

REQUISITI DI CITI PER I FORNITORI

PROPRIETARI:

Responsabile di Citi Procurement & Risk

DATA DI EMISSIONE:

Gennaio 2015

AGGIORNAMENTO:

Settembre 2026

VERSIONE:

9

INDICE

1	PANORAMICA GENERALE.....	3
2	PARI OPPORTUNITÀ DI LAVORO.....	5
3	ANTI-CONCUSSIONE E CORRUZIONE (AB&C)	6
4	REGALI E INTRATTENIMENTO.....	6
5	RAPPORTI CON I FORNITORI E PRINCIPI PER I FORNITORI	7
6	DIVIETO DI SCHIAVITÀ MODERNA	7
7	PERSONALE DEL FORNITORE.....	9
8	GESTIONE DELLE FRODI	10
9	INTERAZIONE CON I MEDIA E APPARIZIONI PUBBLICHE	12
10	COMUNICAZIONI ELETTRONICHE SCRITTE	13
11	ATTIVITÀ E CONTRIBUTI POLITICI	13
12	ANTIRICICLAGGIO (“AML”)	14
13	GESTIONE DEI DOCUMENTI.....	16
14	RESILIENZA AZIENDALE/CONTINUITÀ DEL BUSINESS	17
15	GLOBAL BACKGROUND SCREENING STANDARDS	23
16	SPESE	25
17	SICUREZZA DELLE INFORMAZIONI	26
18	LINEE GUIDA SULLA SICUREZZA DEL POSTO DI LAVORO	64
19	INTELLIGENZA ARTIFICIALE/APPRENDIMENTO AUTOMATICO (INCLUDE L’INTELLIGENZA ARTIFICIALE GENERATIVA/L’INTELLIGENZA ARTIFICIALE AGENTICA).....	65
20	RECLAMI DEI CLIENTI.....	66
21	POLITICA DI TRADING E INVESTIMENTO PERSONALE	67
22	BILLING AND INVOICING STANDARDS	67
23	POLITICA SULLE ASSENZE OBBLIGATORIE.....	68
	APPENDICE - DEFINIZIONI.....	69

1 PANORAMICA GENERALE

1.1. Requisiti generali

I presenti requisiti di Citi per i fornitori ("**Requisiti**") descrivono in dettaglio alcuni degli obblighi che i fornitori devono rispettare nel corso delle loro attività commerciali con Citi. Alcuni requisiti sono validi per tutti i fornitori, mentre altri lo sono per un determinato fornitore a seconda del tipo di prodotto/i e servizio/i che fornisce a Citi (questi ultimi sono riassunti nella Sezione 1.2 qui sotto e sono indicati all'inizio di ciascuna disposizione ivi elencata). I termini in maiuscolo hanno il significato loro attribuito nel presente documento, compresa l'appendice allegata, a meno che tale significato non sia indicato nel presente documento, nel qual caso avranno il significato loro attribuito nel Contratto, come definito di seguito.

Questi requisiti rappresentano degli obblighi contrattuali nell'ambito degli accordi del Fornitore con Citi (inclusi, a titolo esemplificativo ma non esaustivo, i documenti transazionali, ad esempio ordini di lavoro, programmi di licenza) (ciascuno definito "**Contratto**") e sono in aggiunta a un qualsiasi obbligo specificato in un qualsiasi Accordo, un qualsiasi obbligo previsto dalla Legge del caso (termine che viene definito di seguito), un qualsiasi avviso da parte di Citi al Fornitore per informarlo dei propri obblighi ai sensi dello stesso (ciascuno definito "**Avviso**"), o di qualsiasi ulteriore requisito più specifico reso effettivo dalle attività o funzioni di Citi. In caso di conflitto tra uno qualsiasi dei requisiti di cui sopra e questi requisiti varranno gli obblighi e i requisiti più restrittivi. I Fornitori devono assumere un ruolo proattivo e consultarsi con il loro contatto commerciale principale all'interno di Citi (o persona designata) in merito a qualsiasi possibile domanda riguardante tali Requisiti, incluse eventuali modifiche, richieste di esenzione o qualsiasi conflitto percepito con essi o con la Legge applicabile.

Il Fornitore dovrà soddisfare tempestivamente qualsiasi richiesta ragionevole di dati che Citi presenti al Fornitore in relazione ai Servizi o al Personale del Fornitore in associazione con l'obbligo di Citi di rispettare la legge applicabile. Il mancato rispetto di tali obblighi da parte del Fornitore sarà considerato una violazione sostanziale dei termini del presente Contratto.

Il mancato rispetto di questi Requisiti o di eventuali ulteriori requisiti specificati da un centro Citi con cui il Fornitore intrattiene rapporti commerciali può comportare la risoluzione del Contratto del Fornitore con Citi. Le violazioni dei Requisiti possono costituire altresì delle violazioni della legge applicabile e comportare quindi risarcimenti per danni civili dovuti a Citi (o terze parti) o sanzioni penali per il Fornitore. Il Fornitore non può utilizzare la conformità alle proprie normative in sostituzione all'obbligo di rispettare le disposizioni dei presenti Requisiti senza il consenso scritto di Citi.

1.2. Requisiti applicabili a fornitori selezionati

Nella tabella seguente sono elencati alcuni Requisiti per determinati Fornitori che soddisfano i criteri di applicabilità ivi indicati. Le sezioni non menzionate di seguito riguardano TUTTI i Fornitori.

Sezione N.	Titolo della sezione	Applicabilità
2	PARI OPPORTUNITÀ IN AMBITO LAVORATIVO/AZIONE POSITIVA	Applicabile ai contratti e agli ordini di acquisto necessari per l'esecuzione di un contratto Citi con il governo federale degli

Sezione N.	Titolo della sezione	Applicabilità
		Stati Uniti; se esiste incertezza sul fatto che il contratto o l'ordine di acquisto costituiscano un subappalto o un ordine di acquisto del governo federale, includere "Se applicabile" all'inizio o alla fine della clausola, a seconda del caso.
12	ANTI RICICLAGGIO	Applicabile ai Fornitori che effettuano certi servizi relativi al cliente (ad es. inserimento di personale, monitoraggio dei conti e delle transazioni dei clienti) o forniscono dati/metriche relativi alle attività di cui sopra; E/O Ai Fornitori che agiscono da intermediari in relazione alla liquidità o agli strumenti finanziari (ad es. servizi di deposito a distanza, corriere, servizi di autoblindo o cassette di sicurezza).
13	GESTIONE DEI DOCUMENTI	Applicabile ai Fornitori che accedono/elaborano/archiviano le informazioni di Citi.
14	CONTINUITÀ DELL'ATTIVITÀ AZIENDALE	Applicabile ai Fornitori che erogano servizi o ospitano infrastrutture/applicazioni tecnologiche utilizzate da Citi. Il Titolare Citi Business Activity Owner (BAO) ha la responsabilità di comunicare l'applicabilità e i requisiti COB al Fornitore.
15	GLOBAL BACKGROUND SCREENING STANDARDS	Applicabile ai Fornitori che forniscono servizi a Citi.
16	SPESE	Applicabile ai Fornitori che hanno il diritto contrattuale di richiedere il rimborso delle spese aziendali.
17	SICUREZZA DELLE INFORMAZIONI	Applicabile ai Fornitori, compresi soggetti in subappalto, che hanno accesso / elaborano / gestiscono /conservano informazioni di Citi; <u>E/O</u> Fornitori responsabili in qualità di Host per le applicazioni Internet a marchio Citi; <u>E/O</u> Fornitori con connettività alle risorse di rete di Citi; <u>E/O</u> Fornitori che necessitano di accesso senza scorta alle strutture di Citi.
18	LINEE GUIDA SULLA SICUREZZA DEL POSTO DI LAVORO	
19	INTELLIGENZA ARTIFICIALE/APPRENDIMENTO AUTOMATICO (include l'intelligenza artificiale generativa/l'intelligenza artificiale agentic)	Applicabile ai Fornitori che utilizzano l'intelligenza artificiale/l'apprendimento automatico (AI/ML), secondo quanto definito da Citi per qualsiasi parte del prodotto/servizio che stanno fornendo.
20	POLITICA DI TRADING E INVESTIMENTO PERSONALE	Applicabile ai Fornitori che necessitano di un accesso regolare a MNPI come parte delle loro responsabilità lavorative presso Citi.
23	POLITICA SULLE ASSENZE OBBLIGATORIE	Questa Policy è applicabile ai non dipendenti ("Lavoratori") che detengono posizioni sensibili (come definito nel Glossario) ("Lavoratori sensibili"), nonché responsabili diretti e supervisori dei dipendenti sensibili ("Responsabili") e contatti aziendali di Citi dei non dipendenti sensibili.

2 PARI OPPORTUNITÀ DI LAVORO

2.1 Pari opportunità di lavoro.

Citi ha ideato un programma per garantire pari opportunità di lavoro a tutte le persone qualificate indipendentemente da razza, colore, religione, sesso, orientamento sessuale, identità di genere, origine, nazionalità, stato di immigrazione, età, stato civile, informazioni genetiche, disabilità, stato protetto di reduce di guerra o qualsiasi altro motivo protetto dalla legge.

I Fornitori devono rispettare e fare in modo che il loro personale si conformi ai requisiti di tutte le leggi e regolamenti applicabili in materia di non discriminazione, tra cui, a titolo esemplificativo ma non esaustivo, qualsiasi legge o regolamento che Citi notifichi per iscritto al Fornitore di dover rispettare.

I Fornitori dovranno esaminare e adottare le misure appropriate in linea con l'U.S. Equal Employment Opportunity Policy Statement, reperibile all'indirizzo www.citigroup.com/global/eeo-aa-policy.

2.2 Contratti governativi

I contratti e gli ordini di acquisto necessari per l'esecuzione di un contratto Citi con il governo federale devono contenere testualmente la seguente clausola in grassetto, come visualizzato di seguito. (In caso di dubbi sul fatto che si tratti di un subappalto/ordine di acquisto del governo federale, includere e aggiungere "Se applicabile" all'inizio della sezione).

[Se applicabile,] il Fornitore rispetterà tutte le leggi federali antidiscriminazione applicabili e certifica di non gestire alcun programma in violazione di alcuna legge federale antidiscriminazione applicabile.

2.3 Appendice dei Contratti governativi

I contratti e gli ordini di acquisto necessari per l'esecuzione di un contratto di Citi con il governo federale devono contenere il seguente avviso nell'appendice del subappalto o dell'ordine di acquisto. (In caso di dubbi sul fatto che si tratti di un subappalto/ordine di acquisto del governo federale, includere e aggiungere "Se applicabile" alla fine dell'avviso di seguito.)

In qualità di appaltatore del governo federale, Citigroup fornisce al sottoscritto appaltatore o Fornitore una notifica scritta dei nostri obblighi di pari opportunità di lavoro per conto dei reduci di guerra protetti e delle persone con disabilità. Citigroup rispetta pienamente la Sezione 503 del Rehabilitation Act e del Vietnam Era Veterans' Rejustment Assistance Act, nonché le normative applicabili ai sensi rispettivamente di 41 CFR § 60-741 e 41 CFR § 60-300. La nostra dichiarazione sulla politica delle pari opportunità di lavoro Equal Employment Opportunity Policy è disponibile all'indirizzo www.citigroup.com/global/eeo-aa-policy. Eventuali domande sui nostri obblighi di pari opportunità di lavoro possono essere indirizzate al contatto fornito nella nostra Policy Statement.

[Se applicabile] chiediamo di intraprendere azioni appropriate coerenti con la nostra Policy Statement e le normative.

3 ANTI-CONCUSSIONE E CORRUZIONE (AB&C)

Citi ha adottato policy, procedure e controlli interni ragionevoli per conformarsi alle leggi anticorruzione AB&C del caso e vieta severamente i pagamenti per corruzione o sollecitazione in qualsiasi forma. I Fornitori (compresi i Business Introducers), il loro personale o chiunque agisca per conto di Citi, direttamente o indirettamente, dovranno svolgere le proprie attività in conformità con i più elevati standard etici e in conformità con l'US Foreign Corrupt Practices Act (FCPA) degli Stati Uniti, l'UK Bribery Act (UKBA) britannico, ciascuna successiva modifica e tutte le altre leggi AB&C locali applicabili dei paesi in cui opera Citi.

Né il Fornitore, né alcuno del suo Personale, che opera per conto di Citi, o in relazione a qualsiasi accordo o rapporto del Fornitore con Citi, (i) effettuerà, conferirà, autorizzerà o offrirà pagamenti, benefici, vantaggi o qualsiasi altra cosa di valore a nessuna persona; o (ii) riceverà o accetterà pagamenti, benefici, vantaggi o qualsiasi altra cosa di valore da qualsiasi persona, in ciascuno dei casi (i)-(ii) in violazione dell'FCPA, dell'UKBA o di qualsiasi altra legge AB&C. Il Fornitore e il suo Personale devono condurre le proprie attività e transazioni per conto di Citi, o in relazione a qualsiasi accordo o rapporto del Fornitore con Citi, in conformità ai Requisiti applicabili inclusa questa Sezione. Il Fornitore e il suo Personale devono inoltre mantenere un programma di conformità AB&C e policy e procedure ideate e applicate per garantire la sua conformità a tutte le leggi AB&C.

Per una panoramica del Programma AB&C di Citi, visitare il sito [Investor Relations di Citigroup](#) (in Citi Policies, selezionare AB&C Program).

4 REGALI E INTRATTENIMENTO

I Fornitori e il loro personale non possono fornire doni od offrire alcunché di valore al personale di Citi (incluso l'intrattenimento), in quanto ciò creerebbe un conflitto di interessi effettivo o apparente, comprometterebbe l'integrità o il giudizio del dipendente o potrebbe comunque influire in modo inappropriato sulle sue decisioni, spingerlo ad agire in modo contrario alle sue funzioni o essere in altro modo in violazione delle leggi del caso. Senza limitare quanto sopra, il dipendente deve aderire alla Sezione Prohibited Gifts and Entertainment Section (Doni e intrattenimenti vietati) dello standard G&E. I Fornitori e il loro personale non devono offrire a nessun dipendente di Citi regali aziendali non in contanti superiori, in totale, a 300 dollari statunitensi per persona per anno solare.

Quando un Fornitore fornisce un'attività di intrattenimento aziendale (ad esempio, un invito al ristorante, un evento sportivo, culturale o altro) a un dipendente di Citi, il Fornitore deve partecipare all'evento e l'intrattenimento deve essere appropriato, consueto e ragionevole, non lussuoso o troppo frequente. Inoltre, se il Fornitore non è presente all'evento, l'intrattenimento sarà considerato un regalo aziendale e soggetto alle segnalazioni del caso previste nel Citi Gifts and Entertainment Standard. Il Fornitore non può, per conto di Citi o presumibilmente per conto di Citi, fornire oggetti di valore, anche a spese del Fornitore o di un dipendente di Citi, a nessuna persona, direttamente o

indirettamente, o indurre un'altra persona a fare lo stesso, se farlo sarebbe, o sarebbe ragionevolmente percepito, corrotto, inappropriato o in violazione della legge applicabile.

5 RAPPORTI CON I FORNITORI E PRINCIPI PER I FORNITORI

<https://www.citigroup.com/citi/suppliers/>Citi si impegna con i Fornitori su una serie di iniziative e per sensibilizzare i potenziali fornitori delle comunità in cui operiamo sul programma di approvvigionamento di Citi. Inoltre, tali iniziative mirano a individuare Fornitori promettenti, in particolare quelli che propongono soluzioni innovative per affrontare problematiche aziendali emergenti. Ulteriori informazioni sulle aspettative di Citi nei confronti dei fornitori sono disponibili sul sito [Doing Business with Citi](#) qui sotto:

[Citi Statement of Supplier Principles](#)
[Citi Sustainable Progress Strategy](#)

6 DIVIETO DI SCHIAVITÀ MODERNA

Citi si impegna a implementare pratiche volte a identificare e a cercare di prevenire il rischio che la schiavitù moderna e la tratta di esseri umani possano avvenire all'interno della sua organizzazione o in una delle sue catene di approvvigionamento. Tutti i Fornitori di Citi devono aderire ai Requisiti stabiliti di seguito e sviluppare policy, procedure e/o pratiche efficaci a livello aziendale per identificare e affrontare il rischio della schiavitù moderna e della tratta di esseri umani all'interno delle proprie operazioni e catene di approvvigionamento. I Fornitori sono tenuti a completare il questionario sulla responsabilità aziendale di Citi, su richiesta di Citi, oltre a fornire altre informazioni necessarie, per consentire a Citi di valutare l'esposizione al rischio e le potenziali misure di mitigazione, in particolare per i Fornitori nei settori e nelle aree geografiche a rischio più elevato. Ci si aspetta che i subappaltatori del fornitore seguano la stessa procedura.

6.1 Elusione del lavoro minorile

I Fornitori non devono impiegare manodopera minorile. Il termine "minore" si riferisce a qualsiasi persona di età inferiore all'età minima di impiego ai sensi delle leggi applicabili o, in assenza di tali leggi, ai soggetti di età inferiore a 15 anni o di età inferiore a quella prevista per il completamento dell'istruzione obbligatoria, a seconda di quale requisito preveda l'età più elevata. Fatto salvo il divieto assoluto di utilizzo del lavoro minorile, qualora siano impiegati lavoratori di età inferiore a 18 anni, si dovrà prestare particolare attenzione alle mansioni che svolgono e alle condizioni in cui sono tenuti a lavorare, per garantire che non subiscano danni fisici, mentali o di altra natura come conseguenza diretta o indiretta del loro lavoro o delle condizioni di lavoro.

6.2 Libera scelta dell'occupazione

Il Fornitore deve garantire che i lavoratori non siano obbligati, costretti mentalmente o fisicamente, legati, asserviti o sottoposti a lavoro involontario in carcere o a traffico di schiavi o sottoposti a lavoro obbligatorio in qualsiasi forma, compresi gli straordinari forzati. Qualsiasi lavoro deve essere eseguito volontariamente. Gli obblighi del Fornitore

ai sensi del presente documento includono, a titolo esemplificativo ma non esaustivo, la garanzia di quanto segue:

1. **Contratti, salari e orari di lavoro:** le condizioni di impiego o di assunzione dei lavoratori dovranno essere stabilite in un documento scritto che sia facilmente comprensibile e che stabilisca chiaramente i loro diritti e obblighi. Il presente documento scritto deve includere, a titolo esemplificativo ma non esaustivo, termini trasparenti in merito a salari, retribuzione degli straordinari, periodi di pagamento, orario di lavoro e diritti relativi a pause e ferie. Tali condizioni scritte dovranno essere fornite al lavoratore prima dell'inizio del lavoro, dovranno essere rispettate dal datore di lavoro, dovranno rispettare gli standard del settore e i requisiti minimi delle leggi e dei contratti collettivi del caso nel luogo in cui viene svolto il lavoro.
2. **Diritto di interrompere liberamente il lavoro:** i lavoratori devono avere il diritto di recedere liberamente dal loro rapporto di lavoro, ove opportuno, previo un preavviso ragionevole, in conformità alle leggi applicabili e ai contratti collettivi, e senza l'imposizione di sanzioni improprie.
3. **Trattamento disumano:** i lavoratori, le loro famiglie e le persone a loro strettamente associate non dovranno essere sottoposti a trattamenti duri o disumani, inclusi, a titolo esemplificativo ma non esaustivo, punizioni fisiche, violenza o coercizione fisica, psicologica o sessuale, abusi verbali, molestie o intimidazioni. I lavoratori migranti, le loro famiglie e le persone a loro strettamente associate non possono essere soggetti a discriminazioni nelle condizioni di lavoro a causa della loro nazionalità.
4. **Stipendi, benefici e orario di lavoro:** la retribuzione deve essere conforme a tutte le leggi salariali del caso, comprese quelle relative al salario minimo, alle ore di straordinario e ai benefit previsti dalla legge. I dipendenti devono essere pagati per intero, nei tempi previsti e con documentazione trasparente sulla retribuzione. Non vi saranno detrazioni di natura punitiva, né trattenute su salari o benefici come misura disciplinare. La durata delle settimane lavorative non deve superare il massimo stabilito dalla legge locale e gli straordinari devono essere volontari, entro limiti legali, e il rifiuto di lavorare negli straordinari non deve essere punito.
5. **Nessuna confisca dei documenti di identità:** ai lavoratori non dovranno essere confiscati o trattenuti i documenti d'identità o di viaggio, i passaporti o altri documenti ufficiali o altri oggetti di valore come condizione per l'impiego e il trattenimento di oggetti di proprietà non dovrà essere utilizzato, direttamente o indirettamente, per limitare la libertà dei dipendenti o per creare schiavitù sul posto di lavoro.
6. **Nessuna commissione di reclutamento o servitù per i debiti:** le commissioni o i costi associati all'assunzione dei lavoratori (inclusi, a titolo

esemplificativo ma non esaustivo, le commissioni relative ai permessi di lavoro, alle spese di viaggio e alle spese per il rilascio dei documenti) non saranno addebitati ai lavoratori, né direttamente né indirettamente. Analogamente, i lavoratori non saranno tenuti a effettuare pagamenti che abbiano la finalità o l'effetto di creare la schiavitù sul posto di lavoro, compresi i pagamenti di garanzia, né dovranno rimborsare un debito attraverso il lavoro. Se si accerta che tariffe o costi sono stati addebitati ai lavoratori in relazione al processo di reclutamento o sono stati sostenuti durante il corso del rapporto di lavoro, il Fornitore dovrà adottare misure ragionevoli per ottenere tempestivamente il rimborso di tali costi. Laddove sia necessario assumere lavoratori assunti tramite terzi, come ad esempio un'agenzia di collocamento, dovranno essere assunte solo agenzie di collocamento affidabili. Laddove i lavoratori vengano reclutati per essere assunti direttamente, devono essere coinvolte solo agenzie di reclutamento affidabili. Il divieto sulle commissioni di reclutamento pagate dai lavoratori si applica a tutti i reclutatori, agenti e subagenti. I Fornitori devono predisporre controlli che garantiscano la conformità. **Libertà di movimento:** I lavoratori devono essere liberi di muoversi senza restrizioni irragionevoli e non devono essere fisicamente confinati nel luogo di lavoro o in altri luoghi controllati dal datore di lavoro (ad esempio, blocchi di alloggi). I lavoratori non hanno l'obbligo di alloggiare in locali controllati dal datore di lavoro, salvo quando ciò sia necessario a causa del luogo o della natura del lavoro svolto.

7. **Reclami senza ritorsione:** i lavoratori saranno liberi di presentare rimostranze ai propri datori di lavoro in merito al trattamento riservato loro dal datore di lavoro e i lavoratori non devono subire danni, ritorsioni o vittimizzazione per aver presentato una rimostranza.

