiasi verifica della sicurezza. Ciascuna Parte sosterrà i propri costi in relazione a qualsiasi revisione/audit/valutazione.

Appendice A: Schema di Etichettatura delle informazioni e Requisiti di trattamento dei dati di Barclays

Tabella A1: Schema di Etichettatura delle informazioni di Barclays

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

	Queste informazioni non sono destinate alla diffusione generale ma possono essere inoltrate o condivise dai destinatari secondo il principio need-to-know.	• Nuovi materiali per offerte (ad esempio 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	Le informazioni destinate alla diffusione generale o la cui divulgazione non avrebbe un impatto negativo sull'organizzazione devono essere classificate come Non riservate.	• Materiali di marketing • Pubblicazioni • Annunci pubblici • Annunci di lavoro • Informazioni che non influiscono su Barclays

Tabella A2: Schema di Etichettatura delle informazioni e requisiti di trattamento dei dati di Barclays

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

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

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

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

Appendice B: Definizioni

Per **Informazioni riservate di Barclays** si intendono tutte le informazioni ottenute dal o accessibili al Responsabile del Fornitore, al Fornitore o a qualunque dipendente del Fornitore in relazione alle presenti Condizioni generali e/o a qualunque Contratto relativo a qualsiasi (i) attività di business, prodotto e/o sviluppo di qualsiasi entità Barclays, passato, presente o futuro, e/o in relazione a (ii) dipendenti, clienti, controparti, Terze parti/Fornitori e/o appaltatori di qualsiasi entità Barclays (diversa dalle entità del Fornitore), compresa tutta la proprietà intellettuale di qualsiasi entità Barclays (anche in virtù di qualsiasi

Contratto) o di tali Fornitori/appaltatori di terze parti, Dati personali protetti, le presenti Condizioni generali, ciascun Modulo e ciascun Contratto, nonché le registrazioni mantenute ai sensi di qualsiasi Contratto e tutte le informazioni relative ai piani, ai prezzi, alle metodologie, ai processi, ai dati finanziari dell'entità o della persona interessata, ai Diritti di proprietà intellettuale, alle ricerche, ai sistemi, ai programmi e/o alle tecnologie informatiche;

Per **Dati Barclays** si intendono tutti i dati, le informazioni, il testo, i disegni e gli altri materiali incorporati con qualsiasi mezzo, compresi tutti i supporti elettronici, ottici, magnetici o materiali, che (i) sono accessibili al Fornitore in relazione a qualunque Contratto, (ii) vengono forniti al Fornitore da qualsiasi Entità Barclays oppure (iii) che vengono generati, raccolti, elaborati, archiviati o trasmessi dal Fornitore in relazione a qualsiasi contratto, esclusi i Materiali del Fornitore stesso.

Per **Sistemi Barclays** si intendono i sistemi informativi elettronici formati da uno o più componenti hardware, apparecchiature, software, periferiche e reti di comunicazione controllati, gestiti e/o utilizzati da, oppure appartenenti a, qualsiasi entità Barclays.

Per **Incidente informatico** si intende qualsiasi evento, inclusi gli eventi che si sono effettivamente verificati o per cui il Fornitore o Barclays ha ragionevolmente motivo di ritenere che si siano verificati (sulla base di una minaccia credibile, di un'indagine o di altre informazioni), che ha messo o potrebbe mettere a rischio (i) la riservatezza, l'integrità o la piena disponibilità dei Dati di Barclays oppure (ii) la riservatezza, l'integrità o la piena disponibilità e il normale funzionamento di un Sistema del Fornitore o di Barclays.

Incidente tecnologico - Interruzione non pianificata di un Servizio IT o riduzione della qualità di un Servizio IT, incluso, a titolo di esempio non esaustivo, il guasto di un Componente della configurazione che non ha ancora prodotto effetti negativi sul servizio. **Incidente maggiore** - Incidente che comporta un rischio/impatto significativo per Barclays e può produrre conseguenze gravi, come una grave perdita di produttività, danni reputazionali, conseguenze legali ed effetti negativi sui principali processi di business, sui controlli o sui sistemi chiave.

Per **Valutazione dell'impatto sulla protezione dei dati** si intende una valutazione dell'impatto prodotto dalle operazioni di trattamento previste relativamente alla protezione dei Dati personali, come richiesto dalle Normative in materia di Protezione dei dati.

Per **Normative in materia di Protezione dei dati** si intende, nella misura applicabile all'adempimento di qualsiasi obbligo del Fornitore ai sensi di qualunque Contratto: (i) la direttiva UE sulla privacy e le comunicazioni elettroniche 2002/58/CE (e successive modifiche o sostituzioni), (ii) il Regolamento generale sulla protezione dei dati della UE 2016/679 (**GDPR, General Data Protection Regulation**), le decisioni e le linee guida della Commissione europea e tutte le normative nazionali di attuazione, (iii) il GDPR del Regno Unito, (iv) le disposizioni del Gramm-Leach-Bliley Act relative alle Informazioni personali non pubbliche, (v) l'Health Insurance Portability and Accountability Act del 1996, e (vi) tutte le altre leggi, normative e linee guida ufficiali applicabili in materia di protezione e riservatezza dei dati in (a) qualsiasi giurisdizione in cui vengono adempiuti gli obblighi del Fornitore o in cui si trova l'entità Barclays in questione, la persona interessata in questione o qualsiasi Informazione personale protetta da trattare, archiviare o utilizzare e (b) qualsiasi giurisdizione da cui il Fornitore adempie ai propri obblighi ai sensi di qualsiasi Contratto.

Per **Obblighi di controllo della riservatezza dei dati** si intende qualsiasi programma in materia di privacy dei dati incluso nell'Allegato 7 (Obblighi di controllo dei fornitori esterni).

Il termine **Interessato** ha il significato ad esso attribuito dalle Normative in materia di Protezione dei dati. Nei casi in cui tale termine non sia definito dalle Normative in materia di Protezione dei dati, si intende una persona fisica che viene o può essere identificata, direttamente o indirettamente, soprattutto facendo riferimento a un identificatore come nome, codice fiscale, dati di localizzazione, identificatori online o a uno o più aspetti specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica.

Per **Buone pratiche di settore** si intende, in relazione a qualsiasi impresa e a qualsiasi circostanza, l'esercizio del massimo grado di competenza, diligenza, prudenza e previsione che ci si può ragionevolmente aspettare da una persona altamente qualificata ed esperta, impegnata nello stesso tipo di impresa, nelle stesse circostanze o in circostanze analoghe.

Il termine **Dati personali** ha il significato ad esso attribuito dalle Normative in materia di Protezione dei dati. Laddove tale termine non sia definito dalle Normative in materia di Protezione dei dati, si intende qualsiasi informazione relativa a un Interessato o che consente di identificarlo, direttamente o indirettamente.

Il termine **Violazione dei Dati personali** ha il significato ad esso attribuito dalle Normative in materia di Protezione dei dati. Laddove tale termine non sia definito dalle Normative in materia di Protezione dei dati, indica qualsiasi violazione della sicurezza che comporti la distruzione, la perdita, l'alterazione, la divulgazione o l'accesso accidentale o illegale a Dati personali trasmessi, archiviati o Elaborati in altro modo.

Il termine **Trattamento/Elaborazione** ha il significato ad esso attribuito dalle Normative in materia di Protezione dei dati. Laddove tale termine non sia definito dalle Normative in materia di Protezione dei dati, indica qualsiasi operazione o serie di operazioni eseguite sui Dati personali, anche in modo automatico, come (a titolo di esempio non esaustivo) la raccolta, la registrazione, l'organizzazione, l'archiviazione, l'adattamento, l'alterazione, il recupero, la consultazione, l'utilizzo, la divulgazione mediante trasmissione, diffusione o altra forma di rilascio, l'allineamento, la combinazione, il blocco, la cancellazione o la distruzione. In tali casi, i termini **Elaborazione** e **Trattamento** avranno il significato corrispondente.

Per **Subappaltatore** si intende qualsiasi terza parte che, di volta in volta, fornisce beni e/o servizi in relazione a: (a) fornitura di Prodotti, Servizi e/o Deliverable e/o (b) Trattamento o altro utilizzo dei Dati personali protetti, con le modalità consentite da un Contratto.

Per **Fornitore/Personale di terze parti** si intendono tutte le persone e/o le entità che svolgono qualsiasi parte dei Servizi, o forniscono un Prodotto ai sensi di qualsiasi Contratto, inclusi i dipendenti, i Subappaltatori e/o gli agenti del Fornitore o di uno qualsiasi dei suoi Subappaltatori.

Per **Sistemi del Fornitore/di terze parti** si intendono tutti i sistemi informativi elettronici (che possono includere uno o più componenti hardware, apparecchiature, software, periferiche e reti di comunicazione) che vengono, anche parzialmente: (i) utilizzati per fornire Prodotti o Servizi a qualsiasi Affiliata Barclays in connessione con un Contratto o (ii) gestiti, amministrati, monitorati o controllati dal Fornitore o da un suo Subappaltatore in connessione con un Contratto.

Per **Sistema** si intende qualunque sistema informativo elettronico (che può includere uno o più componenti hardware, apparecchiature, software, periferiche e reti di comunicazione) che venga utilizzato, anche parzialmente, per fornire beni o Servizi a qualsiasi Affiliata Barclays in connessione con un Contratto.