7 PERSONALE DEL FORNITORE

7.1 Formazione, assegnazione, nuova assegnazione e gestione del personale del Fornitore.

Il fornitore utilizzerà un numero adeguato di individui con formazione, istruzione, esperienza e abilità adeguate per eseguire i Servizi nel modo più efficace e coerente con qualsiasi Contratto e dimostrerà, su richiesta, le qualifiche di tali individui. Una volta che il Personale è stato assegnato a un Progetto, il Fornitore non riassegnerà né utilizzerà alcun Personale per altre questioni che riducano la sua disponibilità a lavorare sul Progetto senza il previo consenso scritto di Citi e generalmente assegnerà il Personale ai Progetti in modo da ridurre al minimo le interruzioni causate dalla necessità di riorientamento. Il Fornitore garantirà che il proprio Personale non si spacci per dipendenti o agenti di Citi, né cerchi di essere trattato come dipendente di Citi per alcun motivo, comprese le rivendicazioni di diritto a benefit forniti da Citi, o per reddito di invalidità, imposte o benefici della previdenza sociale, imposte statali sulla disoccupazione, sussidi di disoccupazione statali o ritenute fiscali statali sul reddito. Il fornitore è l'unico responsabile di tutte le responsabilità relative al datore di lavoro per quanto riguarda il suo personale, tra cui, ma non solo, il mantenimento di tutte le coperture assicurative richieste, il deposito di tutte le dichiarazioni fiscali applicabili e l'esecuzione di tutti i

pagamenti e depositi fiscali richiesti in modo coerente con lo stato del fornitore come appaltatore indipendente.

7.2 Sostituzione del Personale del Fornitore

Il Fornitore rimuoverà e sostituirà il Personale assegnato dal Fornitore a un Progetto qualora Citi notificchi al Fornitore che tale persona è inaccettabile per Citi per un qualsiasi motivo che non sia di natura discriminatoria. Il fornitore accetta inoltre di rimuovere e sostituire qualsiasi Personale assegnato a un Progetto e di impedirgli di fornire Servizi a Citi (o da qualsiasi responsabilità in relazione alla consegna o alla supervisione dei Servizi) qualora non sia in grado o non voglia fornire i Servizi in modo tempestivo e professionale.

7.3 Supplier's Personnel Policies

Il fornitore dichiara, garantisce e concorda di mantenere e gestire in modo efficace policy e procedure esaustive per la qualificazione dei propri dipendenti che sono persone fisiche e che sono destinati a fornire Servizi in loco a Citi, e che tali policy e procedure includono la verifica dell'autorizzazione al lavoro, il controllo dei precedenti lavorativi e delle condanne penali, come ulteriormente indicato nel presente documento, e il test antidroga pre-assunzione, il tutto nella misura consentita dalla Legge applicabile e da qualsiasi contratto collettivo di lavoro applicabile. Fatto salvo quanto precede, il Fornitore dichiara, garantisce e si impegna inoltre a fornire controlli e procedure per garantire la piena conformità del Fornitore a tutte le Leggi applicabili in materia di immigrazione, inclusa la convalida che tutto il Personale del Fornitore assegnato a Citi sia autorizzato a lavorare per tutta la durata dell'incarico nel pieno rispetto di tutte le Leggi applicabili in materia di immigrazione. Su richiesta, il fornitore fornirà tempestivamente a Citi la prova scritta dell'autorizzazione al lavoro per tutto il personale del fornitore assegnato a Citi e la sua conformità alla Legge applicabile in materia di immigrazione e sostituirà il Personale che non abbia l'autorizzazione al lavoro in conformità con la Legge applicabile con altro personale adeguatamente qualificato, fornendo anche tutta la formazione e l'orientamento necessari per garantire la fornitura tempestiva ed efficace dei Servizi, in ogni caso senza costi aggiuntivi per Citi.

7.4 Proprietà del Fornitore

Per rispettare le leggi e i regolamenti applicabili nelle giurisdizioni in cui Citi svolge le proprie attività, su richiesta di Citi, i Fornitori sono obbligati a fornire i dettagli dei proprietari, che siano una persona fisica e/o un'entità, compresi i proprietari immediati del Fornitore fino a, e incluso, il titolare effettivo finale che detiene la proprietà o il controllo, direttamente o indirettamente tramite la propria influenza o con altri mezzi, sull'incarico, sul prodotto o sul servizio.

8 GESTIONE DELLE FRODI

In connessione con gli sforzi di Citi per identificare e mitigare il rischio di frode ("Gestione delle frodi").

8.1 Tutti i Fornitori sono tenuti a:

1. Cooperare con qualsiasi indagine di Citi su fatti sospetti o presunti di furto, frode o altre potenziali attività criminose o illecite e qualsiasi accusa di

comportamento fraudolento o criminoso nella massima misura prevista dalla legge;

2. Garantire un tempestivo resoconto e la segnalazione di eventuale e potenziale frode a Citi tramite la linea diretta [Ethics Hotline](#). Ciò include, a titolo esemplificativo ma non esaustivo, furti tentati, sospetti, presunti o effettivi, frodi (ad es. invio di dati consapevolmente falsi, inesatti o travisati relativi al Fornitore, schemi di fatturazione, scomparsa di fondi o titoli, ecc.), reati o azioni illecite che coinvolgano Citi, un dipendente di Citi, un Fornitore o agente di Citi o un dipendente di aziende diverse da Citi (ad es. dipendenti a tempo determinato e appaltatori);
3. Permettere il monitoraggio e la supervisione da parte di Citi e dei suoi rappresentanti e sostenere Citi, e le forze dell'ordine, durante le indagini su potenziali attività fraudolente che coinvolgono quel Fornitore;
4. Segnalare tempestivamente eventuali conflitti di interesse (inclusi i conflitti di interesse tra Fornitori/Dipendenti Fornitori e/o Dipendenti Citi) di cui i Fornitori vengano a conoscenza; e
5. Supportare i processi di prevenzione delle frodi di Citi durante l'impostazione o l'aggiornamento del conto bancario di un fornitore nel sistema di pagamento dei Fornitori di Citi.

8.2 Inoltre, i Fornitori che forniscono servizi intrinsecamente più esposti al rischio di frodi sono **tenuti** a:

1. Documentare e seguire un Programma di gestione dei rischi di frode che identifica i rischi di frode relativi ai servizi che forniscono a Citi, i controlli e le procedure in atto per mitigare tali rischi;
2. Completare il corso di formazione sulla consapevolezza sulle frodi (entro 90 giorni di calendario dall'assunzione e successivamente annualmente) e addestrare il personale su elementi specifici dei rischi di frode relativi ai servizi specifici forniti a Citi.
3. Monitorare le istanze di tentativi di frode e mantenere controlli efficaci per mitigare il rischio di frode in relazione ai servizi che forniscono a Citi, documentare le procedure per i controlli e testare l'efficacia dei controlli su base continuativa, segnalando eventuali carenze al Titolare dell'attività commerciale (Business Activity Owner, BAO).
4. Fornire al titolare dell'attività (Business Activity Owner, BAO) tutte le informazioni necessarie per la due diligence/il monitoraggio/la valutazione dell'esposizione al rischio di frode.
5. La due diligence include il modello di valutazione Third-Party Fraud Impact Assessment Template ("TP-FIAT"), ideato per eseguire valutazioni di controllo dei Fornitori in relazione alla mitigazione del rischio di frode. La presente procedura operativa descrive una serie di passaggi che devono essere rispettati dal Business Activity Owner (BAO) o dal Third-Party Officer (TPO) e dal Fraud Risk Management Officer ("FRMO") per identificare e gestire il rischio di frode.

8.3 I fornitori con un rischio di frode intrinseco più elevato includono, senza limitazioni, quelli che:

1. hanno accesso a dati classificati come riservati o di livello superiore (quando non sono sotto il diretto controllo o la supervisione di Citi) che possono essere utilizzati per frodi quali l'accesso a conti interni, transazioni finanziarie, transazioni in contanti.
2. avere connettività alle reti/sistemi Citi; e
3. fornire, supportare o avere accesso a servizi e funzionalità che potrebbero essere mirati a commettere o consentire frodi, tra cui:
 - a) Identificazione, on-boarding o elaborazione delle domande di nuovi clienti.
 - b) Attività di pagamento/trasferimento di fondi di Citi o del cliente e/o autenticazione dei clienti di Citi per accedere a questi servizi;
 - c) Apporto, controllo o implementazione di modifiche dei dati di Citi o dei clienti di Citi (ad es. dati demografici);
 - d) Fornitura, manutenzione o autorizzazione di strumenti transazionali (ad es. carte di debito/credito, eWallet, libretti degli assegni, ecc.);
 - e) Fornitura o supporto di attività operative di gestione delle frodi a Citi, relative alla prevenzione, all'individuazione o alla risposta a casi di frode.
 - f) Fornire accesso fisico a denaro contante, strumenti finanziari e risorse/beni fisici;
 - g) Accesso senza scorta o fuori orario alle strutture Citi;
 - h) Bilanci: attività contabili, come la registrazione delle voci nel GL/SL;
 - i) Ricezione e distribuzione di premi per attività incentivate.

9 INTERAZIONE CON I MEDIA E APPARIZIONI PUBBLICHE

Citi Enterprise Services and Public Affairs è l'unico dipartimento autorizzato a rilasciare comunicati stampa o dichiarazioni pubbliche per conto di Citi. I fornitori non possono emettere comunicati stampa che identifichino direttamente o indirettamente Citi, alcun Contratto o accordo tra un Fornitore e Citi o qualsiasi prodotto e servizio acquistato da Citi presso un Fornitore. I Fornitori non possono acconsentire o intraprendere alcuna attività di pubbliche relazioni relativa a Citi con Clienti, dipendenti di Citi, altri Fornitori di Citi, altri clienti di Fornitori o qualsiasi altra terza parte senza previa approvazione scritta da parte del loro principale contatto commerciale di Citi.

I Fornitori non possono pubblicare o postare materiale in forma scritta o elettronica (inclusi libri, articoli, podcast, webcast, blog, pubblicazioni su siti web, foto, video, social media o altri media), tenere discorsi, concedere interviste o fare apparizioni pubbliche che menzionino Citi, le operazioni, i clienti, i prodotti o i servizi di Citi, senza previa approvazione scritta del loro principale referente aziendale di Citi e l'alto funzionario per gli affari pubblici a livello nazionale.

Che sia o meno nell'ambito della fornitura di servizi o di prodotti a Citi, i fornitori non potranno utilizzare alcun indice, marchio commerciale, marchio di servizio, nome

commerciale, logo, simbolo o nome di marchio esclusivi di Citi, senza, in ogni caso, il previo consenso scritto di Citi. I fornitori non possono utilizzare il nome, il logo o i marchi commerciali, le strutture o i rapporti di Citi, nel quadro di attività al di fuori di Citi (incluso su carta intestata o siti web personali, blog o altri siti di social network). Inoltre, i Fornitori non possono utilizzare in alcun modo il nome, le strutture o le relazioni di Citi per scopi benefici o pro bono.

10 COMUNICAZIONI ELETTRONICHE SCRITTE

Nell'interazione con il personale di Citi o durante l'adempimento dei propri obblighi in nome o per conto di Citi, i Fornitori sono autorizzati a utilizzare solo le apparecchiature, i sistemi e i servizi di comunicazione elettronica scritta approvati da Citi. I Canali Citi eComm nuovi, ampliati o modificati, sia come strumenti autonomi che integrati in una piattaforma più ampia, fornita da Citi o da terze parti, devono essere approvati in conformità ai Requisiti di Citi applicabili di cui il Fornitore è stato informato per iscritto dal proprio BAO. È vietato parlare delle attività di Citi con il personale Citi su piattaforme di messaggistica non approvate da Citi, quali WhatsApp, WeChat, LINE, Slack, Signal, Telegram, iMessage, SMS, Viber o qualsiasi altra piattaforma elettronica interattiva.

Inoltre, i fornitori non devono avere alcuna aspettativa di privacy in relazione alle comunicazioni elettroniche scritte create, scoperte, utilizzate, consultate, scaricate, archiviate, trasmesse, ricevute o eliminate tramite le apparecchiature, i sistemi e i servizi di comunicazione forniti da Citi. Citi può monitorare le apparecchiature, i sistemi e i servizi di comunicazione elettronica e le comunicazioni elettroniche. Tali comunicazioni elettroniche sono di proprietà di Citi e possono essere conservate in conformità ai requisiti applicabili di conservazione della documentazione (soggetti alle leggi e ai regolamenti locali).

<https://policydirectory.citi.net/cpd/ layouts/15/DocIdRedir.aspx?ID=CPDPROD-13-8739>

11 ATTIVITÀ E CONTRIBUTI POLITICI

Una serie di leggi diverse, come quelle relative a: ingerenze straniere; finanziamento delle campagne; omaggi e forme di ospitalità; attività di lobbying presso organi legislativi, di base (grassroots), istituzionale e regolamentare; appalti pubblici; pratiche di pay-to-play; e mercati finanziari, disciplinano le attività politiche di Citi e dei suoi Fornitori, nonché gli obblighi di informativa connessi a tali attività. È vietata una qualsiasi attività politica svolta dai Fornitori che non sia conforme alle policy, agli standard, alle leggi o ai regolamenti pertinenti di Citi.

L'attività politica include, ma non si limita a:

1. Effettuare contributi politici a titolo aziendale o personale, sollecitare contributi politici, utilizzare fondi o risorse aziendali (quali strutture, attrezzature, software o personale) o svolgere servizi personali volontari durante l'orario di lavoro per conto di un

- candidato ad un ufficio pubblico, un comitato di un partito politico o un comitato politico;
2. Fare pressione o cercare di influenzare soggetti pubblici, direttamente o tramite parti terze, e altresì cercare di influenzare funzionari, decisioni legislative e, a seconda delle giurisdizioni, cercare eventualmente di influenzare l'adozione di una norma amministrativa o l'assegnazione di un appalto statale; o
 3. Cercare, accettare o ricoprire cariche politiche associate a un governo, inclusi consigli di amministrazione, commissioni o altre organizzazioni simili.

Nessuna attività politica può essere intrapresa o condotta da un Fornitore per conto di (o presumibilmente per conto di) Citi senza previa autorizzazione scritta del Government Affairs Global Operations Control (ggacontrol@citi.com) di Citi. Anche se Citi potrà pagare una commissione e/o rimborsare le spese per servizi di attività politica consentiti e ordinati al fornitore, quali quelli di lobbying, Citi non rimborserà mai un fornitore o uno dei suoi dipendenti per contributi politici personali o aziendali di qualsiasi tipo.

12 ANTIRICICLAGGIO (“AML”)

Applicabile ai Fornitori che eseguono determinati servizi connessi al cliente (ad es. on-boarding, monitoraggio dei conti e delle transazioni dei clienti) o la consegna di dati/metriche relativi alle attività di cui sopra; E/O che agiscono come intermediari per quanto riguarda le transazioni o gli strumenti finanziari (ad esempio, deposito di assegni da remoto, corrieri, servizi di blindato o cassette di sicurezza, trasferimenti elettronici di fondi e attività digitali).

12.1 Obblighi relativi all'antiriciclaggio (AML):

1. Conformità ai processi di Citi e alle leggi applicabili:

- Mantenere e rispettare i processi e le procedure di Citi progettati per soddisfare i requisiti delle leggi applicabili, tra cui (i) il Gramm-Leach-Bliley Act e i regolamenti emanati ai sensi dello stesso; (ii) l'USA PATRIOT Act e i regolamenti emanati ai sensi dello stesso; (iii) qualsiasi legge o regolamento in materia di riciclaggio di denaro; e (iv) qualsiasi legge o regolamento relativo alle sanzioni economiche. Tali policy e procedure affronteranno i ruoli e le responsabilità in materia di antiriciclaggio, compresi i requisiti per segnalare tempestivamente una qualsiasi attività osservata che appaia insolita o potenzialmente insolita in relazione alle attività finanziarie, alle transazioni e alla ricezione di denaro contante.

2. Formazione annuale ed elementi del programma per il personale:

- Garantire che il personale che fornisce servizi a Citi riceva una formazione annuale in merito ai ruoli e alle responsabilità in materia di

antiriciclaggio, compresi gli obblighi di segnalare tempestivamente una qualsiasi attività osservata che appaia insolita o potenzialmente insolita in relazione alle attività finanziarie, alle transazioni e alla ricezione di denaro contante. La formazione comprenderà, tra gli altri, i seguenti argomenti:

- a. Segnalazione ed escalation di attività sospette.
- b. Un programma “Conosci il tuo cliente” (KYC), che include un programma di identificazione del cliente (CIP), sanzioni e screening dei nomi, due diligence del cliente (CDD), due diligence rafforzata (EDD) e l'identificazione e la verifica dei titolari effettivi ufficiali (**Ultimate Beneficial Owner, UBO**).
- c. Monitoraggio delle transazioni in tutti gli strumenti finanziari e le attività rilevanti.
- d. Reporting/Metriche periodiche, comprese le segnalazioni sui cambiamenti legali e normativi e sulle modifiche sostanziali del programma AML
- e. Test e controlli dell'efficacia del programma AML, comprese le visite in loco.

3. Conformità alle disposizioni del contratto:

- Rispettare tutte le disposizioni contrattuali che definiscono un programma che deve essere istituito dal Fornitore.

4. Segnalazione tempestiva di inosservanze sospette:

- Segnalare tempestivamente a Citi per iscritto qualsiasi sospetta violazione della legge, inclusa una qualsiasi attività osservata che appaia insolita o potenzialmente insolita in relazione all'entrata di denaro in relazione a Citi o ai suoi clienti.

5. Prevenzione e segnalazione dell'evasione fiscale:

- Rispettare tutte le leggi e le normative fiscali applicabili nei paesi in cui operano.
- In nessun caso i Fornitori devono essere coinvolti in evasioni fiscali illegali deliberate o facilitare tali evasioni per conto di terzi, come lo svolgimento di attività che potrebbero aiutare a eludere il pagamento delle tasse dovute e pagabili o nascondere informazioni alle autorità fiscali.

- Pertanto i Fornitori devono adottare ragionevoli procedure di prevenzione relative all'evasione fiscale e segnalare tempestivamente a Citi per iscritto eventuali violazioni o sospette violazioni relative alla loro attività con Citi.

12.2 Policy e procedure interne del fornitore:

I fornitori devono inoltre mantenere policy e procedure appropriate per rispettare tutte le leggi e i regolamenti antiriciclaggio attualmente in vigore o di seguito attuati.

13 GESTIONE DEI DOCUMENTI

Applicabile ai Fornitori che accedono/elaborano/archiviano le informazioni Citi.

Citi richiede che tutti i Fornitori in custodia delle Informazioni di Citi collaborino con il proprio Business Activity Owner (“**BAO**”) o con il contatto commerciale principale di Citi per (i) identificare e classificare le informazioni come Record o Informazioni transitorie ai fini della gestione dei record di Citi, (ii) classificare i Record in conformità con il Master Record Catalogue (“**MRC**”) di Citi, (iii) archiviare le Informazioni in base ai requisiti di conservazione di Citi e (iv) in assenza di vincoli di conservazione, eliminare in modo appropriato le Informazioni alla fine del relativo ciclo di vita.

Il BAO o il contatto commerciale principale di Citi deve collaborare con il Fornitore per garantire che il Fornitore abbia identificato e classificato i registri in base ai codici relativi di Citi nell'MRC e che l'inventario venga aggiornato almeno una volta all'anno. Il Fornitore ha l'obbligo di rispettare i requisiti di gestione dei documenti comunicati dal BAO. I documenti che soddisfano i criteri per lo smaltimento devono essere adeguatamente smaltiti il prima possibile, ma non oltre sei mesi dopo che sono stati soddisfatti i requisiti di conservazione, a meno che non siano soggetti a vincoli di conservazione. Le Informazioni transitorie devono essere distrutte non oltre due anni dopo il loro ultimo utilizzo, a meno che non siano soggette a vincoli di conservazione. Le Informazioni transitorie che contengono informazioni personali devono essere cancellate una volta che la finalità per la quale sono state raccolte è stata raggiunta, a meno che non siano soggette a vincoli di conservazione. Il Fornitore deve sospendere la distruzione o l'alterazione delle Informazioni di Citi quando viene informato di un vincolo di conservazione. In caso di incertezza, il Fornitore deve contattare il proprio principale referente aziendale di Citi o BAO.

Ogni trimestre, le regole di conservazione elencate nei calendari relativi per paese vengono riviste e aggiornate, secondo necessità, dal DRIM per essere conformi alle modifiche normative e interne. Qualora si verifichi un cambiamento che abbia un impatto sul Fornitore, BAO ne darà comunicazione al Fornitore. Il Fornitore deve valutare l'impatto e implementare modifiche nei rispettivi sistemi, processi e inventari. Tipi di record di sua proprietà e che gestisce entro 90 giorni dalla notifica da parte del BAO.

I Fornitori che conservano i documenti per conto di Citi sono tenuti a preservare ("hold"), raccogliere e fornire tutte le informazioni ritenute rilevanti per un procedimento legale o di altro tipo entro il tempo necessario, come richiesto loro dal BAO. Il Fornitore dovrà, su richiesta, restituire le informazioni di Citi come richiesto dai termini contrattuali applicabili. I Fornitori non devono smaltire alcuna Informazione di Citi, indipendentemente dalla sua classificazione (ad esempio, Riservata, Non Riservata) senza l'approvazione del loro principale contatto commerciale di Citi o BAO, che deve includere la conferma che nessun vincolo attivo di conservazione delle informazioni si applica alle Informazioni da eliminare. Gli obblighi di gestione e conservazione dei documenti nonché tutti gli altri obblighi di gestione delle informazioni rimarranno in vigore anche dopo la risoluzione o la scadenza del Contratto, salvo diverso accordo esplicito.

I fornitori dovranno conservare la documentazione che elenca tutti i membri del personale del fornitore responsabili di sovrintendere alla gestione delle informazioni di Citi che ha in custodia il fornitore e tenere riunioni periodiche con i propri principali referenti aziendali di Citi o Records Management Officer per esaminare e aggiornare i nomi dei contatti, i dettagli procedurali, i ruoli e le responsabilità e l'inventario dei documenti dei fornitori di Citi.

14 RESILIENZA AZIENDALE/CONTINUITÀ DEL BUSINESS

Applicabile ai Fornitori che erogano servizi o ospitano infrastrutture/applicazioni tecnologiche utilizzate da Citi. Il Titolare Citi Business Activity Owner (BAO) ha la responsabilità di comunicare l'applicabilità e i requisiti COB al Fornitore.

14.1 Risorse di ripristino

Il Piano di disaster recovery dei Fornitori deve fornire risorse alternative in grado di fornire tutti i prodotti e servizi a Citi nel caso in cui le sedi primarie del Fornitore vengano disattivate. Le risorse per il ripristino devono essere ubicate in posizioni geograficamente separate dalle posizioni primarie, con una separazione sufficiente a ridurre al minimo o eliminare la minaccia che lo stesso evento catastrofico possa colpire sia le posizioni primarie sia le posizioni di ripristino.

1. Le risorse per il ripristino non sono limitate ai sistemi informatici, ma includono tutte le risorse necessarie per la continuità dell'erogazione di prodotti e servizi a Citi e possono includere personale, edifici, attrezzature aziendali, centri dati, reti dati e reti vocali e servizi di trasporto.
2. I Fornitori di applicazioni possono implementare un'architettura di tipo Hot/Hot per garantire una configurazione ad alta disponibilità (HA). Questa architettura richiede che ci siano (come minimo) due sistemi configurati in modo identico, attivi e disponibili per i clienti/utenti. La caratteristica più importante offerta da questo modello è che gli ambienti alternativi vengono gestiti contemporaneamente al data center primario (di produzione).

14.2 Livelli di servizio di ripristino

Per essere efficienti per Citi la continuità aziendale dei Fornitori deve soddisfare i livelli di servizio stabiliti. Come minimo, il Piano di disaster recovery del fornitore stabilirà valori specifici per:

1. Obiettivo dei tempi di ripristino
2. Obiettivo del punto di ripristino
3. Risorse di ripristino/Capacità tecnologica
4. Durata del ripristino

14.3 Piano di disaster recovery

Il Fornitore manterrà un Piano di disaster recovery per la prosecuzione dell'attività (e fornirà, se richiesto da Citi, prova della sua verifica attuale e periodica) in modo che, nonostante una qualsiasi interruzione da parte del Fornitore di fornire i prodotti/servizi o di adempiere agli altri obblighi previsti dal presente documento da qualsiasi luogo particolare o tramite l'impegno di un individuo particolare, il Fornitore sarà prontamente in grado di fornire i prodotti/servizi e adempiere ai propri obblighi da una sede alternativa o con personale sostitutivo. Una copia del Piano di disaster recovery deve essere fornita a Citi entro dieci (10) giorni solari dalla data di entrata in vigore di ogni ordine di lavoro stipulato tra Citi e il Fornitore per i servizi rivolti al cliente e successivamente ogni anno per tutto il tempo in cui ciascun ordine di lavoro è in vigore. Il Fornitore fornirà a Citi tutte le istruzioni o le altre informazioni necessarie affinché Citi possa continuare a ricevere i Servizi/Prodotti dal Fornitore in circostanze in cui il Fornitore abbia dovuto invocare il Disaster Recovery Plan. Il Fornitore dichiara, garantisce e concorda che il Piano di disaster recovery includerà almeno:

1. Procedure e strategie di ripristino, inclusi ricollocamento, trasferimento del lavoro e/o accesso remoto per mitigare gli effetti delle interruzioni, inclusa l'indisponibilità della tecnologia (Denial of Service/DoS), l'indisponibilità del luogo di lavoro principale (Denial of Access/DoA) e l'indisponibilità del personale (compresi i subappaltatori);
2. Il mantenimento da parte del Fornitore (a titolo esemplificativo) di un sito secondario di disaster recovery separato dalle sedi di prodotti/servizi, l'archiviazione di supporti di back-up in un luogo separato dalle sedi dei prodotti/servizi, l'uso di linee di comunicazione e server ridondanti;
3. Procedure per il back-up/ripristino del funzionamento e dell'applicazione dei prodotti/servizi, compreso un piano dettagliato e documentato per rispondere a una sospensione prolungata dei prodotti/servizi, causata da un'interruzione di corrente, un guasto del sistema, un disastro naturale o altre circostanze impreviste che includa processi e procedure per riprendere le operazioni entro un periodo di tempo concordato;
4. Procedure per la protezione di tutti i contenuti;
5. Procedure ed eventuali accordi con terzi per la sostituzione di apparecchiature (es. apparecchiature informatiche);
6. Procedure per eventuali impianti di produzione fuori sede; e
7. inoltre, il Piano di disaster recovery del Fornitore prevede che:
 - a. Il Fornitore informi tempestivamente Citi di qualsiasi disastro che potrebbe avere un impatto negativo sui prodotti/servizi;

- b. Il Fornitore fornisca a Citi, entro 24 ore da tale avviso, un piano per continuare a fornire i prodotti/servizi presso una struttura di elaborazione alternativa;
- c. I Prodotti/Servizi debbano essere pienamente operativi entro il Obiettivo dei tempi di ripristino (RTO) richiesto, che, se non diversamente definito nel Contratto applicabile, è pari o inferiore a 4 ore per i processi classificati critici "Enterprise Critical" o con un livello di criticità "ALTO", 24 ore o meno per i processi valutati da Citi con un livello di criticità "MEDIO" e 72 ore o meno per i processi classificati da Citi con un livello di criticità "BASSO"; e
- d. Nel caso in cui parti delle strutture del Fornitore non siano operative, il Fornitore tratterà Citi non meno favorevolmente di quanto il Fornitore tratti i suoi altri clienti commerciali.

14.4 Requisiti del Piano di disaster recovery applicabili ai servizi ospitati

Nella misura in cui il Fornitore gestisce e fornisce un Servizio Ospitato (Hosted Service) a Citi, si applicheranno anche le disposizioni che seguono. Il Piano di disaster recovery includerà almeno:

1. Procedure per il back-up/ripristino del funzionamento e dell'applicazione dei servizi ospitati, compreso un piano dettagliato e documentato per rispondere a una sospensione prolungata dei servizi, causata da un'interruzione di corrente, un guasto del sistema, un disastro naturale o altre circostanze impreviste che includano processi e procedure per riprendere le operazioni entro un periodo di tempo concordato;
2. Inoltre, il Piano di disaster recovery del fornitore prevede che: (a) Il Fornitore informerà Citi per iscritto entro due (2) ore da qualsiasi disastro che potrebbe avere un impatto negativo sui servizi ospitati; (b) Il Fornitore fornirà a Citi, entro 24 ore da tale avviso, un piano per continuare a fornire i servizi in hosting presso una struttura di elaborazione alternativa e (c) i servizi in hosting devono essere pienamente operativi entro 48 ore dall'avviso iniziale;
3. Il Fornitore accetta, su richiesta, di rilasciare le informazioni necessarie per permettere a Citi di sviluppare un piano di ripristino e un piano di continuità aziendale, che funzionerà insieme al piano di Disaster Recovery e al piano di continuità aziendale del Fornitore; e
4. Nel caso in cui parti delle strutture del Fornitore non siano operative, il Fornitore tratterà Citi non meno favorevolmente di quanto il Fornitore tratti i suoi altri clienti commerciali.

14.5 Modifiche al Piano di disaster recovery

Il Fornitore può modificare il proprio Piano di disaster recovery purché tali modifiche non compromettano il piano in modo tale da influire negativamente sui servizi (ad esempio, prolungando gli RTO). Il Fornitore comunicherà tempestivamente a Citi eventuali modifiche al proprio Piano di disaster recovery e, su richiesta di Citi, spiegherà tali modifiche in modo che Citi possa comprenderle appieno e rispondere ad esse.

14.6 Piano di disaster recovery dei subappaltatori

Il fornitore garantirà che qualsiasi Subappaltatore del fornitore mantenga un Piano di disaster recovery e il relativo piano di continuità aziendale che sia pienamente coerente con i requisiti di Citi per i Fornitori. Il Fornitore deve fornire un'adeguata supervisione dei Subappaltatori, inclusa una revisione periodica di tali controlli e risultati dei test, e garantire un tempestivo rimedio a eventuali lacune identificate.

14.7 Invocazione del Piano di disaster recovery e notifica di crisi

Il Fornitore comunicherà tempestivamente al principale referente aziendale di Citi:

1. Quando il Fornitore invoca il Piano di disaster recovery; e;
2. Prevede una crisi, una minaccia, un allarme o un intervento informatico nei confronti del Fornitore o dei suoi Subappaltatori che possa ragionevolmente avere un impatto negativo sui Servizi o sui Prodotti forniti a Citi.

14.8 Test

Tutte le risorse e i piani di ripristino del Fornitore devono essere testati entro 120 giorni dall'implementazione della produzione (90 giorni in caso di applicazioni classificate da Citi come Enterprise Critical) e almeno una volta all'anno (ogni 12 mesi). Il test deve dimostrare la capacità del fornitore di soddisfare i livelli di ripristino del servizio per tutti i prodotti e servizi forniti a Citi. Tali test devono essere completi e includere l'intera gamma dei servizi forniti a Citi. I fornitori devono fornire a Citi un preavviso di almeno 30 giorni per testare il ripristino dei prodotti/servizi forniti a Citi. Citi può partecipare o osservare i test di ripristino del Fornitore sulle applicazioni utilizzate da Citi per convalidare la funzionalità aziendale dell'applicazione nell'ambiente di ripristino. Se Citi desidera partecipare, il fornitore fornirà a Citi gli obiettivi del test, il piano del test e le procedure di connessione al sito del test prima di condurre il test. Entro dieci (10) giorni lavorativi dal completamento di ciascun test, il Fornitore fornirà a Citi un riepilogo degli obiettivi del test, del piano dei test e dei risultati dei test, compresi i tempi necessari per il ripristino e le prove dei risultati dei test (ad es. gli screenshot).

14.9 Convalida del volume

Un Fornitore che ospita applicazioni classificate da Citi come Enterprise Critical deve dimostrare che i Volumi di Produzione possono essere elaborati nel suo ambiente COB/di disaster recovery. Citi e il Fornitore devono concordare la metodologia da utilizzare per la convalida.

14.10 Utilizzo dei sistemi di Citi per fornire servizi

Se richiesto da Citi o dalle affiliate di Citi, i Fornitori che utilizzano i Sistemi di Citi parteciperanno, senza costi o oneri per Citi, alle esercitazioni di disaster recovery di Citi.

14.11 Valutazione dei risultati dei test

Se i risultati di un test tra quelli eseguiti dal Fornitore mostrano il mancato raggiungimento degli obiettivi del test o di qualsiasi RTO applicabile, il Fornitore si impegnerà a eseguire un'analisi delle cause all'origine e a porre rimedio tempestivamente a eventuali carenze identificate. A seguito dell'implementazione di tale rimedio, il Fornitore dovrà effettuare un nuovo test entro e non oltre centoventi (120) giorni di calendario (90 giorni di

calendario in caso di applicazioni classificate come Enterprise Critical da Citi) dal test iniziale non superato (o al periodo di tempo specificato nell'ordine di lavoro pertinente).

14.12 Gestione delle crisi

Parallelamente al piano di continuità operativa, il fornitore dovrà mantenere un piano di gestione di crisi per la direzione e il controllo delle operazioni di ripristino. Come minimo, il piano di gestione delle crisi del Fornitore individuerà specifici soggetti muniti di autorità sufficiente per attivare un'operazione di ripristino, definirà protocolli di comunicazione ed escalation per raccogliere e diffondere informazioni sulla crisi e includerà protocolli di notifica ed escalation per comunicare con Citi in caso di crisi.

14.13 Valutazioni della continuità aziendale

I Fornitori sono soggetti al processo "Third-Party Continuity of Business Assessment Process" di Citi per la valutazione delle policy, delle procedure e dei controlli del Fornitore in merito alla conformità ai requisiti di Citi e a qualsiasi requisito legale e/o normativo (applicabile a Citi o al Fornitore) relativo alla continuità aziendale. La valutazione consiste in questionari che richiedono risposte da parte del Fornitore con prove di supporto e potrebbe includere visite alle sedi del Fornitore. Qualora i risultati di una valutazione rivelassero o indicassero problemi o preoccupazioni, Citi documenterà i risultati e collaborerà con il Fornitore per identificare un modo per risolvere i problemi. I Fornitori devono apportare tempestivamente le correzioni necessarie e/o aggiungere o compensare con controlli per rispondere alle preoccupazioni di Citi in modo ragionevolmente soddisfacente per Citi.

14.14 Resilienza operativa

I Critical Business Services sono i servizi che, in caso di interruzione della fornitura, potrebbero causare un impatto negativo significativo su Citi, sui suoi clienti o sul sistema finanziario. Il Fornitore dovrà garantire che una qualsiasi interruzione della fornitura di elementi dei servizi che equivalgono a servizi aziendali critici o supportano la fornitura di servizi aziendali critici da parte di Citi, come specificato da Citi di volta in volta ("Critical Business Services") non ecceda la durata stabilita da Citi o in altro modo violi qualsiasi metrica pertinente impostata da Citi ("Impact Tolerances") come notificato di volta in volta al Fornitore. Le tolleranze all'impatto saranno espresse come una metrica vincolata da scadenza che equivale al tempo di interruzione del servizio. Citi e il Fornitore esamineranno annualmente le tolleranze all'impatto come parte dei processi di governance del contratto in corso. Laddove Citi sia tenuta a impostare più di una tolleranza all'impatto per un singolo servizio aziendale critico a causa dei requisiti di più di un organismo di regolamentazione, Citi può specificare tolleranze all'impatto separate per tale servizio aziendale critico. Il fornitore deve:

1. Notificare a Citi non appena si rende conto che non è riuscito (o è ragionevolmente probabile che non riesca) a erogare un servizio aziendale critico entro la corrispondente tolleranza/e all'impatto stabilita da Citi, insieme a una spiegazione delle ragioni di qualsiasi fallimento potenziale o attuale delle misure adottate per mitigare l'impatto di tale fallimento;
2. Ove richiesto, fornire un'assistenza ragionevole a Citi per consentirle di identificare le persone, i processi, la tecnologia, le strutture e le informazioni che sono necessarie al Fornitore per fornire qualsiasi servizio

aziendale critico;

3. Fornire a Citi un'assistenza ragionevole per consentirle di condurre:
 - a. qualsiasi test della capacità interna del Fornitore di rimanere entro le tolleranze all'impatto per ciascun servizio aziendale critico in caso di un'interruzione grave ma plausibile delle proprie operazioni o le operazioni del Fornitore; e
 - b. qualsiasi lezione appresa esercitata a seguito di un test di scenario per permettere a Citi di identificare i punti deboli e qualsiasi azione necessaria per migliorare la capacità del fornitore di rispondere e riprendersi efficacemente da future interruzioni.

Qualora un test interno di Citi identifichi vulnerabilità o limitazioni del Fornitore di fornire servizi aziendali critici entro la corrispondente tolleranza/e all'impatto fissata da Citi e a seguito di una qualsiasi mancata fornitura da parte del Fornitore di un qualsiasi servizio aziendale critico entro la corrispondente tolleranza/e all'impatto stabilita da Citi, le parti concorderanno un piano (comprensivo di un calendario di attuazione), per garantire che il Fornitore adotti le misure necessarie per risolvere o mitigare tali vulnerabilità o limitazioni o per porre rimedio alla causa del mancato rispetto della tolleranza/e all'impatto (a seconda dei casi), non appena sia ragionevolmente possibile.

14.15 Accordo di deposito in garanzia.

Su richiesta di Citi, i Fornitori (i) che concedono in licenza il software a Citi per il funzionamento nell'ambiente di Citi o (ii) che forniscono un Servizio ospitato a Citi, dovranno garantire che i materiali di deposito siano depositati presso l'agente di deposito designato da Citi e sottoscrivere un programma di registrazione dei depositanti o altri moduli richiesti dall'agente di deposito in relazione ai materiali di deposito ai sensi dell'accordo di deposito applicabile. Successivamente, per tutta la durata residua del contratto applicabile in relazione alla licenza o al servizio ospitato, il Fornitore depositerà le versioni aggiornate dei materiali di deposito presso l'agente di deposito per garantire che il codice sorgente depositato e gli altri materiali depositati rimangano aggiornati con l'ultima versione del software applicabile al software o ai servizi ospitati utilizzati da Citi. Gli aggiornamenti del codice sorgente o di altri materiali depositati dovranno essere consegnati all'agente di deposito entro trenta (30) giorni dalla data di un qualsiasi aggiornamento al software concesso in licenza a Citi o dalle modifiche ai Servizi ospitati utilizzati da Citi. Il Fornitore rispetterà pienamente tutti gli obblighi e i requisiti di un depositante come stabilito nel contratto di deposito a garanzia. Il Fornitore è l'unico responsabile di tutti i costi e le commissioni di deposito a garanzia, inclusi, a titolo esemplificativo ma non esaustivo, le commissioni di attivazione, le commissioni annuali, le commissioni di deposito, le commissioni per i servizi e qualsiasi altra commissione e costo di garanzia. In caso di un Evento di rilascio, l'agente di deposito rilascerà i materiali del deposito a Citi o a un suo delegato, in conformità con i termini dell'accordo sottostante e dell'accordo di deposito.

Se il Codice sorgente (o altri Materiali di deposito) vengono consegnati a Citi o a un suo delegato (direttamente dal Fornitore o dall'Agente di deposito in adempimento dei propri obblighi ai sensi di un accordo di deposito applicabile), il Codice sorgente e i Materiali di deposito sono soggetti alla licenza esistente ai sensi dell'accordo pertinente tra il

Fornitore e Citi; a condizione che ciascuna licenza sia considerata autorizzata a Citi per utilizzare e modificare il Codice sorgente e altri materiali di deposito secondo quanto ragionevolmente necessario per: (i) integrare e garantire la compatibilità del software e degli altri Materiali di Deposito con i Sistemi di Citi, (ii) fare in modo che il software o gli altri Materiali di Deposito siano conformi alla legge applicabile, agli standard del settore o alle prassi di mercato, (iii) consentire al software o agli altri Materiali di Deposito di rimanere aggiornati con le innovazioni tecnologiche e (iv) consentire al software e agli altri Materiali di Deposito di soddisfare gli scopi commerciali di Citi e delle sue Affiliate nell'ambito della Licenza esistente. Tutte le versioni del Software che includono una modifica sviluppata da o per conto di Citi utilizzando il Codice Sorgente sono soggette a tutte le disposizioni della presente Sezione e del contratto sottostante; a condizione, tuttavia, che il Fornitore non abbia alcun diritto, titolo o interesse su tali modifiche e che tutti i diritti di proprietà intellettuale su tali modifiche siano attribuiti esclusivamente a Citi.

Il Fornitore si impegnerà in modo commercialmente ragionevole con le terze parti che hanno fornito il software utilizzato nel Software per consentire al Fornitore di inserire il codice sorgente di tale software di terze parti nel Deposito del codice sorgente. Se la terza parte si rifiuta di concedere al Fornitore tale diritto, il Fornitore dovrà impegnarsi in modo commercialmente ragionevole per far sì che il contratto di licenza software di terze parti applicabile sia trasferibile a Citi in caso di Evento di rilascio.

Il Codice sorgente fornito a Citi in conformità alla presente Sezione sarà soggetto alla Licenza esistente per il Software concesso in licenza o per i Servizi ospitati applicabili, a condizione che Citi possa utilizzare e modificare il Codice sorgente e il Software in relazione ai propri requisiti aziendali e operativi, per consentire al Software di rimanere aggiornato con le innovazioni tecnologiche e di conformarsi alla Legge applicabile. Tutte le versioni del Software che includono una modifica sviluppata da o per conto di Citi utilizzando il Codice Sorgente sono soggette a tutte le disposizioni del contratto applicabile; a condizione, tuttavia, che il Fornitore non abbia alcun diritto, titolo o interesse su tali modifiche e che tutti i Diritti di Proprietà Intellettuale su tali modifiche siano attribuiti esclusivamente a Citi.

15 GLOBAL BACKGROUND SCREENING STANDARDS

Applicabile a tutti i Fornitori terzi che forniscono servizi a Citi.

15.1 Panoramica – Esame dei precedenti

L'esame dei precedenti deve essere effettuato conformemente a tutte le leggi e le normative locali applicabili. Tutte le informazioni e le informazioni autonome descritte in questo documento devono essere fornite dai rappresentanti del Fornitore, dal personale del fornitore e dai subappaltatori, ove appropriato. La falsificazione o l'omissione di informazioni su un curriculum, durante un'intervista, su un modulo di inserimento o durante il processo di inserimento, a prescindere da quando siano scoperte, possono costituire motivo di rifiuto o cessazione dell'incarico presso Citi in conformità alla legge locale. I risultati negativi emersi da un controllo eseguito, a prescindere da quando siano scoperti, possono costituire motivo di rifiuto o cessazione dell'incarico presso Citi in conformità alla legge locale.

Ulteriori informazioni sul completamento dello screening dei precedenti sono disponibili all'indirizzo

https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf

15.2 Raccolta di informazioni di base e verifica dell'identità

Prima che un membro del personale del Fornitore inizi un incarico presso Citi, il Fornitore dovrà procurarsi il nome e cognome, l'indirizzo postale e l'indirizzo di residenza permanente (se diverso), il numero di telefono e l'indirizzo e-mail (se applicabile) delle persone interessate. Il personale del fornitore deve inoltre fornire la documentazione che convalidi la propria identità. Ciò può includere la fornitura di informazioni e/o della documentazione relative a un numero di identificazione nazionale, una carta d'identità rilasciata dal governo con una fotografia o un passaporto.

15.3 Controllo delle sanzioni

Tutto il personale dei Fornitori che svolge attività per conto di Citi, nonché qualsiasi soggetto che detenga una partecipazione pari o superiore al 25% in un fornitore di Citi, compresi i Subappaltatori, indipendentemente dal fatto che abbia accesso ai dati, ai sistemi o alle reti di Citi e/o ai locali di Citi, deve essere sottoposto a verifica rispetto all'elenco degli individui Specially Designated Nationals and Blocked Persons ("SDN List") dell'Office of Foreign Assets Control ("OFAC") del Dipartimento del tesoro degli Stati Uniti, nonché rispetto all'elenco delle regioni e delle giurisdizioni soggette alle sanzioni imposte dagli Stati Uniti ("U.S. Sanctions"). Deve inoltre essere sottoposto a verifica rispetto a qualsiasi elenco emanato e alle giurisdizioni soggette a sanzioni imposte da autorità al di fuori degli Stati Uniti, tra cui l'Elenco consolidato delle sanzioni finanziarie dell'Unione europea (UE), l'Elenco consolidato del Consiglio di sicurezza delle Nazioni Unite (ONU), l'Elenco delle sanzioni del Regno Unito (UK) e gli elenchi previsti dalla normativa applicabile nella giurisdizione locale ("Sanzioni non statunitensi").

Gli elenchi OFAC sono disponibili al pubblico su questo sito web: <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

15.4 Conformità alle norme sull'immigrazione

Il fornitore deve dimostrare di mantenere e implementare protocolli volti a verificare che tutto il personale sia autorizzato a lavorare nei Paesi in cui svolge l'incarico. Inoltre, il Fornitore deve: (1) garantire che tutto il personale sia autorizzato al lavoro e (2) mantenere la conformità a tutte le leggi, i regolamenti e le policy applicabili (inclusi i requisiti di idoneità e verifica dell'impiego). Il fornitore deve inoltre dimostrare che dispone di e mantiene protocolli volti a garantire che il suo personale sia altrimenti conforme a tutte le leggi e le normative applicabili in materia di immigrazione e che il proprio personale detenga l'appropriato status/l'appropriata categoria di visto per gli incarichi e le attività che svolge.

15.5 Storia lavorativa

Se richiesto dalle normative locali i Fornitori devono convalidare il passato lavorativo del proprio personale negli ultimi sette (7) anni o 10 anni. Il passato lavorativo dell'individuo deve essere convalidato per garantire che i datori di lavoro, le posizioni, le date e le mansioni siano stati rappresentati accuratamente. Il personale del Fornitore deve inoltre dichiarare gli impieghi o gli incarichi precedenti come consulenti o lavoratori temporanei presso Citi o una delle sue società predecessori (inclusi, ma non solo: Citibank, Citicorp, Travelers, Salomon Brothers e/o Smith Barney).

15.6 Livello di istruzione

I Fornitori devono convalidare il più alto livello di istruzione del proprio personale. Le informazioni confermate devono includere le date dei corsi di istruzione frequentati, il/i nome/i e l'indirizzo o gli indirizzi dell'istituto e i titoli conseguiti.

15.7 Precedenti penali

Se permesso dalle leggi locali, il personale e i subappaltatori di un fornitore devono notificare a Citi se vengono sottoposti ad arresto, citazioni, mandati, incriminazioni o condanne per un qualsiasi illecito penale, compresa la dichiarazione di colpevolezza o mancanza di appello di contestazione e la partecipazione a un programma prima del processo o a misure analoghe. La verifica amministrativa dei documenti penali e/o i controlli delle impronte digitali devono essere completati prima della data di inizio dell'incarico quando è legalmente ammissibile e disponibile. Le condanne penali per reati riguardanti furti, frodi, disonestà o abuso di fiducia, o simili reati definiti in modo diverso dalla legge locale, salvo ove altrimenti vietato dalla legge, possono comportare l'esclusione e/o l'inidoneità per l'incarico presso Citi. Altre condanne potrebbero comportare il rifiuto e/o l'inidoneità all'incarico sulla base delle leggi e dei regolamenti locali applicabili.

15.8 Nuova verifica

Il personale del Fornitore il cui incarico a termine deve essere nuovamente selezionato nel caso in cui venga riassegnato a Citi. Per ulteriori informazioni sui requisiti di un nuovo screening, fare riferimento a https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdf

15.9 Trasferimenti internazionali

Tutti gli screening devono essere completati in conformità con le normative del paese dell'incarico. Se il personale del Fornitore si trasferisce in un nuovo Paese l'individuo deve essere nuovamente sottoposto a controlli in base alle esigenze del nuovo Paese.

16 SPESE

Fornitori che hanno il diritto contrattuale di richiedere il rimborso delle spese aziendali.

16.1 Panoramica

Citi rimborserà solo le spese ragionevoli relative alle attività che sono state pre-approvate per iscritto da Citi e sono state sostenute dal Fornitore in relazione alla fornitura di prodotti e servizi a Citi, conformemente ai termini applicabili del Contratto o della politica di gestione delle spese, ovvero la Citi's Operating Expense Governance Policy, ove appropriato, e adeguatamente motivate mediante ricevute, fatture, itinerari o altre forme di documentazione ritenute accettabili da Citi.

16.2 Rimborsi

Queste spese devono essere documentate correttamente e fatturate a Citi in conformità ai requisiti di fatturazione di Citi. Le spese del Fornitore non devono essere sostenute da un dipendente Citi per conto del Fornitore. Ogni spesa presentata a Citi per il rimborso di una o più voci di spesa valide e approvate deve includere (oltre a tutti gli altri requisiti di fatturazione):

1. Lo scopo commerciale della spesa;
2. L'importo e la descrizione della spesa;
3. Luogo e data della spesa;
4. Il nome/descrizione del progetto per il quale il Fornitore fornisce servizi;
5. I nomi e il rapporto commerciale del rappresentante di Citi che ha richiesto i servizi per i quali sono state sostenute tali spese; e
6. Numero dell'ordine di acquisto, ove applicabile.

Per informazioni sulle spese aziendali rimborsabili ammissibili, contattare il proprio referente aziendale di Citi. Insieme alla richiesta di rimborso, devono essere fornite ricevute, fatture, itinerari o altre forme di documentazione ritenute accettabili da Citi. Le richieste di rimborso devono essere conformi alle disposizioni del Contratto del caso o alla Operating Expense Governance Policy di Citi, oltre agli Standard e le Procedure del caso, se pertinenti, e approvate dallo sponsor aziendale opportuno e/o dal principale referente aziendale di Citi e approvate da un individuo debitamente autorizzato e con una quantità sufficiente di prodotti corrispondenti. Le richieste non conformi non verranno rimborsate.

17 SICUREZZA DELLE INFORMAZIONI

Applicabile ai Fornitori, compresi i Subappaltatori, che accedono, elaborano, archiviano o gestiscono le informazioni di Citi come sono classificate e definite nell'Appendice; o applicazioni rivolte a Internet con marchio Host Citi; o hanno connettività alle risorse di rete di Citi; o richiedono l'accesso senza scorta alle strutture di Citi.

17.1 Panoramica

Questa sezione contiene i requisiti minimi per i Fornitori di Citi, compresi i sub-incaricati o subappaltatori dei fornitori, che archiviano, elaborano, gestiscono o accedono alle informazioni di Citi o ospitano applicazioni di Citi, oppure hanno una connessione via rete con Citi, in merito ai controlli della protezione delle informazioni previsti da Citi. Tali requisiti garantiscono che le informazioni siano protette in conformità con i requisiti legali e normativi applicabili e con i più elevati standard di settore (ad esempio, ISO/IEC

27001/2) nei luoghi in cui operano Citi e i suoi fornitori. Se le leggi o i regolamenti locali, nonché gli standard di settore pertinenti stabiliscono standard superiori a quelli qui descritti, i Fornitori devono rispettare tali leggi, regolamenti o standard. Inoltre, i Fornitori potranno essere tenuti ad integrare ulteriori procedure e prassi di sicurezza delle informazioni per conformarsi alle altre policy di Citi e ai termini e alle condizioni contrattuali. Se un Fornitore decide di implementare ulteriori prassi di sicurezza o procedure dettagliate per la sicurezza delle informazioni, deve garantire che tali prassi e procedure non siano in contrasto con i controlli minimi definiti in questa sezione.

17.2 Politica sulla sicurezza delle informazioni e governance

I fornitori devono avere documentato le policy e gli standard sulla sicurezza delle informazioni. La governance delle policy deve includere ruoli e responsabilità chiaramente definiti, nonché policy annuali e revisione/aggiornamento degli standard per garantire la coerenza con lo stato attuale della tecnologia, gli standard di settore, i requisiti legali e normativi.

17.3 Separazione dei compiti

I fornitori devono mettere in atto dei processi che garantiscano che nessuna persona individuale possa svolgere due funzioni operative o due delle funzioni IT, o due delle funzioni dei sistemi informatici controllati con accesso continuo alla stessa attività, modifica, sistema informatico o transazione senza autorizzazione o rilevazione, salvo qualora non siano attivi adeguati controlli compensativi per mitigare il rischio.

Tabella A

Funzioni	Descrizione della funzione
Sviluppo / Progettazione	Progettare, creare o modificare software, hardware e configurazioni; alcuni esempi possono includere: - Progettazione e creazione di nuovo codice applicativo e relativi schemi di database - Prodotti per infrastrutture di ingegneria e componenti applicativi - Personalizzazione dei prodotti tecnologici da integrare con software e servizi
Approvazione	Approvare la promozione delle modifiche di codice da implementare
Sistemi di implementazione/amministrazione	Installare, implementare o amministrare software, hardware e modifiche alla configurazione. Alcuni esempi: - Esecuzione di un rilascio di codice automatizzato o manuale all'infrastruttura di produzione - Installazione di un prodotto o di un apparecchio tecnologico

	- Avviare o interrompere i servizi per supportare la risoluzione dei problemi e la correzione dei sistemi con dati di produzione
Revisione dell'attività degli ID privilegiati	Verificare l'attività di gestione delle modifiche o degli eventi del sistema relativi alla sicurezza (ad es. audit trail)
Amministrazione degli ID	Aggiungere, modificare ed eliminare gli ID (User, FID e bot), i diritti o le password
Funzione aziendale	Descrizione della funzione
Iniziare la transazione aziendale	Avviare (anche indicato come inserire o eseguire o creare) transazioni aziendali e modificare le informazioni dei clienti
Approvare la transazione aziendale	Approvare (anche indicato come autorizzare o controllare o rilasciare) le transazioni aziendali
Funzione IT	Descrizione della funzione
Operazioni sulla rete	Gestione dei dispositivi e supporto operativo dei prodotti che forniscono servizi di infrastruttura di rete. Router di rete, switch, firewall e servizi di nomi di dominio (DNS) ne sono degli esempi
Operazioni non di rete	Gestione dei dispositivi e supporto operativo di prodotti che non forniscono servizi di infrastruttura di rete. Server, telefoni e computer ne sono degli esempi

17.4 Impegno del management in materia di sicurezza delle informazioni

I Fornitori che ospiteranno un'applicazione Internet a marchio Citi e/o hanno accesso alle informazioni di Citi con una classificazione di riservatezza o di livello superiore sono soggetti al processo di valutazione della sicurezza delle informazioni di terze parti, Third Party Information Security Assessment Process (TPISA) di Citi per la valutazione delle policy, delle procedure e dei controlli del Fornitore in merito alla conformità ai requisiti di Citi e i requisiti legali e/o normativi (applicabili a Citi o al Fornitore) che riguardano la sicurezza delle informazioni.

La valutazione consiste di questionari sulla sicurezza che richiedono risposte da parte del Fornitore con prove a supporto e può includere visite alle sedi del Fornitore in cui le informazioni riservate o di livello superiore di Citi possono essere archiviate, elaborate, gestite o accessibili da parte di terzi. Inoltre, il team di monitoraggio continuo di terze parti TPISA può monitorare il Fornitore utilizzando strumenti di monitoraggio della sicurezza informatica che sfruttano informazioni pubblicamente disponibili per identificare sistemi, host, applicazioni e server vulnerabili rivolti a Internet per elementi quali software fuori produzione, porte aperte sfruttate, vulnerabilità o altri compromessi. Se le conclusioni di una valutazione TPISA rivelano o indicano problemi di sicurezza, Citi presenterà tali conclusioni in un documento di notifica al Fornitore, con il quale collaborerà per identificare i mezzi per correggere detti problemi. I Fornitori devono apportare tempestivamente le correzioni necessarie, aggiungere/o compensare i controlli per rispondere ai sospetti di Citi, a sola discrezione di Citi, e rispettare le tempistiche richieste di 180 giorni di calendario per i problemi ad alto rischio, 240 giorni di calendario per i problemi a medio rischio e prima della successiva data di conformità per i problemi a basso rischio, poiché tali problemi sono classificati come rischio da Citi.

1. Il Fornitore deve effettuare regolarmente valutazioni delle sue attività aziendali e dei relativi controlli rispetto ai suoi standard, alle sue policy e alle sue procedure di sicurezza delle informazioni. Le valutazioni periodiche devono comprendere, almeno:
 - a) Valutazione dei processi che il Fornitore utilizza per garantire la conformità alle policy e agli standard di sicurezza delle informazioni;
 - b) Valutazione delle risorse di supporto, come le applicazioni e le infrastrutture utilizzate dal fornitore e i processi di sicurezza delle informazioni utilizzati dai subappaltatori del fornitore (ove applicabile) che supportano le loro attività aziendali o consentire a Citi di effettuare tali valutazioni. La conformità è richiesta nel caso in cui una terza parte firmi un nuovo contratto o rinnovi un contratto esistente con un subappaltatore che accede, elabora, gestisce o smaltisce le informazioni di Citi classificate come riservate o di livello superiore.
2. I problemi identificati a seguito di una valutazione dei rischi in materia di sicurezza delle informazioni dovranno essere documentati e monitorati fino a risoluzione con prove di rimedio fornite a Citi.
3. Se la funzione di gestione della sicurezza delle informazioni del Fornitore viene trasferita oltre i confini nazionali, il Fornitore deve ottenere l'approvazione documentata da parte di Citi prima di tale trasferimento.
4. Se il Fornitore acquisisce una nuova entità, deve completare una valutazione dell'entità acquisita sotto il profilo della conformità a questi Standard.
5. Il Fornitore non deve dare in appalto le funzioni di gestione della sicurezza, incluso, a titolo esemplificativo e non esaustivo, la gestione dei firewall, la gestione delle configurazioni di sicurezza, la gestione delle patch o le funzioni di amministrazione della sicurezza delle informazioni (Information Security Administration, ISA), per i sistemi utilizzati per memorizzare, elaborare e/o trasmettere le informazioni di Citi, salvo previa approvazione scritta di Citi.
6. Se il Fornitore ospita un software o un sito web che contiene informazioni di Citi o contiene il marchio di Citi, è necessario eseguire delle valutazioni di vulnerabilità periodiche in accordo con lo Standard System Security Testing Standard (SSTS) di Citi e gli eventuali problemi rilevati durante la valutazione devono essere risolti

entro i tempi previsti dallo Standard. Poiché la SSTS non è approvata per la distribuzione esterna, i Fornitori devono collaborare con il proprio Relationship Manager di Citi per garantire la conformità alla documentazione di riferimento. Inoltre, il Fornitore deve rispettare gli ISO/IEC 27001 Information Security management standards pertinenti (o standard di gestione della sicurezza delle informazioni successivi che stabiliscono standard e protocolli più elevati) e rispettare le disposizioni sulla sicurezza delle informazioni contenute nella presente Sezione (17).

7. Se è necessaria la connettività a server e/o sistemi informatici sulla rete interna di Citi, il Fornitore è tenuto a segnalarlo al proprio principale referente aziendale di Citi in modo che si possa seguire l'attuale processo per la connettività.
8. Il Fornitore deve tempestivamente notificare all'appropriato referente di Citi (Business Activity Owner (BAO) un qualsiasi accesso o acquisizione non autorizzati o la perdita, l'alterazione o la cancellazione delle informazioni di Citi o qualsiasi altra compromissione dei sistemi informatici utilizzati per memorizzare, elaborare o trasmettere le informazioni di Citi.
9. Il Fornitore deve garantire che tutte le attività ad alto rischio o le modifiche ai dati sensibili dispongano di controlli che consentano di attribuire tali azioni alle persone che le hanno eseguite.
10. Il Fornitore deve garantire che tutti i dati sensibili siano mascherati su schermo e su carta (inclusi ad esempio il monitoraggio, le eccezioni, le normative e altri report).
11. Il Fornitore deve limitare la stampa, la registrazione o la copia di dati sensibili, anche con i propri dispositivi. Il Fornitore deve impegnarsi ragionevolmente per restituire o distruggere tutte le informazioni di Citi in un momento concordato o alla fine dell'accordo a meno che non sia proibito da leggi o regolamenti.
12. Il Fornitore deve garantire che tutto il suo personale (dipendenti, appaltatori, interinali, subappaltatori) con accesso alle informazioni di Citi firmi un accordo di non divulgazione o riservatezza.
13. Ai dipendenti del Fornitore deve essere fornito un manuale per i dipendenti o un documento simile che contenga un processo disciplinare per la mancata conformità alle violazioni del codice di condotta del Fornitore e delle policy delle risorse umane che devono essere riconosciute come parte del loro processo di inserimento.
14. Il fornitore dispone di una procedura per recuperare tutti i beni quando un dipendente o un non dipendente viene licenziato o si dimette.
15. Se una qualsiasi informazione riservata viene mantenuta, o in qualsiasi modo archiviata su un sito web o un sistema accessibile dal web, il Fornitore deve divulgare tali informazioni a Citi. Tale informativa potrà essere inclusa nella descrizione dei Servizi. Se il Fornitore conserva o archivia informazioni riservate di Citi, il Fornitore farà eseguire una verifica SSAE 18 (o una qualsiasi valutazione autorevole successiva approvata da Citi) una volta all'anno per la durata del presente Contratto e fornirà a Citi, almeno una volta all'anno, una copia delle relazioni che documentano i risultati di tale controllo SSAE 18 o di qualsiasi valutazione autorevole successiva approvata da Citi.
16. Se il Fornitore viene acquisito o acquisisce un'altra entità tramite una fusione o acquisizione o una transazione simile, e tale transazione avrà probabilmente un impatto sui servizi, il Fornitore deve informare tempestivamente Citi per iscritto e

deve eseguire una valutazione della sicurezza delle informazioni sull'entità risultante, in linea con i presenti Requisiti, per garantire che tale cambiamento non abbia un impatto sulla conformità agli stessi.

17.5 Rischi per la sicurezza delle informazioni con subappaltatori

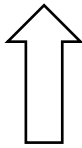
Il Fornitore deve esigere che i subappaltatori con accesso ai dati riservati o di livello superiore di Citi richiedano valutazioni pre-contrattuali e post-contrattuali periodiche della sicurezza delle informazioni (IS) da parte di personale qualificato per la sicurezza delle informazioni. Tali valutazioni devono essere effettuate secondo un processo approvato dalla direzione che tenga conto di tutte le fasi del processo di valutazione, dall'inizio alla gestione del problema. La valutazione dei sistemi informativi del subappaltatore dovrebbe avvalersi di un questionario o di uno strumento equivalente che valuti la posizione del subappaltatore nei domini dei sistemi informativi allineati a quelli inclusi nel questionario di valutazione dei sistemi informativi di terze parti, Third Party IS Assessment Questionnaire (TPAQ) di Citi e includere un metodo logico per calcolare il rischio dei sistemi informativi associato all'interazione con il subappaltatore. Il Fornitore deve monitorare il completamento della valutazione e gestire i problemi rilevati e i piani di azioni correttive fino alla chiusura.

17.6 Responsabilità degli asset

1. Il Fornitore deve garantire che sia mantenuto un inventario di tutte le applicazioni e dell'hardware sotto il suo controllo, utilizzati per memorizzare, elaborare e/o trasmettere le informazioni di Citi.
2. Il Fornitore deve garantire che un inventario del patrimonio informativo di Citi sia mantenuto sotto il suo controllo in conformità al processo utilizzato per mantenere in modo appropriato l'accuratezza e la completezza di tale inventario.
3. Il fornitore deve essere responsabile della protezione di tutte le informazioni di Citi sotto il suo controllo.
4. Il Fornitore deve garantire la responsabilità dell'attività dei propri utenti in modo conforme alla prassi di settore.
5. L'accesso dell'utente agli account e-mail Internet esterni personali deve essere limitato dalla rete globale del Fornitore in cui risiedono le informazioni di Citi.

17.7 Classificazione e gestione delle informazioni

Citi classifica le informazioni in base alla seguente tabella della Classificazione delle informazioni: si prega di consultare l'appendice per le definizioni e gli esempi di ogni classificazione riportata di seguito.

LIMITATE (RESTRICTED)	Le più sensibili
INFORMAZIONI IDENTIFICATIVE PERSONALI PII SENSIBILI	
INFORMAZIONI IDENTIFICATIVE PERSONALI PII RISERVATE	
RISERVATE	
INFORMAZIONI IDENTIFICATIVE PERSONALI PII INTERNE	
INTERNE	
PUBBLICHE	
	Le meno sensibili

1. Sulla base della classificazione delle Informazioni di Citi, Citi deve collaborare con il fornitore per specificare il livello di sicurezza richiesto per proteggere tali informazioni e il fornitore deve garantire che siano attivati controlli sufficienti, nonché tutti i livelli accresciuti o modificati che Citi può successivamente impostare.
2. Le informazioni riservate o di livello più elevato devono essere memorizzate su dispositivi gestiti da terze parti soggetti a un contratto tra la terza parte e Citi che contiene disposizioni di riservatezza coerenti con le policy e gli standard di Citi.
3. Se il Fornitore consente l'uso di dispositivi non di proprietà dell'azienda per memorizzare i dati di Citi (per esempio, dispositivi gestiti da una quarta parte), il Fornitore deve disporre di una policy in atto che richieda l'approvazione specifica della direzione nonché di linee guida e procedure di monitoraggio per l'uso e lo smaltimento delle informazioni di Citi.
4. Il fornitore deve sempre proteggere le informazioni di Citi dall'accesso, la modifica o l'eliminazione non autorizzata.
5. Le informazioni di Citi classificate come riservate o di livello più elevato trasferite tramite mezzi elettronici trasportabili (ETM) devono essere crittografate utilizzando un algoritmo crittografico approvato e la consegna deve essere confermata. Il Fornitore deve confermare che l'ETM è stato ricevuto dal destinatario. Se la conferma di ricezione non viene ricevuta entro la data di consegna prevista, il Fornitore dovrà informare Citi.

17.8 Configurazione sicura

1. Il Fornitore è tenuto a mantenere uno standard di configurazione sicura documentato per tutte le risorse che possono essere utilizzate per archiviare, elaborare, accedere o trasmettere le informazioni di Citi.
2. Il Fornitore deve incorporare procedure di sicurezza delle informazioni nei suoi processi e procedere per la selezione, lo sviluppo e l'implementazione di applicazioni, prodotti e servizi.

3. Il fornitore deve disporre di una procedura di versione sicura per tutti i sistemi in cui le informazioni di Citi sono memorizzate, elaborate e/o trasmesse.
4. Il fornitore deve mantenere un'immagine o un modello sicuri per tutti i sistemi.
5. Tutti gli account utente e le password predefiniti vengono rimossi e/o modificati da sistemi, dispositivi di rete e applicazioni supportati dal fornitore.
6. Qualsiasi sistema o servizio che sia stato compromesso deve essere ricostruito e configurato utilizzando un'immagine o un modello di comprovata integrità.
7. Una modifica da apportare a una configurazione sicura deve essere approvata dalla direzione tramite un processo di gestione delle modifiche.
8. Il Fornitore deve notificare a Citi eventuali modifiche alla configurazione sicura.
9. La procedura della versione sicura deve includere strumenti atti a supportare il controllo automatico della configurazione di sicurezza/standard al momento dell'avvio della produzione e il monitoraggio continuo della conformità o delle modifiche alla configurazione di base.

17.9 Requisiti di crittografia

Il Fornitore non trasmetterà informazioni riservate o ad alto rischio non crittografate. Le informazioni classificate come riservate o di livello più elevato devono essere crittografate **end-to-end** con strumenti o soluzioni approvati da Citi. I protocolli approvati e i rispettivi numeri di versione per la trasmissione crittografata dei dati sono i seguenti:

1. Durante lo scambio di informazioni di autenticazione e autorizzazione: SAML v2.0, OAuth v2.0 (solo autorizzazione),
2. Per proteggere i canali di comunicazione e il relativo scambio di chiavi sono permessi solo i seguenti protocolli di sicurezza della rete:
 - a) TLS v1.3 è preferibile e sono consentite tutte le suite TLS v1.3. Se TLS v1.3 è l'unico protocollo consentito, non è necessaria alcuna altra revisione.
 - b) Se TLS v1.3 non è tecnicamente possibile e TLS v1.2 è consentito, è attualmente accettabile un grado B o superiore da SSLabs e non è necessaria alcuna ulteriore revisione.

I dati archiviati in modo persistente nell'ambiente di terze parti Citi, o quando vengono scambiati, devono essere completamente crittografati utilizzando strumenti e soluzioni approvate da Citi. Gli algoritmi approvati e le lunghezze delle chiavi per la crittografia dei dati sono i seguenti:

1. **Standard di crittografia avanzata (AES):** Lunghezze chiave approvate: 256 o più bit. Modalità limitate: Il modo Electronic Codebook (ECB) è proibito, a meno che la quantità di testo in chiaro sia inferiore o uguale alla lunghezza del blocco. Crittografia dell'unità disco: Si consiglia AES con chiave a 256 bit. Come opzione per il cifrario TLS è consentito l'algoritmo AES con lunghezza della chiave di 128 bit; tuttavia, questi verranno disattivati in favore di 256 o superiore intensità di bit entro il 31 dicembre 2028, per consentire l'allineamento di Citi con le tempistiche internazionali (rif. NIST 8547 IPD).
2. **ChaCha20 (un cifrario a flusso per casi d'uso associati):** Lunghezze chiave approvate: 128 o 256 bit, con nonce a 96 bit e conteggio blocchi a 32

bit oppure nonce a 64 bit e conteggio blocchi a 64 bit. Dimensione massima dei dati: 16 petabyte.

I sistemi crittografici a chiave pubblica approvati, lo scambio di chiavi, i meccanismi di accordo, il digest del messaggio e le funzioni di derivazione della chiave sono i seguenti:

Avviso relativo alla prontezza quantistica del Fornitore: I Fornitori sono tenuti a presentare il loro piano di copertura della *tabella 2* e della *tabella 4* del NIST IR 8547 (ipd) al team del programma Citi Quantum Readiness tramite ([survey link](#)).

1. **Crittosistemi a chiave pubblica e dimensioni minime della lunghezza della chiave:**
 - a) Rivest–Shamir–Adleman (RSA): 2048 bit.
 - b) Digital Signature Algorithm (DSA): 2048 bit. L'algoritmo DSA non deve essere utilizzato per proteggere i dati di Citi elaborati o archiviati al di fuori di Citi.
 - c) Elliptic Curve Digital Signature Algorithm (ECDSA): 256 bit e come specificato in ANSI X9.62 con curve consigliate NIST.
2. **Meccanismi di scambio e accordi di chiavi e dimensioni minime della lunghezza delle chiavi:**
 - a) Diffie-Hellman (DH) / Effimero Diffie-Hellman (DHE): 2048 bit.
 - b) Elliptic-curve Diffie–Hellman (ECDH) / Ephemeral Elliptic-curve Diffie–Hellman (ECDHE): 256 bit e come specificato in ANSI X9.63 con curve consigliate NIST¹.
3. **Funzioni di message digest:** è vietato creare una chiave di crittografia di lunghezza superiore al numero di bit casuali nel materiale utilizzato per generare l'hash.
 - a) SHA-1 Accettabile solo per applicazioni di firma non digitale. Famiglia SHA-2, famiglia SHA-3 e POLY-1305: accettabile per tutte le applicazioni di funzioni di hash crittografiche.
4. **Funzioni di derivazione delle chiavi basate su password e requisiti minimi:**
 - a) PBKDF2: numero minimo di iterazioni di 10000 con un salt di almeno 16 byte.
 - b) HKDF: deve avere un salt e deve essere incluso il valore di input delle informazioni.
 - c) SCRYPT: il numero minimo di round/fattore di costo è 10.
 - d) L'uso di NIST SP800-108 KDF per Stream Encryption è proibito. Sono accettabili le modalità NIST SP 800-108 KDF, vale a dire Counter, Feedback e iterazione a coppia per pipeline.
 - e) Si consiglia Argon2.
5. **Funzioni hash della password e requisiti minimi:**
 - a) Bcrypt (per l'archiviazione locale del materiale di autenticazione): numero minimo di round/fattore di costo di almeno 10.
 - b) Per l'hashing delle password, quando si memorizzano le password localmente su qualsiasi sistema o ambiente distribuito di prodotti del Fornitore, si consiglia di usare Argon2 o PBKDF2.

¹ È preferibile l'ECDHE.

17.10 Posta elettronica esterna

I requisiti di crittografia per le singole e-mail contenenti informazioni ritenute riservate o di livello più elevato secondo la classifica delle informazioni di Citi, in cui il Fornitore non è autorizzato a utilizzare software o strumenti di crittografia end-to-end approvati da Citi in base alla regolamentazione e/o la policy del Fornitore, possono essere soddisfatti pienamente tramite la crittografia di trasmissione (ad es. la crittografia gateway-to-gateway tramite Transport Layer Security (TLS)). I protocolli di posta elettronica sicuri approvati sono:

1. **Identify-Based Encryption (IBE)** che è dotato di posta elettronica crittografata e può essere utilizzato solo nelle soluzioni Citi rivolte ai clienti e solo nei sistemi di posta elettronica e eDelivery.
2. **Mandatory TLS (MTLS)** che è dotato di crittografia della sessione (non crittografia il payload della posta elettronica) ed è destinato all'uso con fornitori, partner e clienti che hanno accordi pre-negoziati per il suo utilizzo.
3. **Domain Keys Identified Mail (DKIM)** che è dotato di autenticazione e gestione delle chiavi e può essere utilizzato con fornitori, partner e clienti.

17.11 Reti private

Le reti private che sono regolamentate in modo indipendente da un'autorità riconosciuta e che rispettano gli standard del settore dei servizi finanziari per l'attività di transazione tra controparti autorizzate o accreditate (ad es. SWIFT o rete di una banca centrale) possono essere considerate esenti dal requisito di crittografia in trasmissione delle informazioni PII riservate fino a quando tali reti non siano in grado di offrire l'infrastruttura necessaria per supportare pienamente le trasmissioni criptate.

17.12 Voce e Fax

Le informazioni con classificazione di riservate o di livello più elevato da parte di Citi inviate via fax o discusse durante le chiamate vocali (incluso Voice Over IP [VOIP]) possono essere inviate non crittografate. Quando richiesto, il Fornitore deve sviluppare procedure e linee guida specifiche per proteggere le informazioni riservate o di livello più elevato inviate tramite questi canali.

17.13 Gestione della chiave crittografica e dei certificati

Il termine limite sicuro utilizzato in questa sezione si riferisce a un programma di convalida Cryptographic Module Validation Program (CMVP), come Federal Information Protection Standard (FIPS), il limite convalidato (FIPS 140-2/3 Livello 2 è il livello di sicurezza minimo accettabile). (Sono accettabili enclave di elaborazione riservate come AWS Nitro Enclaves. Altri casi di sicurezza unici devono essere approvati da Citi).

1. Il Fornitore deve implementare gli attuali algoritmi crittografici standard del settore e le lunghezze minime delle chiavi per la crittografia e la firma (comprese le chiavi SSH). Il Fornitore deve fornire garanzie tramite il processo di gestione delle modifiche quando tali algoritmi e le lunghezze delle chiavi vengono aggiornati per allinearsi agli standard del settore.
2. Il Fornitore deve avere una chiave formale e documentata, segreta, e un processo di gestione del ciclo di vita certificato con controlli in atto per proteggere il materiale sensibile da un uso o un'esposizione non autorizzata. Tutti i segreti sulla crittografia e gli eventi del ciclo di vita delle chiavi devono

verificarsi solo all'interno di un ambiente sicuro. Tutti gli accessi agli ambienti privilegiati e sicuri devono essere ben documentati. Il Fornitore deve fornire un diagramma di sequenza per tutti gli eventi chiave del ciclo di vita evidenziando gli attori, le entità e i confini coinvolti.

3. Le chiavi crittografiche devono avere uno scopo univoco e non devono mai essere utilizzate per altri scopi, ad esempio non utilizzare la stessa chiave di crittografia per la crittografia del disco e dei dati o la stessa chiave di crittografia per la crittografia del carico utile e del database. Il riutilizzo delle chiavi crittografiche in più tenant da parte di un fornitore SaaS è vietato per impostazione predefinita e può essere consentito solo per casi di utilizzo non critici e a basso rischio che coinvolgono informazioni di Citi classificate sotto PII riservate, PII sensibili e Limitate, soggetta all'approvazione esplicita del Security Architecture Council.
4. Per tutte le chiavi crittografiche (simmetriche o asimmetriche), la chiave privata o il materiale della chiave privata (come nodi o parte di una chiave privata) non devono mai essere visualizzati in chiaro. La chiave privata o il materiale della chiave privata (come nodi o parte di una chiave privata) non devono mai oltrepassare il limite sicuro, ad eccezione delle chiavi temporanee come le chiavi di sessione dinamiche. Se il progetto richiede la trasmissione di una chiave simmetrica o di una chiave privata o di materiale di una chiave privata tra enclavi sicure/ambienti di accesso privilegiati, la trasmissione deve avvenire in forma crittografata solo utilizzando un Symmetric Key Wrapping Key o Public Key Transport Key esclusivamente tramite tunnel crittografati TLS reciproci e tale trasmissione deve essere approvata da Citi per iscritto. La Private Key Transport Key non deve mai fuoriuscire dal limite sicuro di accesso privilegiato in cui è stata generata in questi casi.
5. La Symmetric Key Wrapping Key deve essere divisa in due o più componenti chiave ed essere XORed prima della distribuzione e per l'inserimento/caricamento manuale della chiave. La Symmetric Key Wrapping Key deve avere elenchi di controlli di accesso Access Controls Lists (ACLs) adeguati associati all'interno del limite sicuro, come moduli convalidati CMVP, e la chiave Symmetric Key Wrapping non deve mai fuoriuscire dal limite sicuro.
6. L'accesso umano, di servizio o automatizzato agli archivi di chiavi o ai limiti sicuri contenenti chiavi private o segreti o materiale di chiave privata (come nodo o parte di una chiave privata) deve essere adeguatamente segregato con controlli che limitino l'accesso solo al personale o ai sistemi autorizzati.
7. Ogni richiesta di accesso ai keystore contenente chiavi private o simmetriche deve essere registrata e documentata con dettagli tra cui chi, quando e lo scopo dell'accesso a fini di audit.
8. Il Fornitore non deve utilizzare certificati autofirmati e con caratteri jolly o certificati SSL predefiniti.
9. Tutte le chiavi crittografiche devono avere un intervallo di tempo di validità crittografica definito come suggerito in NIST SP800-57 parte 1, revisione 6: Le chiavi devono essere aggiornate o alternate prima della scadenza per adattarsi ai periodi di modifica, ai conflitti di pianificazione e ai blocchi del sistema.

- a) Durante la sostituzione di un certificato scaduto, è vietato il riutilizzo della vecchia coppia di chiavi asimmetriche.
- 10. Le chiavi crittografiche devono essere considerate compromesse, e trattate di conseguenza, non appena si sospetta che l'integrità della chiave, il supporto in cui la chiave è archiviata o condivisa o la riservatezza della chiave simmetrica o privata siano compromessi. Tutte le chiavi compromesse devono essere rimosse dall'uso operativo e tutti i certificati corrispondenti devono essere revocati.
- 11. Le reti wireless devono essere crittografate con algoritmi di crittografia standard del settore.
- 12. I fornitori che utilizzano qualsiasi forma di meccanismo crittografico devono utilizzare strumenti e tecniche di gestione delle chiavi rispondenti agli standard di settore. Il ruolo di gestione chiave deve essere separato dalla gestione operativa.
- 13. I fornitori possono sfruttare KMS e PKI cloud-nativi solo quando l'interoperabilità con i servizi di sicurezza dei dati di Citi forniti PKI & è garantita e il controllo crittografico non viene delegato al di fuori della governance crittografica di Citi.

17.14 Responsabilità dei controlli di accesso

Per proteggere tutti i sistemi informativi controllati utilizzati per archiviare, accedere, gestire, elaborare o trasmettere informazioni riservate di livello più elevato di Citi da accessi non autorizzati, il Fornitore è responsabile di applicare il principio del privilegio minimo, limitando i diritti dell'utente al livello minimo di accesso richiesto per ciascuna funzione lavorativa e gestendo la fornitura di accesso logico a tutti i sistemi e applicazioni. I controlli devono essere completamente documentati e verificabili. La fornitura dell'accesso e il deprovisioning, compreso reimpostare e abilitare la password, sono azioni che devono essere eseguite attraverso un processo automatizzato, ove possibile, per garantire la mitigazione del rischio di potenziali errori umani causati da eccesso di diritti e per allinearsi agli standard del settore.

- 1. Il fornitore è responsabile dei diritti di accesso di tutti gli utenti nella sua organizzazione.
- 2. Il Fornitore deve implementare controlli di accesso che garantiscano agli utenti di ottenere solo quei privilegi e diritti necessari per svolgere la propria funzione.
- 3. Il Fornitore deve implementare un processo per garantire che tutte le funzionalità di accesso predefinite siano rimosse, disattivate o protette per impedire l'utilizzo non autorizzato.

17.15 Gestione dell'accesso degli utenti

Il Fornitore deve gestire la disponibilità dell'accesso logico a sistemi e applicazioni che elaborano, archiviano e/o trasmettono informazioni riservate o di livello più elevato a Citi. Ciò comprende:

- 1. Identificazione e inventario dei sistemi di autenticazione approvati.
- 2. Richiesta che tutti gli accessi ai dati di Citi siano approvati da un responsabile o da un suo incaricato e dal proprietario del sistema. È responsabilità del

Fornitore garantire che a tutto il suo personale con accesso ai dati di Citi venga concesso l'accesso in base alla necessità di dover sapere.

3. Il requisito secondo cui la combinazione di privilegi/funzioni per un singolo utente non possa essere fornita in caso di conflitto di interesse o di una violazione delle regole del maker-checker.
4. Un processo di monitoraggio per monitorare e gestire i diritti di accesso concessi/revocati a ciascun utente del sistema.
5. Le richieste di accesso non devono basarsi sulla replica o sulla clonazione delle autorizzazioni di un altro utente; devono invece specificare esplicitamente i ruoli e le autorizzazioni richiesti, corredati da una giustificazione aziendale, al fine di prevenire l'accumulo progressivo di privilegi (privilege creep) e garantire l'applicazione del principio del privilegio minimo (least privilege).

17.16 Identificazione e autenticazione dell'utente

Tutti i sistemi informatici controllati dal fornitore devono autenticare l'identità degli utenti o dei sistemi che accedono a queste piattaforme prima di avviare una sessione o transazione in cui è possibile accedere alle informazioni di Citi.

1. Gli utenti devono essere identificati univocamente o associati alla piattaforma tecnologica da un ID utente.
2. Gli utenti devono essere autenticati sulla piattaforma tecnologica utilizzando un metodo di autenticazione approvato. Il Fornitore deve contattare il proprio contatto commerciale principale (BAO) per ottenere gli attuali metodi approvati.
3. Gli usi dell'infrastruttura di autenticazione condivisa (ad es. Single Sign-on, Reduced Sign-on e altri servizi di autenticazione condivisi) devono essere usati in conformità con i requisiti di autenticazione di Citi; il Fornitore deve contattare il suo principale referente BAO per ottenere i metodi attualmente approvati.
4. Gli Identity Verification Data (IVD) utilizzati per autenticare un utente in un sistema informativo devono essere crittografati durante la trasmissione e l'archiviazione. Vedere la sezione 17.9 per i requisiti di crittografia.
5. Tutti gli account utilizzati dal personale del Fornitore per accedere ai sistemi Citi devono essere mappati su un identificatore assegnato di Citi univoco (ad esempio, GEID); Gli ID utente generici/condivisi per gli utenti umani sono vietati per garantire la tracciabilità, l'applicazione dei sistemi SOD e la disponibilità agli audit.

17.17 Identificazione degli accessi privati e accesso privilegiato temporaneo

Il Fornitore deve mantenere un inventario di tutte le identità e identificare quelle che hanno accesso privilegiato o hanno accesso agli archivi elettronici (set di dati o database che supportano applicazioni aziendali) che contengono informazioni classificate come

PIL riservate o di livello più elevato. Il Fornitore deve implementare controlli che proteggano dall'uso non autorizzato di queste identità. Se un lavoratore richiede l'accesso a un ID privilegiato o alle responsabilità elettroniche menzionate prima l'accesso deve essere concesso attraverso un processo di gestione degli accessi temporanei che:

1. Imponga al richiedente di essere su un elenco di utenti autorizzati pre-approvati o abbia un'approvazione al momento dell'uso.
2. Richieda una giustificazione documentata in una domanda di modifica/risoluzione dei problemi prima che sia assegnato l'accesso.
3. Includa una revisione indipendente dell'attività svolta con l'accesso.
4. Includa un processo per avviare la revoca/eliminazione dell'accesso al termine della durata di rilascio dell'accesso temporaneo.
5. Consenta di prolungare l'accesso fino a un massimo di sette (7) giorni, in caso di produzione e di stabilizzazione post-implementazione dopo un significativo aggiornamento o un intervento di assistenza.

17.18 Verifica dei diritti di accesso dell'utente

1. Il Fornitore deve implementare un processo documentato per esaminare, verificare ed eliminare i diritti di utente non necessari nei sistemi informatici controllati utilizzati per memorizzare, elaborare, gestire e/o trasmettere le informazioni di Citi almeno ogni sei mesi.
2. Gli utenti non devono esaminare o approvare i propri diritti o i diritti di una persona che ha delegato loro la responsabilità della verifica.
3. A seguito di un cambio di funzione da parte di un dipendente all'interno di Citi, il fornitore ha 14 giorni solari per eseguire una revisione dell'accesso e dei diritti e rimuovere l'accesso ai dati di Citi se non è più necessario per la nuova funzione.

17.19 Procedure di accesso sicuro

1. Gli ID di accesso utente bloccati devono essere nuovamente abilitati tramite un servizio di ripristino conforme agli standard del settore o mediante un'altra funzione autorizzata. Un testo banner, se supportato dal sistema operativo o dall'applicazione, deve essere visualizzato in tutti i punti di ingresso della rete dove un utente si è inizialmente iscritto o è autenticato.

17.20 Sistema di gestione delle password

1. Le password statiche degli utenti non devono mai essere visualizzate sullo schermo in chiaro. La funzionalità di visibilità della password è esente da questo requisito, a condizione che:
 - (1) l'inserimento della password sia mascherato per impostazione predefinita,
 - (2) La visibilità della password possa essere attivata solo da un'azione esplicita dell'utente,
 - (3) La password venga ri-mascherata automaticamente entro un massimo di 15 secondi dopo l'interruzione dell'azione dell'utente.
2. Le password degli ID funzionali privilegiati non devono essere codificate in chiaro.

3. Le password statiche devono contenere un minimo di dieci (10) caratteri, fra cui lettere e numeri e riconoscere maiuscole e minuscole. La sensibilità maiuscola/minuscola delle password statiche deve essere convalidata in ciascun punto di autenticazione. Le password statiche degli ID funzionali (FID) devono contenere un minimo di 15 caratteri sulle applicazioni implementate dopo il 31 agosto 2026.
4. I PIN possono essere utilizzati come unico metodo di autenticazione per accedere ai sistemi informatici solo se i PIN sono necessari per soddisfare le limitazioni del dispositivo fisico (ad es. tastiera, telefono, smart card).
5. Tutte le password statiche devono essere modificate come minimo ogni 90 giorni di calendario.
6. Tutte le password statiche devono essere bloccate dopo non più di sei (6) tentativi consecutivi di accesso falliti o dopo sei (6) tentativi consecutivi di reset. Le password devono essere sbloccate tramite una funzione di amministratore dell'ID o sbloccate automaticamente dopo almeno 30 minuti.
7. Tutti i sistemi di autenticazione devono avere un controllo di inattività/non utilizzo dell'accesso non superiore ai 100 giorni di calendario. Se tecnicamente fattibile, gli accessi disabilitati possono essere riabilitati dall'utente o da un'altra funzione autorizzata.
8. Il processo di autenticazione deve garantire che la stessa password non venga utilizzata entro almeno le ultime sei (6) modifiche.

17.21 Utilizzo delle utilità di sistema

Il Fornitore deve assicurarsi che l'utilizzo di programmi di utilità in grado di eludere i controlli del sistema e dell'applicazione (ad es. boot da dispositivi periferici) sia limitato e controllato.

17.22 Tempo sessione - Scaduto

1. Tutti gli utenti di un sistema informatico controllato utilizzato per memorizzare, elaborare e/o trasmettere informazioni di Citi devono eseguire un nuovo accesso e una nuova autenticazione.
2. Agli utenti deve essere chiesto di ripetere l'autenticazione dopo un periodo di inattività non superiore a 30 minuti. L'attività include qualsiasi input al punto terminale (mouse, tastiera, touch screen, ecc.). Laddove la misura sia implementata tramite la protezione dello schermo con password, il riavvio dell'applicazione/la ripetizione della procedura di Single Sign On non sono necessari.

17.23 Cessazione dell'accesso utente

1. In caso di risoluzione del contratto di lavoro o di dimissioni, l'accesso dell'utente o le autorizzazioni che potrebbero consentire l'accesso a dati riservati o di livello più elevato di Citi, l'accesso utente a Desktop/Active Directory, Single Sign-on (SSO), e-mail, token One Time Password (OTP) e l'accesso remoto devono essere immediatamente rimossi.
2. Se un dipendente ha accesso ai sistemi di proprietà e amministrati da Citi, Citi Business Relationship Manager, BAO o il supporto BAO devono essere

informati immediatamente in caso di cambio di funzione o licenziamento di tale dipendente per garantire che il Citi Business Manager inizi la rimozione dell'accesso per i lavoratori licenziati entro la data di cessazione.

3. Quando un dipendente o non dipendente viene licenziato o si dimette il Fornitore dispone di un processo documentato per recuperare l'accesso da tutte le risorse in linea entro i tempi stabiliti nella sezione 17.23.2.
4. Se il Fornitore rileva una qualsiasi anomalia in merito ai punti 17.23.1-17.23.3, deve informare immediatamente il Citi Business Relationship Manager, BAO o il supporto BAO, con una valida motivazione e i controlli a disposizione.

17.24 Accesso remoto

Il Fornitore deve disporre di controlli di accesso remoto per proteggere l'accesso alle reti in grado di archiviare, elaborare o trasmettere dati riservati o di livello più elevato di Citi che includono i seguenti requisiti:

1. L'accesso remoto a sistemi informatici utilizzati per memorizzare, elaborare, gestire e/o trasmettere le informazioni di Citi deve essere protetto dall'utilizzo non autorizzato.
2. Tutti i computer portatili del Fornitore e tutti i computer desktop utilizzati per memorizzare, elaborare e/o trasmettere le informazioni di Citi, utilizzando l'accesso remoto dove esiste un'archiviazione/elaborazione a livello locale di informazioni di Citi ritenute riservate o di livello più elevato, devono essere crittografati utilizzando uno strumento di crittografia che soddisfi gli standard del settore.
3. Le connessioni remote devono essere stabilite solo tramite soluzioni di accesso remoto approvate, che utilizzano l'autenticazione a più fattori (MFA).
4. Le macchine gestite dal Fornitore devono avere un firewall personale attivo quando è collegato direttamente (ovvero non tramite un firewall o un proxy gestiti dal fornitore) a Internet.
5. I dispositivi gestiti dal Fornitore devono essere regolarmente collegati alla rete del Fornitore per ricevere e installare aggiornamenti periodici di software/antivirus onde poter avere accesso completo alla rete. L'accesso limitato può essere consentito per il preciso scopo di aggiornare il dispositivo.
6. Se vengono utilizzati dispositivi non di proprietà e non gestiti dal fornitore per accedere a informazioni riservate o di livello più elevato di Citi, è necessario utilizzare una soluzione autorizzata che non consenta il download sul computer locale. Devono essere in atto i seguenti controlli:
 - a) I dati di Citi non possono essere scaricati su dispositivi personali a meno che non si tratti di una soluzione gestita dall'azienda.
 - b) Il Fornitore deve garantire che tale accesso sia protetto da un'autenticazione basata su un token o certificata, usando tecnologie standard di accesso remoto (ad es. Virtual Desktop Interface (VDI),).
 - c) Le soluzioni di accesso remoto come Terminal Services e VMware Horizon devono essere configurate per disabilitare la condivisione delle note e Drive Mapping su protocolli Blast, PCoIP e per disabilitare protocolli RDP e SSH.
7. Se si usano soft token per l'autenticazione multifattori (Multifactor Authentication, - MFA); come per accedere a un'applicazione software su un dispositivo mobile, il software di autenticazione soft token deve autenticare

l'utente (per esempio, tramite password, dati biometrici, ecc.) e impedirne l'uso se il telefono cellulare è jailbroken o rooted (utilizzando un sistema operativo diverso da quelli certificati e forniti dal fornitore del dispositivo mobile).

8. Tutto il personale del Fornitore, compresi, a titolo esemplificativo ma non esaustivo, i dipendenti permanenti/temporanei, gli appaltatori e i subappaltatori, che richiedono un accesso speciale, privilegiato e/o amministrativo a sistemi, archivi di dati, applicazioni e/o infrastrutture, compresi, ma non solo, amministratori di sistema, amministratori di database, amministratori di controllo degli accessi, amministratori di firewall, amministratori di siti web, ecc, che sono collegati direttamente o indirettamente ai Servizi forniti per Citi, dovranno utilizzare solo l'autenticazione a più fattori e tali accessi saranno registrati e monitorati in modo indipendente dal Fornitore per identificare eventuali attività sospette e/o accessi non autorizzati, in conformità con questi requisiti.
9. Per i dispositivi di proprietà personale e quelli di proprietà di terzi, il Fornitore deve disporre di un metodo o di una soluzione efficace per garantire che tali dispositivi dispongano di una versione del sistema operativo, livelli di patch e soluzioni antivirus e antimalware approvati, prima che tali dispositivi siano consentiti per accedere alla rete.
10. Il Fornitore deve garantire che tutto il suo personale manterrà quanto segue:
 - a) Uno spazio di lavoro remoto privato e dedicato che non contenga alcun dispositivo di assistenza vocale (ad esempio, Siri, Alexa), dispositivi di registrazione video e/o qualsiasi altro dispositivo di ascolto/registrazione di foto, video o audio. A nessun membro non autorizzato del personale sarà consentito visualizzare dati, sistemi, applicazioni che possono apparire sullo/gli schermo/i dei sistemi informatici remoti.
 - b) Il blocco del dispositivo informatico, quando viene lasciato incustodito, per garantire che l'accesso non autorizzato alla visualizzazione dello schermo sia adeguatamente mitigato.

17.25 Politica della scrivania libera

Il personale del fornitore è tenuto a proteggere le informazioni di Citi in tutte le forme, incluse le informazioni fisiche utilizzate o memorizzate nel proprio spazio di lavoro. I fornitori sono tenuti a comunicare questo requisito a tutto il loro personale almeno una volta all'anno tramite un corso IS.

17.26 Sicurezza antincendio

1. Il Fornitore deve rispettare i requisiti legali e normativi applicabili che regolano la sicurezza fisica e la creazione di un ambiente di lavoro sicuro, compresi i codici antincendio locali.
2. Il fornitore deve utilizzare uno o più sistemi di rilevazione, allarme ed estinzione degli incendi. Tali sistemi devono essere sottoposti a ispezione e test ogni anno.

17.27 Sicurezza fisica

1. Le informazioni di Citi devono essere salvate in aree sicure con controlli che limitano l'accesso solo al personale autorizzato.
2. Il Fornitore deve disporre di un sistema di accesso fisico documentato e verificabile.
3. Il Fornitore deve utilizzare una combinazione di sistemi di allarme/anti-intrusione di sicurezza che includano un allarme di sicurezza monitorato da agenti della sicurezza e video sorveglianza come appropriato per l'ambiente e i servizi forniti.
4. Il Fornitore deve disporre di una policy documentata per i visitatori che preveda l'obbligo per tutti i visitatori di fornire un documento d'identità verificabile all'arrivo, all'ingresso e all'uscita.

17.28 Procedure di sicurezza operative e responsabilità

1. Il processo di gestione delle modifiche del Fornitore deve includere controlli chiave dei punti di controllo relativi alla registrazione, revisione, test, approvazione, implementazione e chiusura delle modifiche. Il Fornitore deve inoltre disporre di un processo di modifica di emergenza che richieda che tutte le fasi elencate includano una gerarchia delle approvazioni obbligatorie.
2. Il Fornitore deve disporre di un processo verificabile della gestione che includa (a titolo esemplificativo ma non esaustivo) parametri/indicatori di disponibilità, capacità e prestazioni; valutazione dell'impatto aziendale; monitoraggio proattivo, investigazione e risoluzione dei problemi di prestazione e capacità.
3. Ove applicabile, il Fornitore deve garantire che gli ambienti di laboratorio, sviluppo, test e produzione siano tutti separati fisicamente e/o logicamente tra di loro.

17.29 Sicurezza per lo sviluppo del software

Applicabile ai fornitori che forniscono software sviluppato per l'utilizzo esclusivo da parte di Citi. I Fornitori devono rispettare questi requisiti o dimostrare di disporre di un processo Software Development Lifecycle ("SDLC") documentato e approvato con un approccio equivalente di pari qualità.

17.30 Iniziazione e pianificazione

Il Fornitore deve definire la portata e gli obiettivi della soluzione in linea con i requisiti e gli obblighi contrattuali di Citi. Ciò comprende:

1. Documentazione dei requisiti funzionali e non funzionali;
2. Fornire stime dello sforzo e della tempistica; e
3. Identificazione di tutti i componenti o le dipendenze di terze parti.

Le attività per la conformità, comprese le valutazioni del rischio per la sicurezza, devono essere avviate all'inizio del progetto. I ruoli, le responsabilità e i punti di controllo dell'approvazione devono essere chiaramente comunicati.

Tutti gli ambienti devono essere classificati come Sviluppo (DEV), Test (TEST) o Produzione (PROD) e devono rimanere rigorosamente segregati durante l'intero ciclo di vita. La classificazione dell'ambiente determina i permessi di accesso e il tipo di dati che possono essere elaborati. Il Fornitore deve limitare l'accesso in base alla designazione

dell'ambiente e allineare le implementazioni con il completamento della fase SDLC appropriato per impedire l'accesso o l'esposizione non autorizzati ai dati.

17.31 Progettazione

Il Fornitore deve documentare un approccio progettuale che garantisca che la soluzione fornita soddisfi tutti i requisiti dichiarati (un "Piano di test"). Come minimo, un piano di test deve includere e descrivere:

1. Tutti i test che devono essere eseguiti dal team di sviluppo, inclusi test unitari e test funzionali e non funzionali, e test sugli aspetti delle prestazioni, con tracciabilità ai requisiti;
2. Identificazione del/i revisore/i che confermerà il completamento;
3. Requisiti per i test di sicurezza, come le valutazioni della vulnerabilità e la modellizzazione delle minacce; e
4. L'ambiente di test, l'approccio, il processo e il percorso di promozione.

Deve essere preparata una strategia di rilascio che definisca i prerequisiti e il processo per il rilascio negli ambienti TEST e PROD, inclusi i criteri di disponibilità al rilascio, il contenuto e la cadenza di consegna durante la durata del progetto.

Dove specificato nel Contratto, le distribuzioni di software devono essere confezionate in un formato approvato da Citi utilizzando strumenti e flussi di lavoro approvati da Citi.

17.32 Test

I test devono essere pianificati ed eseguiti in un ambiente controllato per convalidare che la soluzione soddisfi i requisiti definiti e i criteri di successo. I casi di test devono essere tracciabili in base ai requisiti e ai commit del codice.

Il Fornitore deve preparare un rapporto che riassume i risultati del superamento/fallimento, test aggiuntivi eseguiti durante lo sviluppo e qualsiasi test non completato (con i motivi) (un "Rapporto di esito del test"). I difetti e le capacità differite devono essere documentati insieme ai piani di mitigazione per le questioni irrisolte.

Su richiesta di Citi, il Fornitore deve fornire prove di:

1. Un piano di test dettagliato;
2. Completamento del test e risultati dettagliati in un Test Exit Report; e
3. Tracciabilità dei risultati dei test ai requisiti e agli impegni di codice.

17.33 Messa in produzione

Prima della messa in produzione, il Fornitore deve completare tutti i test di sicurezza richiesti, comprese le scansioni delle vulnerabilità e la modellazione delle minacce. Il processo di rilascio deve essere strutturato con registri delle modifiche documentati, strategie di rollback e con le approvazioni richieste. I piani di implementazione e i runbook di implementazione devono includere protocolli di monitoraggio ed escalation.

Dopo la messa in produzione, il Fornitore deve completare gli identificatori di sistema e aggiornare tutti gli artefatti correlati per garantire la disponibilità per gli audit.

17.34 Sicurezza

1. Deve essere inclusa nell'SDLC una valutazione strutturata condotta durante la fase di progettazione dell'SDLC per identificare e affrontare

potenziali rischi per la sicurezza, vulnerabilità e punti deboli architettonici prima che il codice sia scritto (una “Security Design Review”), con controlli preventivi e investigativi in linea con gli standard del settore come OWASP.

2. È necessario applicare pratiche di codifica sicure.
3. Il Fornitore deve incorporare procedure di sicurezza delle informazioni nei suoi processi e procedere per la selezione, lo sviluppo e l'implementazione di applicazioni, prodotti e servizi.
4. Il fornitore deve disporre di una procedura di build sicura per tutti i sistemi in cui le informazioni di Citi sono memorizzate, elaborate e/o trasmesse e deve mantenere un'immagine o un modello sicuri per tutti i sistemi.

17.35 Controlli contro i malware

Il Fornitore deve assicurarsi che siano prese le necessarie precauzioni per prevenire e rilevare l'introduzione di un qualsiasi codice dannoso (ad esempio virus, worm, virus Trojan Horse, adware, spyware, ransomware o altri simili attacchi informatici in grado di compromettere i dati). Il fornitore deve:

1. Implementare, aggiornare e mantenere una tecnologia antivirus e antispyware su tutti i personal computer e le tecnologie su tutti i server della rete locale (LAN), i server di posta elettronica e gli altri dispositivi che memorizzano, elaborano e/o trasmettono i dati di Citi.
2. Avere impostazioni di sicurezza in atto per impedire agli utenti finali di disabilitare l'antivirus/antimalware e le scansioni pianificate.
3. Disporre di procedure automatizzate e gestite centralmente per la configurazione e l'aggiornamento del software antivirus e antimalware
4. Implementare processi per identificare e indirizzare i computer non conformi in cui le firme antivirus o i motori di scansione sono obsoleti.
5. Controllare l'accesso alle porte/interfacce di comunicazione che consentono la connessione a dispositivi esterni inclusi, ma non solo, i supporti di memorizzazione.

17.36 Controlli per i codici mobili

I Fornitori devono garantire l'implementazione di controlli sulle pratiche di sicurezza del codice mobile. Quando l'utilizzo dei codici mobili è autorizzato, la configurazione deve almeno soddisfare tutti gli standard del settore e gli obblighi contrattuali rilevanti di Citi, e il Fornitore deve garantire che il codice mobile autorizzato operi in base a una policy di sicurezza chiaramente definita e documentata e impedire l'esecuzione di un codice mobile non autorizzato.

Per il codice mobile che può influire sul sistema operativo o la piattaforma sottostante (ad es. al di fuori del “sandbox”), il Fornitore deve assicurare quanto segue:

1. Il codice mobile pubblicato dal Fornitore deve essere firmato da un'autorità di certificazione approvata da Citi e il ciclo di vita del certificato deve essere gestito dal Fornitore per far fronte alla scadenza o alla rotazione del certificato.
2. Il codice mobile firmato con i certificati scaduti deve essere rimosso dalla produzione.

17.37 Log di audit

Il Fornitore deve garantire che tutti i sistemi informatici controllati utilizzati per accedere, memorizzare, elaborare, gestire e/o trasmettere i dati di Citi utilizzino audit trail a livello di infrastruttura o di applicazione per registrare quanto segue:

1. Azioni relative alla sicurezza dell'infrastruttura per la piattaforma associata
2. Tutti gli allarmi di sistema associati a un firewall o a un evento di sicurezza generato dai sistemi IDS/IPS
3. Tutti i tentativi di violazione della sicurezza del sistema (ad es. tentativi di login utente falliti)
4. Tentativi non autorizzati di accesso alle risorse (software, dati, processi, ecc.)
5. Azioni dell'amministratore
6. Informazioni relative alla ricezione di informazioni specifiche da parte di un utente o di un altro sistema
7. Tutti gli eventi significativi relativi a transazioni finanziarie e informazioni di Citi che includono in particolare i seguenti elementi:
 - a. aggiornamenti delle transazioni finanziarie
 - b. aggiornamenti dei dati PII riservati o sensibili
 - c. aggiornamenti dei dati riservati
 - d. aggiornamenti dei dati di autenticazione
8. Tutte le sessioni stabilite
9. I dati della sessione come l'ID univoco del dispositivo, devono essere acquisiti, quando tecnicamente fattibile e registrati per le applicazioni connesse a Citi (ad es. siti web e applicazioni mobili) per sostenere le indagini sulle frodi. Questi artefatti devono contenere almeno indirizzi IP. Questi dati devono essere acquisiti per le transazioni di Citi e per l'attività di apertura dei conti di Citi. Le informazioni devono essere acquisite in modo che i dati della sessione possano essere collegati alla transazione o all'apertura del conto.
10. Gli audit trail devono documentare l'attribuzione di un'attività specifica a un individuo specifico per impedirne il ripudio.
11. Gli eventi relativi a Significant Information Security Administration (ISA) significativi devono essere registrati in modo specifico e comprendere i seguenti elementi:
 - a) creazione utente
 - b) Modifica dei diritti di accesso utente
 - c) Cancellazione, creazione, e modifica di profili sui Controlled Information Systems.
 - d) Reimpostazione di password
 - e) modifiche alla configurazione di sicurezza del sistema
 - f) È necessario registrare tutte le attività interattive degli ID funzionali privilegiati.
 - g) I log di sicurezza devono contenere almeno le seguenti informazioni, indipendentemente dal sistema che genera il log, a meno che non sia tecnicamente impossibile:
 - I. data e ora dell'evento (ora in formato UTC)
 - II. ID utente dell'individuo che esegue l'azione
 - III. tipo di evento
 - IV. nome dell'attività o della risorsa interessata
 - V. tipo di accesso (elimina, modifica, ecc.)

- VI. successo o fallimento dell'evento
- VII. fonte (terminale, porta, posizione, IP, nome host, ecc.)

17.38 Protezione delle informazioni di registro o log

Il Fornitore deve garantire l'implementazione di controlli di accesso per preservare l'integrità delle tracce di controllo durante l'avvio, l'arresto, l'archiviazione e la trasmissione.

1. Per impedire modifiche non autorizzate dei log di audit, il Fornitore deve garantire che i log non possano essere sovrascritti o modificati dagli utenti del sistema di cui monitorizzano l'attività.
2. Il Fornitore deve fornire a Citi una procedura di conservazione dei dati di log che definisca il modo in cui vengono gestiti i dati e includa misure di conformità che facciano riferimento a tutti i requisiti legali e normativi applicabili.
3. Gli orologi di tutti i sistemi di elaborazione delle informazioni rilevanti all'interno di un'organizzazione o un dominio di sicurezza devono essere sincronizzati con una fonte temporale accurata.

17.39 Monitoraggio dell'uso dei sistemi

I seguenti eventi devono essere acquisiti, registrati e rivisti direttamente o tramite un processo automatizzato di verifica:

1. Tutti gli allarmi di sistema associati a un episodio di sicurezza generato da firewall o un sistema di rilevamento delle intrusioni (Intrusion Detection Systems, IDS)/sistema di prevenzione delle intrusioni (Intrusion Prevention System, IPS).
2. Tutti gli aggiornamenti delle risorse critiche identificate nella versione standard protetta.
3. Tutte le attività interattive eseguite da qualsiasi ID (funzionale, privilegiato, di sistema, temporaneo, ecc.) con accesso a informazioni classificate come PII riservate o di livello più elevato.
4. Eventi ISA significativi elencati nella sezione relativa alla registrazione di controllo precedente con la seguente eccezione:
 - a) La rimozione dei diritti da un utente, ruolo o profilo quando l'amministrazione della sicurezza delle informazioni viene svolta da un sistema di flussi di lavoro/ottimizzazione automatico con controlli di integrità end-to-end.

17.40 Revisione e correlazione dei log

1. Quando un evento registrato attiva un avviso e l'evento viene rivisto, il Fornitore deve iniziare azioni di follow-up e indagini qualora l'evento indichi che potrebbe essersi verificato un incidente di sicurezza delle informazioni potenzialmente dannoso.
2. Il Fornitore deve garantire che i log di audit siano aggregati a un sistema centrale di gestione dei log quale un sistema SIEM (Security Information and Event Management) o uno strumento di analisi dei log per l'analisi e la revisione della correlazione dei log.

3. I Fornitori devono periodicamente rivedere e adattare la configurazione del loro SIEM o dello strumento di analisi dei log per migliorare l'identificazione degli eventi attuabili.

17.41 Controllo del software operativo

Il Fornitore deve garantire che siano utilizzati solo i sistemi operativi e il software attualmente supportati da un fornitore commerciale approvato nel settore o che rilascino periodicamente e in maniera appropriata patch e aggiornamenti della configurazione per risolvere i problemi di sicurezza.

Il Fornitore deve garantire che venga implementato un processo documentato che specifichi i tempi di risoluzione in cui vengono applicate tutte le patch e le configurazioni di protezione approvate.

A prescindere da eventuali accordi di manutenzione separati tra il Fornitore e Citi, il Fornitore deve garantire che il software sviluppato per Citi, e disciplinato da un contratto di licenza, non consenta l'uso di versioni software non supportate con vulnerabilità note e che il software sia aggiornato e munito delle patch necessarie in modo tempestivo.

Il software applicativo utilizzato per elaborare le informazioni di Citi deve essere acquisito da Fornitori noti e deve essere concesso in licenza, catalogato e supportato.

17.42 Vulnerabilità e gestione delle minacce

1. Il Fornitore deve implementare un processo di gestione delle vulnerabilità e delle minacce che affronti in modo completo e/o includa tutto quanto segue:
 - a. Strumenti e procedure per la scoperta e la gestione delle vulnerabilità in tutte le risorse che possono essere utilizzate per elaborare, archiviare, accedere o trasmettere dati riservati o superiori di Citi.
 - b. Il requisito che le scansioni vengano condotte almeno una volta alla settimana utilizzando la metodologia di reporting e strumenti di vulnerabilità riconosciuta dal settore.
 - c. La classificazione delle vulnerabilità secondo la versione più aggiornata del "Common Vulnerability Scoring System (CVSS)" (vedi <https://www.first.org/cvss>), con tempistiche di risoluzione in base alla gravità.
 - d. Il requisito di testare le correzioni della vulnerabilità prima della distribuzione completa alla produzione.
 - e. Un processo operativo documentato e ripetibile per accelerare la risoluzione delle vulnerabilità critiche.
 - f. Il Fornitore deve tenere traccia delle risorse per tutto il loro ciclo di vita sostenibile per prepararsi agli stati di fine vita (EOL) o fine del supporto del fornitore (EOVS) e disporre di processi in atto per aggiornare o sostituire tali risorse in modo proattivo.
 - g. Qualsiasi vulnerabilità critica CVSS identificata attraverso la raccolta di informazioni, le scansioni di vulnerabilità o i test di penetrazione deve avere la priorità ed essere risolta entro un periodo di tempo ben definito commisurato al rischio di vulnerabilità.

17.43 Applicazioni ospitate da terze parti

Se il Fornitore conserva o archivia le informazioni riservate di Citi o dati più sensibili su un sito web o su un sistema accessibile via Internet, o un sito web col nome di Citi, allora, al fine di proteggersi da una vulnerabilità o da una minaccia che coinvolge prodotti o servizi che riguardano Citi (ciascuno definito una "vulnerabilità"), il Fornitore deve rispettare i requisiti seguenti:

1. Nominare un dipendente del Fornitore per rispondere alle richieste di Citi in merito alla sicurezza informatica.
2. Utilizzare le procedure migliori note all'interno del settore per monitorare almeno a livello settimanale, fonti affidabili di informazioni sulle vulnerabilità della sicurezza informatica, come FIRST, CERT/CC, CISA Known Exploited Vulnerabilities Catalog, e le mailing list dei fornitori, e adottare misure appropriate per ottenere, testare accuratamente, applicare e fornire a Citi pacchetti di servizi, patch, aggiornamenti e soluzioni alternative.
3. Testare, su base almeno trimestrale, l'attuazione delle misure di sicurezza delle informazioni utilizzando strumenti di scansione e/o test di penetrazione delle vulnerabilità della rete, sistema e applicazione.
4. Consentire a Citi o a una terza parte approvata da Citi di eseguire in tempi ragionevoli controlli della vulnerabilità, attacchi etici o altre valutazioni di sicurezza, per verificare la conformità del Fornitore agli obblighi previsti da qualsiasi contratto e dai presenti requisiti, tra cui, a titolo esemplificativo ma non esaustivo, la revisione di policy processi e procedure, la valutazione in loco delle disposizioni di sicurezza fisica, della rete, dei sistemi e delle applicazioni e i test di penetrazione, utilizzando strumenti disponibili sul mercato e/o pratiche standard del settore al fine di effettuare tali ispezioni.
5. Qualsiasi appaltatore che fornirà al Fornitore servizi di valutazione della vulnerabilità deve appartenere all'elenco dei fornitori di servizi di valutazione della vulnerabilità approvato da Citi. Nel caso in cui il Fornitore utilizzi appaltatori o subappaltatori per la fornitura dei Servizi, il Fornitore dovrà, a proprie spese, garantire che qualsiasi valutazione della vulnerabilità richiesta ai sensi dei presenti requisiti sia completata con la stessa tempestività con cui il Fornitore fornirebbe direttamente tali Servizi e dovrà garantire che l'obbligo di qualsiasi appaltatore o subappaltatore di facilitare tali valutazioni sia incluso nel contratto tra Fornitore e appaltatore/subappaltatore relativo al servizio, compreso il linguaggio che autorizza Citi a eseguire tali valutazioni.
6. **Notifica.**
 - a) Nel caso in cui il Fornitore identifichi una vulnerabilità che coinvolge un prodotto o un servizio che interessa Citi, il Fornitore informerà Citi per iscritto entro 24 ore dall'identificazione e includerà una descrizione delle azioni correttive adottate dal Fornitore.
 - b) Qualora il Fornitore venga a conoscenza di una vulnerabilità che coinvolge un prodotto o un servizio che interessa Citi a seguito di una divulgazione pubblica responsabile dei canali di processo (pubblicazione della vulnerabilità nel National Vulnerability Database

(NVD) o tramite il catalogo delle minacce fornito a fornitori di sicurezza esterni), il Fornitore informerà Citi per iscritto entro 24 ore da tale pubblicazione. Ogni notifica includerà informazioni sulla vulnerabilità, l'utilità del sistema per i servizi correlati a Citi (ad esempio, se ospita informazioni su Citi o viene utilizzato nella fornitura di servizi o entrambi), se può essere sfruttato da remoto e il punteggio CVE (Common Vulnerabilities and Exposures). Il Fornitore continuerà a fornire aggiornamenti a Citi finché la vulnerabilità non verrà risolta. Nel caso in cui Citi identifichi una vulnerabilità, Citi può darne comunicazione al Fornitore, e il Fornitore dovrà prontamente porre rimedio alla vulnerabilità in conformità con la presente Sezione.

7. **Correzione.** Per ogni notifica di vulnerabilità fornita ai sensi della presente sezione, la parte notificante valuterà il livello di rischio e l'impatto di tale vulnerabilità in base alla gravità e al rischio per Citi e assegnerà un livello di priorità del rischio in base al Common Vulnerability Scoring System (CVSS) come stabilito nell'Appendice A (vedere <https://www.first.org/cvss>). Una volta assegnato e concordato un livello di rischio, il Fornitore rimedierà a qualsiasi vulnerabilità media, alta o critica identificata. Ove possibile, la correzione di qualsiasi vulnerabilità che abbia un impatto dovrebbe essere resa disponibile in un pacchetto di sicurezza in cambio della versione attualmente distribuita.

Se il Fornitore non è in grado o non vuole porre rimedio alla vulnerabilità in modo soddisfacente per Citi, Citi può rescindere la licenza applicabile senza alcuna ulteriore responsabilità o obbligo finanziario (per la parte rescissa) e il Fornitore dovrà prontamente rimborsare a Citi la parte proporzionale dei costi di licenza pagati.

17.44 Controlli della rete di sicurezza delle comunicazioni

1. Le reti dei fornitori utilizzate per accedere, memorizzare, gestire, elaborare e/o trasmettere le informazioni di Citi devono essere protette dalle minacce e devono essere mantenute per i sistemi informatici che utilizzano la rete.

- a. Le informazioni ritenute confidenziali o di livello superiore in base alla classificazione delle informazioni di Citi non devono essere memorizzate in modo continuativo su un sistema in una zona demilitarizzata esposta a Internet. Le reti utilizzate per accedere, archiviare, gestire, elaborare e/o trasmettere informazioni Citi utilizzando reti locali wireless (WLAN) o altre soluzioni di dispositivi wireless che includono controlli ragionevoli per vietare l'accesso non autorizzato (PEAP-TLS, EAP-TTLS, ecc.) possono essere connesse a reti che contengono informazioni su Citi.
 - b. Tutte le connessioni IP esterne alla rete globale sono protette da un firewall gestito dal Fornitore.
 - c. Un sistema real time di rilevazione delle intrusioni, Intrusion Detection System (IDS) deve essere attivo per controllare e proteggere le connessioni Internet alla propria rete dove sono accessibili, gestite, salvate, elaborate e/o trasmesse le informazioni di Citi.
2. Per tutte le applicazioni Internet a marchio Citi, il Fornitore deve garantire che:
- a. Tutti i servizi ospitati presso i siti del Fornitore dispongano di servizi anti-DDoS (Distributed Denial of Service) approvati da Citi o controlli comparabili convalidati da Citi.
 - b. I firewall esterni devono essere configurati con una regola di rifiuto per impostazione predefinita. Le regole del firewall devono essere configurate in base al principio del minore privilegio e tutti i tentativi di connessione che sono rifiutati dal firewall (per es. la consegna di pacchetti) devono essere annotati/registrati.
 - c. Il traffico di comunicazioni di rete dovrebbe essere negato per impostazione predefinita e consentito per eccezione sulle interfacce gestite. Le eccezioni devono essere molto limitate a fonti, destinazioni e servizi specifici.
 - d. Il traffico delle applicazioni Web dovrebbe avere controlli adeguati ed essere filtrato, ad esempio attraverso firewall per le applicazioni Web.

17.45 Segregazione nelle reti

Il Fornitore deve garantire che tutti i Sistemi Informativi e le applicazioni utilizzate per accedere, archiviare, elaborare, gestire e/o trasmettere le Informazioni Citi e accessibili tramite Internet siano accessibili esclusivamente tramite la zona demilitarizzata (DMZ) del Fornitore.

Durante un evento di emergenza, il Fornitore deve essere in grado di filtrare l'accesso tra parti della rete per ridurre l'impatto degli eventi di sicurezza della rete (ad esempio, il filtraggio delle porte durante un'epidemia di virus).

L'accesso remoto e la sicurezza dell'host devono implementare controlli di accesso basati sui gruppi (ad esempio, personale, subappaltatori) per limitare l'accesso alle risorse di rete nella rete del fornitore. A livello di host, il controllo degli accessi può essere effettuato a livello di gruppo o individuale.

17.46 Identificazione delle apparecchiature nelle reti

Le piattaforme tecnologiche devono identificare e autenticare altre piattaforme tecnologiche in relazione ai livelli di rischio di sicurezza informatica nell'interazione e controlli attenuanti.

1. Solo i dispositivi del Fornitore (hardware inclusi, a titolo esemplificativo, computer fissi e portatili) che sono conformi a questi requisiti e autorizzati dal Fornitore, possono accedere alla rete del Fornitore dove le informazioni di Citi sono memorizzate, elaborate o trasmesse.
2. Solo i dispositivi del Fornitore (ovvero hardware, inclusi, a titolo esemplificativo, desktop, laptop, supporti di archiviazione dati rimovibili) conformi a questi requisiti e autorizzati da Citi possono accedere alla rete Citi.

17.47 Analisi e specifiche dei requisiti di sicurezza

Il Fornitore deve incorporare procedure di sicurezza delle informazioni nei suoi processi e nelle procedure per la selezione, lo sviluppo e l'implementazione di applicazioni, prodotti e servizi.

17.48 Transazioni on-line

1. Dove applicabile, il Fornitore deve avere sistemi informatici che usano password dinamiche o certificati digitali per convalidare le credenziali.
2. Tutti i certificati di entità finale devono essere sostituiti almeno una volta ogni 13 mesi.
3. Tutte le applicazioni del fornitore che archiviano, elaborano, gestiscono o accedono alle informazioni di Citi, ospitano applicazioni Internet con marchio Citi o dispongono di connettività alle risorse di rete di Citi devono:
 - a. Avere un metodo di autenticazione basato sui tipi di Dati/Funzioni cui si accede;
 - b. Eseguire una valutazione della conformità al Multifactor Authentication, (MFA) e implementare le raccomandazioni se richiesto;
 - c. Eseguire una valutazione di Suspicious Activity Monitoring (SAM) onboarding e implementare le raccomandazioni, se necessario;
 - d. In tutti questi casi, il Fornitore deve contattare il proprio principale referente aziendale per i requisiti attuali di Citi.

17.49 Procedure di controllo delle modifiche

1. Il Fornitore deve garantire che le modifiche di configurazione ai firewall, ai sistemi di rilevazione delle intrusioni (Intrusion Detection Systems, IDS) e ai sistemi di prevenzione delle intrusioni (Intrusion Prevention Systems, IPS) siano sottoposte al processo di gestione dei cambiamenti del Fornitore.

2. L'accesso concesso alla produzione tramite ID temporanei deve essere registrato e monitorato per controllare le modifiche apportate all'ambiente.
3. In caso di sistemi informatici controllati che contengono informazioni ritenute riservate o di livello più elevato o con una componente di rischio per la sicurezza delle informazioni in termini di "integrità" o "disponibilità" o "alto" secondo la classificazione di Citi, i log acquisiti in conformità alla Sezione 17.32 (Audit logging) devono essere esaminati dal Fornitore. Le verifiche possono basarsi su un'adeguata metodologia di campionamento fondata sui rischi.
4. La verifica deve convalidare che le modifiche apportate nell'ambito dell'accesso privilegiato temporaneo siano state effettuate come previsto.
5. Il Fornitore deve documentare tutte le modifiche, inclusa la memorizzazione delle prove del processo di revisione.

17.50 Perdita di informazioni

Il Fornitore deve disporre di uno standard di codifica di sicurezza documentato che impedisca la fuga di informazioni, tra cui:

1. Informazioni di sistema dettagliate (ad es. tipo di server e tecnologia).
2. Stack trace ed errori di eccezione che rivelano la struttura ad albero delle directory e il tipo di database sottostante.

17.51 Dati di test

Le informazioni riservate o a più alto rischio, in base alla definizione di Citi, non dovranno essere usate o archiviate dal Fornitore negli ambienti di sviluppo o di test delle applicazioni software, o laboratori, a meno che tali informazioni non vengano de-identificate, mascherate e/o offuscate utilizzando strumenti e metodi che soddisfino gli standard di settore, in modo che tali dati non siano più sensibili altrimenti il Fornitore deve implementare controlli della produzione dal vivo in ambienti di sviluppo o test.

17.52 Accettazione del sistema

Il Fornitore deve aver documentato il processo di gestione dell'ambito del progetto e l'accettazione del sistema che soddisfi i pertinenti standard di settore.

17.53 Segnalazione di debolezza della sicurezza delle informazioni

Il Fornitore deve disporre di un processo per garantire che le vulnerabilità delle applicazioni e delle infrastrutture che comportano una compromissione del patrimonio informativo di Citi siano **segnalate immediatamente a Citi.**

17.54 Responsabilità e procedure per incidenti di sicurezza

1. Un SIRT è un evento di sicurezza che compromette uno dei seguenti, indipendentemente da come o dove si è verificato l'incidente di sicurezza, o chi potrebbe aver causato la compromissione di:
 - La riservatezza, l'integrità o la disponibilità dei dati di Citi.

- La riservatezza, l'integrità o la disponibilità di qualsiasi dato (inclusi i Dati personali) per i quali Citi è soggetta a obblighi contrattuali, legali o normativi.
 - L'integrità o la disponibilità dei sistemi informativi di Citi che archiviano, elaborano o trasmettono i dati di Citi.
2. Per le nostre finalità, la compromissione della riservatezza si riferisce all'esposizione dei dati a una persona non autorizzata o a scenari in cui Citi perde la custodia e il controllo dei dati. Tutti gli incidenti di sicurezza devono essere segnalati immediatamente.
 3. Se il fornitore ha subito un SIRT, il fornitore deve collaborare con Citi per fornire le informazioni richieste da Citi in conformità ai processi di risposta agli incidenti di Citi, analizzando i dati compromessi in modo sufficiente per consentire a Citi di soddisfare i requisiti legali, normativi e/o di governance interna; effettuare tutte le notifiche richieste ai sensi della legge, delle regole o dei regolamenti o desiderate da Citi su base discrezionale e su richiesta di Citi e a spese del fornitore e solo dopo che Citi ha avuto l'opportunità di rivedere e modificare il linguaggio dei modelli di notifica proposto; e il fornitore non deve nominare Citi in tali notifiche a meno che Citi non richieda specificamente di essere nominata per iscritto.

17.55 Protezione da fughe di dati (Data Leakage Prevention, DLP)

Il Fornitore deve implementare i controlli per la prevenzione della fuga di dati (DLP), compreso il monitoraggio dei contenuti e degli endpoint che copre tutto il personale con accesso a dati riservati o superiori di Citi.

Il Fornitore deve disporre di controlli per rilevare e / o impedire che i casi di dati riservati o di livello più elevato di Citi vengano spostati dalla propria rete tramite i seguenti canali:

- a. E-mail non crittografate.
- b. Allegati e-mail crittografate.
- c. Stampa dei dati Citi.
- d. Trasferimenti di dati di Citi a posizioni al di fuori della propria rete (ad esempio tramite FTP).
- e. Tentativi di copia dei dati di Citi di tipo Confidenziale o superiore su supporti rimovibili come unità USB, dischi rigidi rimovibili, unità CD / DVD e altri dispositivi rimovibili con capacità di archiviazione dei dati. Questo privilegio dovrebbe essere impedito per impostazione predefinita.
- f. La soluzione DLP deve registrare e avvisare il Fornitore di tutti gli eventi che rappresentano tentativi (riusciti o bloccati) di spostare, trasportare o copiare dati riservati o di livello più elevato di Citi dalla propria rete ad altre destinazioni. Questo privilegio dovrebbe essere impedito per impostazione predefinita.
- g. Caricamento di dati Citi su siti Web esterni, inclusi siti SaaS/di condivisione file. Questo privilegio dovrebbe essere impedito per impostazione predefinita.

17.56 Navigazione sul web

1. Il Fornitore deve disporre di controlli di accesso al Web per impedire la condivisione di informazioni riservate o di livello più elevato di Citi e l'esposizione a malware o attacchi per i dipendenti che hanno accesso ai dati di Citi.
2. Per i dipendenti che hanno accesso alle informazioni riservate di Citi o di livello più elevato:
 - a. Tutti i tentativi di accesso a URL devono essere registrati.
 - b. Tentativi di accesso a siti che possono essere utilizzati per la condivisione non autorizzata di dati di Citi (ad es. Webmail, chat, social media, archiviazione online, Gen-AI, ecc...) devono essere bloccati.
 - c. L'accesso a siti che possono esporre l'ambiente a malware o attacchi dovrà essere bloccato.
 - d. I tentativi di accedere a siti ritenuti non correlati all'attività commerciale devono essere bloccati.
 - e. Il Fornitore deve iscriversi a un servizio di classificazione degli URL che viene aggiornato regolarmente; tutti gli URL non classificati devono venire bloccati per impostazione predefinita oppure tutti gli URL devono essere bloccati per impostazione predefinita e vengono approvati caso per caso.
 - f. I browser Web utilizzati dal Fornitore sono completamente supportati e aggiornati con gli ultimi aggiornamenti di sicurezza dal fornitore del software.

17.57 Messaggistica elettronica

Le reti di messaggistica istantanea peer-to-peer o altri strumenti di collaborazione Internet non possono essere utilizzati per trasmettere o archiviare le informazioni di Citi al di fuori della rete del Fornitore o da reti che contengono le informazioni di Citi, a meno che non sia stata predisposta una crittografia appropriata per tutti i dati di Citi in conformità con la Sezione 17.9 (Policy on the use of cryptographic controls).

17.58 E-mail

Il Fornitore deve disporre di controlli delle e-mail per impedire la condivisione di informazioni di Citi e l'esposizione a malware o attacchi. Ciò comprende:

1. I file allegati in entrata che entrano nel gateway di posta elettronica vengono scansionati e bloccati se rappresentano un rischio per il sistema.
2. Il software di filtraggio della posta elettronica (Anti-Spam, Anti-Phishing) è in uso ed è aggiornato.
3. Qualsiasi dato Citi riservato o di livello più elevato deve essere crittografato quando inviato al di fuori dell'organizzazione del Fornitore.
4. I client e-mail utilizzati dal Fornitore sono completamente supportati e aggiornati con gli ultimi aggiornamenti di sicurezza del fornitore del software.

17.59 Supporti rimovibili

1. Il Fornitore deve proteggere le Informazioni di Citi indipendentemente dal supporto su cui vengono conservate. Il presente Standard si applica, a titolo esemplificativo e non esaustivo, ai seguenti tipi di supporti su cui sono

archivate le informazioni: carte, cassette, compact disc (CD), libretto degli assegni, dischetti o altri dispositivi di memorizzazione rimovibili, dati stampati in formato cartaceo, dischi magnetici, nastri magnetici, microfilm, microfiche, dischi ottici o documenti cartacei.

2. L'impostazione predefinita per l'accesso ai dispositivi di archiviazione/supporti portatili per i sistemi in cui sono archiviate le informazioni Citi deve essere nessun accesso. Se vengono concesse eccezioni e quindi è consentito l'accesso in lettura e scrittura, i dati devono essere crittografati sul dispositivo multimediale portatile.
3. Se è consentito l'uso di supporti rimovibili, tale utilizzo deve avere un processo di approvazione da parte del management, indicante la logica aziendale che richiede l'uso di supporti rimovibili. I supporti rimovibili devono essere inventariati. I supporti rimovibili che contengono dati di Citi riservati o di livello più elevato devono essere crittografati automaticamente senza che sia richiesta alcuna azione da parte dell'utente.

17.60 Smaltimento dei supporti multimediali

1. Quando le informazioni di Citi ritenute riservate o di livello più elevato sono idonee allo smaltimento in conformità con le istruzioni fornite da Citi (cioè nel momento in cui le informazioni non sono più necessarie o utili a Citi, oltre a qualsiasi periodo di ritenzione aggiuntivo richiesto dalla legge, dai regolamenti e/o dalle policy di Citi), il Fornitore deve eliminare tali informazioni in modo da renderle inutilizzabili e non recuperabili.
2. Per cancellare in modo sicuro i supporti montabili deve essere utilizzato uno strumento approvato che sovrascriva in modo casuale i settori dell'unità con caratteri specifici e diversi, secondo le seguenti regole:
 - a. Per i supporti che memorizzano informazioni classificate come Confidenziali o di livello superiore, lo strumento deve completare tre passaggi sul supporto.
 - b. Smagnetizzare i media (se applicabile).
3. Distruggere fisicamente il supporto per renderlo illeggibile (ad es. fare a pezzi, frantumare le unità).
4. I supporti cartacei e gli altri supporti di memorizzazione non elettronici contenenti informazioni riservate o di livello superiore devono essere raccolti e archiviati in modo sicuro in un apposito "Contenitore riservato" prima dello smaltimento finale. I contenitori riservati devono essere sempre chiusi a chiave e apribili solo dal personale autorizzato.
 - a. Fotocopiatrici, stampanti, fax e qualsiasi altro dispositivo dotato di memoria/archiviazione che possa contenere informazioni Confidenziali o di livello più alto di Citi devono essere anch'essi sanificati.

17.61 Gestione e formazione sulla sicurezza delle informazioni

1. Mantenere un programma appropriato di sensibilizzazione ed istruzione alla sicurezza informatica e alle informazioni che include, ma non solo, prevenire il phishing e altri attacchi di ingegneria sociale, gestire in modo appropriato le informazioni riservate o di livello superiore, la segnalazione degli incidenti di sicurezza e la gestione della risposta.
2. Il Fornitore deve garantire che tutti i dipendenti, compresi gli appaltatori e il personale temporaneo, ricevano un'adeguata formazione e siano istruiti in tema di policy e procedure organizzative pertinenti alle loro funzioni lavorative.
3. Deve garantire che il programma di formazione e sensibilizzazione venga rivisto e aggiornato ogni anno per trattare i rischi e le minacce emergenti, le migliori pratiche attuali e le nuove tecnologie nel panorama della sicurezza informatica.
4. Come minimo, devono essere inclusi i seguenti argomenti:
 - b. Etichettatura e gestione delle informazioni
 - c. Trasmissione sicura (posta elettronica protetta, archiviazione sicura di SharePoint, non invio di dati di proprietà di Citi con messaggi di posta elettronica personali)
 - d. Segnalazione degli incidenti di sicurezza delle informazioni
 - e. Luogo di lavoro sicuro (ad es. utilizzo appropriato di Internet, software non autorizzato, divieti sul download di software non approvato)
 - f. Gestione delle password (ad esempio password complesse, divieto di condivisione delle password)
 - g. Ingegneria dei social (ad esempio Phishing, Spear Fishing, Vishing SMishing)
 - h. Lavoro a distanza (ad esempio connessione protetta/sicura, protezione dei dispositivi personali)
5. Ai dipendenti del Fornitore deve essere assegnata la formazione prima o al momento dell'accesso ai sistemi che ospitano i dati Citi che deve essere completata entro la data di scadenza indicata nella notifica di assegnazione.
 - a. Successivamente, ove consentito dalla legge, la formazione IS dovrà essere erogata a tutto il personale almeno una volta all'anno ove non sia vietato dalla legge.
6. La formazione dovrebbe includere un artefatto per registrare il livello di efficacia (ad esempio un quiz al completamento con un punteggio minimo per superarlo) se permesso dalle leggi locali.

17.62 Programma di gestione del rischio informatico

Il Fornitore deve anche, come minimo, mantenere un adeguato programma di gestione del rischio informatico che includa almeno quanto segue:

1. Mantenere un programma ben definito, documentato e di gestione del rischio di sicurezza delle informazioni, e/o un programma di gestione del rischio operativo che abbia una componente di gestione del rischio informatico/delle informazioni chiaramente definita, che definisca la propensione al rischio informatico del Fornitore e assicuri che il suo rischio informatico si allinei a tale propensione.

2. Mantenere un robusto programma di governance della gestione del rischio di sicurezza che include, a titolo esemplificativo ma non esaustivo, la raccolta e/o l'esecuzione di audit e revisioni di sicurezza che valutano lo stato generale della sicurezza all'interno dell'organizzazione e riferiscono regolarmente almeno annualmente alla leadership esecutiva per rivedere e garantire che la propensione al rischio informatico del Fornitore non è stata violata.
3. Mantenere la conformità agli standard di sicurezza dei dati PCI Data Security Standards (PCI-DSS) applicabili al Fornitore quando il Fornitore elabora, memorizza e/o trasmette transazioni, pagamenti e/o informazioni con carta di credito/debito.
4. Mantenere un piano di gestione delle crisi e un piano di risposta Security incident Response Team (SIRT) coerente con gli standard del settore per garantire che il Fornitore sia in grado di rilevare, contenere, esaminare, rispondere e recuperare da qualsiasi incidente di sicurezza informatica tentato, sospetto e/o reale in modo adeguato.

17.63 Applicazioni, API, codice, sistema e sicurezza dell'infrastruttura

Nel caso in cui il Fornitore ospiti, sviluppi, co-sviluppi, fornisca ambienti di sviluppo e/o fornisca una o più applicazioni software, il Fornitore dovrà eseguire revisioni del codice di tale software e/o patch al software per individuare difetti di sicurezza, prevenire accessi non autorizzati, modifiche e/o inserimento di malware o altre forme di codice dannoso, ed effettuare test di vulnerabilità per garantire che le applicazioni (incluse le API), insieme ai servizi di sistema sottostanti, i sistemi operativi, e le reti siano prive di vulnerabilità e difetti noti che potrebbero causare incidenti di sicurezza, violazioni della privacy, frodi, accesso non autorizzato e/o divulgazione di informazioni private, perdita di integrità delle informazioni elaborate, archiviate o trasmesse dalle applicazioni e/o perdita di disponibilità che potrebbe influire sulla qualità dei prodotti e/o servizi che il Fornitore fornisce a Citi.

17.64 Sicurezza mobile

Laddove il Fornitore fornisca una soluzione di app mobile, il Fornitore deve rispettare i seguenti requisiti:

1. L'applicazione mobile deve supportare solo la versione generalmente disponibile (GA)/stabile e non EOL ² delle piattaforme Google Android (escluso Android Go) e/o Apple iOS / iPadOS. Se la soluzione mobile è dotata di supporto per sistemi operativi aggiuntivi, i sistemi operativi/le versioni supportati dovranno essere configurabili da Citi
2. La soluzione mobile non deve supportare piattaforme/dispositivi mobili che non sono dotati di set di istruzioni regolari per supportare algoritmi crittografici inclusa, a titolo esemplificativo, la crittografia come specificato nella sezione 17.9 (Requisiti di crittografia) del presente documento.

² Versioni del prodotto attivamente supportate e che ricevono regolarmente aggiornamenti di sicurezza e manutenzione dal proprietario della piattaforma o dal Fornitore.

3. Le versioni pre-produzione del sistema operativo, tra cui, a titolo esemplificativo ma non esaustivo, le versioni/release beta, di accesso anticipato e di anteprima delle funzionalità, non sono consentite nell'ambiente di produzione.
4. Il Fornitore deve essere in grado di fornire un elenco dei componenti integrati di terze parti tra cui, a titolo esemplificativo, librerie software gratuite e open source raggruppate/sfruttate dalla soluzione mobile.
5. L'app mobile deve rispettare i requisiti e le migliori pratiche che consentono la pubblicazione delle applicazioni mobili tramite app store pubblici, come l'App Store di Apple o Google Play Store. Gli store di applicazioni pubblici elencati costituiranno il metodo preferito e principale per distribuire/pubblicare l'applicazione mobile.
6. Le applicazioni mobili Android devono sfruttare lo schema di firma APK v2+. Non è necessario utilizzare lo schema di firma APK versione 1 (noto anche come firma JAR).
7. Il tipo e la lunghezza della chiave di firma dell'applicazione mobile devono essere conformi alla sezione 17.9 - Requisiti di **crittografia** di questo documento.
8. Ciascuna chiave di firma dell'applicazione e il certificato X.509v3 associato devono essere gestiti individualmente e dedicati a un singolo ID applicativo/ID bundle. Le chiavi di firma non devono essere condivise tra le applicazioni.
9. Se un'applicazione mobile richiede la conservazione dei dati sul dispositivo mobile, deve conservare sul dispositivo solo i dati più recenti necessari per gli scopi dell'app/servizio o per il tempo richiesto ai sensi delle norme legali o dei requisiti normativi.
 - a. La raccolta, l'elaborazione e/o l'archiviazione dei dati dell'utente devono essere conformi alle leggi locali incluse, ma non solo, le normative sulla privacy, come il General Data Protection Regulation (GDPR) e la Direttiva 2002/58/CE (ePrivacy) o le normative regionali equivalenti.
 - b. I componenti integrati di terze parti (ad esempio, le librerie) non devono raccogliere, elaborare e/o archiviare dati dell'utente.
10. Le applicazioni mobili non devono rendere accessibile alcun dato applicativo.
 - a. Se è richiesta la condivisione di dati con altre applicazioni, le applicazioni devono sfruttare tecniche, metodi e controlli commercialmente ragionevoli per i rispettivi sistemi operativi per condividere solo la quantità necessaria di dati con il numero minimo di altre applicazioni in cui tale condivisione dei dati è adeguatamente giustificata e documentata.

11. Le applicazioni mobili devono fare affidamento esclusivamente a strutture di comunicazione sicure fornite dai rispettivi sistemi operativi mobili. Per esempio,
 - a. Le applicazioni Android devono dichiarare esplicitamente che il traffico di rete non protetto non è consentito verso alcun dominio di rete nel manifesto dell'applicazione e/o nel file di configurazione di rete.
 - b. Le applicazioni iOS/iPadOS devono far leva su Application Transport Security (ATS) senza alcuna eccezione.
12. I materiali crittografici devono essere vincolati a un archivio di chiavi sicuro supportato da hardware.
13. Le applicazioni mobili devono essere realizzate in modalità rilascio e non devono contenere:
 - a. Nessuna funzionalità o metodo che possa aggirare i controlli di sicurezza,
 - b. Informazioni di debug, come nomi di file del codice sorgente, nomi di variabili, nomi di simboli, commenti, ecc. che possono potenzialmente facilitare il reverse engineering.
14. Le applicazioni mobili devono essere dotate di efficaci meccanismi anti-hook o anti-manomissione per impedire l'immissione di codice dannoso che potrebbe alterare o monitorare il comportamento dell'applicazione in fase di runtime.
15. Le applicazioni mobili devono implementare tecniche complete di anti-debug o anti-reverse engineering/offuscamento per ostacolare gli attacchi di reverse engineering.
16. I pacchetti di applicazioni mobili devono essere dotati di una funzionalità che consente la verifica dell'autenticità e dell'integrità del suo contenuto (ad esempio, utilizzando checksum crittografico e/o firma digitale).
17. Se l'applicazione mobile richiede l'autenticazione dell'utente, i controlli di integrità dell'applicazione e/o del dispositivo devono essere completati prima dell'avvio dell'autenticazione dell'utente.
18. Applicazioni mobili che accedono/elaborano/archiviano una qualsiasi informazione di proprietà di Citi con una classificazione Citi di riservato o superiore e/o per la quale la loro classificazione di rischio IS è Media o superiore devono sfruttare solo modalità biometriche forti (ad esempio, soddisfare o superare la categoria di Classe 3 / Forte come definito nel corrispondente Android Compatibility Definition Document).
19. Le applicazioni mobili devono implementare contromisure per proteggersi dagli attacchi Man-in-the-middle (MitM).
20. Le applicazioni mobili devono essere in grado di rilevare i dispositivi compromessi che includono, a titolo esemplificativo, dispositivi mobili "jailbroken" o "rooted" e reagire in linea con la valutazione del rischio aziendale e i requisiti normativi.

21. Le applicazioni mobili devono implementare un forte legame con il dispositivo per impedire la clonazione del token software (ad esempio, prova di possesso).
22. Le applicazioni mobili devono utilizzare applicazioni/soluzioni per tastiera sicure (ad esempio, quelle integrate/preinstallate nei sistemi operativi mobili).
23. Le notifiche push non devono contenere informazioni sensibili (ad esempio, informazioni di Citi classificate come riservate o di livello più elevato). Tuttavia, la password monouso (OTP) può essere distribuita tramite notifica push.
24. Le soluzioni applicative mobili devono essere dotate della capacità di rifiutare/ignorare i tentativi di comunicazione con client mobili che utilizzano versioni dell'applicazione con vulnerabilità note/sfruttabili.
25. Le applicazioni mobili devono aderire alle migliori pratiche del settore, comprese, a titolo esemplificativo, le tecniche di prevenzione pubblicate nell'[OWASP MobileTop 10](#).
26. Le applicazioni mobili che sfruttano le tecniche di intelligenza artificiale e di apprendimento automatico (AI/ML) devono farlo in modo etico e in conformità con la Sezione 19 - **Error! Reference source not found.** (comprende AI Generativa/AI agentica).
27. L'applicazione mobile deve sfruttare le autorizzazioni minime del dispositivo necessarie per eseguire gli scopi/funzioni che fanno leva su Citi.
28. Le applicazioni mobili non devono memorizzare informazioni non pubbliche su dispositivi di archiviazione esterni/rimovibili, come le schede SD.**Error! Reference source not found.****Error! Reference source not found.**

17.65 Divulgazione di software

Il Fornitore deve dichiarare tutti i componenti software, inclusi, a titolo esemplificativo e non esaustivo, i componenti software open source contenuti in qualsiasi prodotto o servizio fornito a Citi (collettivamente, i “componenti software”). Il Fornitore non aggiornerà, tramite aggiornamento, o in altro modo, alcun componente software open source in alcuna versione dei prodotti o servizi da installare sui Sistemi Citi senza previa comunicazione a Citi in ogni caso. Inoltre, il Fornitore dovrà garantire che i suoi prodotti o servizi non includano componenti software open source concessi in licenza secondo termini che altrimenti assoggetterebbero Citi o le sue affiliate a obblighi non espressamente divulgati e accettati da Citi in un Contratto. Il Fornitore dovrà divulgare a Citi qualsiasi componente software dannoso rilevato all'interno della sua organizzazione, prodotti o servizi entro 30 giorni dalla scoperta. Nello specifico, il Fornitore dovrà divulgare il proprio utilizzo di componenti software open source su ciascun rilascio e versione dei prodotti o servizi tramite la fornitura a Citi di un Software Bill of Materials (“SBOM”) nel formato file OWASP CycloneDX o nel formato file delle specifiche ISO/IEC 5962: 2021 Software Package Data Exchange (SPDX). Tale divulgazione del Fornitore deve includere l'origine dei componenti software (ad esempio il fornitore commerciale, il database integrato, il gestore di pacchetti binari pubblico, il build del codice sorgente, qualsiasi software integrato o fornitore di componenti software curato) e se il Fornitore o una qualsiasi delle sue dipendenze nella catena di fornitura del software ha preso una copia del componente software (noto come “fork”) e successivamente lo ha integrato nel

suo prodotto o servizio come dipendenza del pacchetto o come codice sorgente integrato nel codice sorgente del Fornitore da cui vengono compilati i prodotti e i servizi.

17.66 Modellazione delle minacce

Il Fornitore deve implementare un processo di modellazione delle minacce che affronti in modo completo e/o includa tutto quanto segue:

1. Definizione di ambito: Il Fornitore deve definire chiaramente l'ambito del modello di minaccia, concentrandosi sui componenti software e sui flussi di dati che elaborano, archiviano o trasmettono le informazioni riservate e di livello più elevato di Citi.
2. Identificazione delle minacce: Il Fornitore deve identificare sistematicamente le potenziali minacce e le vulnerabilità rilevanti per la progettazione, l'architettura e l'uso previsto del software, tenendo conto di vari vettori di attacco e attori della minaccia all'inizio del ciclo di vita del design.
3. Analisi dei rischi: Il Fornitore deve analizzare le minacce identificate per valutare il loro potenziale impatto e la loro probabilità, per consentire la definizione delle priorità dei rischi per la sicurezza.
4. Integrazione dei controlli: Il Fornitore deve definire e integrare adeguati controlli di sicurezza e strategie di mitigazione nella progettazione e nello sviluppo del software per affrontare questi rischi prioritari.
5. Documentazione: Il Fornitore deve documentare il modello di minaccia, includendo minacce identificate, rischi associati e le corrispondenti misure di mitigazione implementate.
6. Revisione periodica: Il Fornitore deve rivedere e aggiornare regolarmente i modelli di minaccia, in particolare quando ci sono modifiche significative all'ambiente di progettazione, alle funzionalità o all'implementazione del software.

17.67 Intelligenza artificiale

1. I Fornitori devono implementare e rispettare un solido ciclo di vita dello sviluppo del software sicuro (SSDLC) per tutti i sistemi e le componenti AI/ML forniti o integrati con Citi. Ciò include progettazione, sviluppo, test, implementazione sicuri e manutenzione continua.
2. I sistemi di intelligenza artificiale forniti dal fornitore devono dimostrare l'integrità nelle loro operazioni e dimostrare una solida resistenza agli attacchi avversari. Ciò include meccanismi di implementazione per il rilevamento tempestivo dell'iniezione, la sanificazione degli input e il mantenimento dell'isolamento dei dati.
3. Gli agenti e i componenti di intelligenza artificiale forniti dai fornitori devono interagire con i sistemi e altri strumenti di Citi in modo sicuro. Ciò richiede una solida gestione delle identità e degli accessi, una rigorosa convalida degli argomenti relativi all'esecuzione degli strumenti e l'isolamento delle operazioni degli strumenti ad alto rischio. I meccanismi Human-in-the-Loop (HITL) devono essere incorporati per azioni sensibili o ad alto rischio.
4. I sistemi di intelligenza artificiale del fornitore devono generare log completi, non modificabili e verificabili per tutti gli eventi significativi. Questi log devono essere protetti da manomissione, aggregati e conservati in conformità con le

policy di Citi. Sono necessarie funzionalità di monitoraggio continuo e rilevamento delle anomalie per identificare e avvisare gli incidenti rilevanti per la sicurezza e le attività sospette.

5. I sistemi di intelligenza artificiale del fornitore devono supportare la supervisione umana basata sul rischio, consentendo un intervento appropriato ed essere progettati con chiara responsabilità per gli output e le azioni di intelligenza artificiale. Ciò include la classificazione degli output dei sistemi di IA in base al livello di rischio e la predisposizione di meccanismi che consentano l'intervento e la prevalenza della decisione umana.
6. Tutti gli agenti, i componenti e i sistemi AI forniti dai fornitori devono implementare solidi controlli di gestione delle identità e degli accessi. Ogni interazione con l'intelligenza artificiale deve essere attribuibile a un'identità identificabile (umana o non umana), con autenticazione richiesta per tutti gli accessi. Gli agenti di IA devono utilizzare identità gestite e rispettare il principio del privilegio minimo quando accedono alle risorse di Citi.
 - a. I Fornitori devono prevedere e garantire che a tutti gli agenti di intelligenza artificiale siano assegnate le identità degli agenti della Citi Object Identity Network (COIN), federati con i sistemi IAM (Identity and Access Management) di Citi, per consentire l'applicazione delle policy di sicurezza di Citi, la gestione centralizzata delle identità e la verificabilità.
 - b. I Fornitori devono caricare agenti di terze parti per COIN utilizzando meccanismi di integrazione approvati da Citi, inclusa l'API COIN resa disponibile tramite gateway sicuri (come SSG Gateway o Apigee), e devono garantire che tale caricamento sia eseguito in modo sicuro in conformità con i requisiti di sicurezza applicabili di Citi.
 - c. I Fornitori le cui soluzioni sono ospitate internamente devono generare un token conforme a COIN. I Fornitori le cui soluzioni sono ospitate esternamente e che autenticano le richieste in ingresso mediante un proprio token federato devono disporre di un meccanismo di scambio di token supportato per la conversione in token Citi, ad esempio mediante lo scambio di token Microsoft (MSFT) con token COIN. Qualsiasi nuovo tipo di token che attualmente non è supportato tramite lo scambio deve essere esaminato per l'approvazione dal team IAM di Citi.
7. Laddove i fornitori utilizzino o forniscano server o clienti Model Context Protocol (MCP), devono implementare MCP RFC 7591 comprese tutte le funzionalità opzionali.
8. I sistemi di intelligenza artificiale del fornitore devono proteggere le richieste di sistema e il funzionamento interno dalla divulgazione o manipolazione. La gestione del contesto deve rispettare limiti rigorosi per impedire la fuga di dati tra tenant, utenti o ambienti.
9. I fornitori devono avere documentato le procedure per rilevare, rispondere a, e segnalare incidenti di sicurezza specifici dell'intelligenza artificiale, inclusi attacchi avversi, manipolazione del modello, azioni non autorizzate dell'intelligenza artificiale o violazioni dei dati che coinvolgono sistemi di intelligenza artificiale. Citi deve essere immediatamente informata di tali incidenti.

18 LINEE GUIDA SULLA SICUREZZA DEL POSTO DI LAVORO

Applicabile ai fornitori che accedono/elaborano/gestiscono/archiviano le informazioni di Citi E/O ospitano applicazioni Internet a marchio Citi rivolte ai clienti E/O hanno connettività alle risorse di rete di Citi E/O richiedono un accesso senza scorta ai locali di Citi.

I Fornitori devono salvaguardare i beni materiali e immateriali di Citi e dei suoi clienti. Le risorse di Citi e dei Clienti possono essere utilizzate solo per scopi approvati e nei modi approvati (ad esempio, in conformità con le licenze, i termini e le condizioni applicabili) e solo in relazione agli scopi aziendali di Citi e dei Fornitori di Citi. Le risorse comprendono liquidità, titoli, beni materiali, servizi, piani aziendali, informazioni relative a Citi, informazioni relative ai fornitori, le informazioni relative ai distributori, la proprietà intellettuale (software, modelli e altri elementi) e tutte le altre informazioni personali, esclusive e riservate. L'appropriazione indebita e la divulgazione non autorizzata degli asset di Citi costituiscono una violazione degli obblighi nei confronti di Citi e possono essere considerate una frode nei confronti di Citi. Allo stesso modo, anche la negligenza, lo spreco o l'uso non autorizzato dei beni di Citi costituiscono una violazione dei vostri doveri nei confronti di Citi.

Voce	Requisiti
Informazioni di Citi (documentazione elettronica e cartacea)	Chiudere a chiave e conservare in sicurezza le informazioni di Citi dopo il normale orario di lavoro e ogni volta che il Fornitore si allontana dall'area di lavoro designata.
Computer desktop personali (PC) e laptop	I PC e i laptop utilizzati per accedere o visualizzare una qualsiasi informazione di Citi devono essere protetti da password per lo screen saver dopo un periodo di inattività. Ogni volta che un Fornitore si allontana dall'area di lavoro designata, deve bloccare il PC e/o il laptop con CTRL + ALT + CANC e selezionare "Blocca computer". Se un Fornitore utilizza un computer portatile per visualizzare le Informazioni di Citi, il Fornitore deve assicurarsi che tale computer portatile sia fissato tramite cavo o lucchetti di sicurezza all'unità di base durante l'orario di lavoro e chiuso a chiave in modo sicuro dopo il normale orario di lavoro.
Chiudere a chiave	Gli schedari e i cassetti in cui sono conservate le informazioni Citi devono essere chiusi a chiave dopo il normale orario di lavoro.
Aree ufficio aperte	Gli spazi open space non devono essere utilizzati come file server o mini data center per archiviare informazioni di Citi, a meno che non siano stati specificamente progettati per tale uso e documentati con Citi.
Stampanti, fotocopiatrici e vassoi per fax	Tutto il materiale correlato a Citi deve essere rimosso da stampanti, fotocopiatrici e fax.
Smaltimento	Smaltire le informazioni di Citi che non sono più necessarie (rispettare specifici programmi di conservazione). I documenti devono essere distrutti o inseriti in un apposito contenitore per la raccolta differenziata sicuro e chiuso a chiave. I supporti magnetici devono essere smaltiti in

Voce	Requisiti
	modo sicuro dopo che sono state rispettate le appropriate procedure di cancellazione.

19 INTELLIGENZA ARTIFICIALE/APPRENDIMENTO AUTOMATICO (INCLUDE L'INTELLIGENZA ARTIFICIALE GENERATIVA/L'INTELLIGENZA ARTIFICIALE AGENTICA)

Applicabile ai fornitori che utilizzano Intelligenza Artificiale/ Apprendimento automatico (AI/ML), compresa l'intelligenza artificiale generativa/l'intelligenza artificiale agentica, come definito da Citi in questi Requisiti per i fornitori, in qualsiasi parte del prodotto/servizio che stanno fornendo.

19.1 Il Fornitore non utilizzerà, e garantirà che alcun Subappaltatore non utilizzi, AI/ML come descritto di seguito, a meno che tale utilizzo non sia stato concordato tra le Parti nel Programma o nell'ordine di lavoro applicabile ai sensi del Contratto:

- a. Utilizzato, contenuto o altrimenti incorporato in qualsiasi prodotto o servizio per il quale è sotto contratto da fornire direttamente o indirettamente a Citi, o in una sua parte, inclusi prodotti o servizi di terze parti in esso contenuti o incorporati; o
2. Utilizzato in qualsiasi modo nell'esecuzione di qualsiasi Contratto da parte del Fornitore, indipendentemente dal fatto che tale AI/ML sia utilizzato, contenuto o altrimenti incorporato nel prodotto o servizio effettivamente consegnato a Citi; o
3. Utilizzato dal Fornitore in modi che possono esporre le informazioni di Citi a tale AI/ML, incluso, a titolo esemplificativo, qualsiasi AI/ML utilizzato dal Fornitore nelle sue operazioni aziendali non commerciali (ad esempio, la tenuta di registri aziendali, il miglioramento dei processi, la ricerca e lo sviluppo, la conformità e la revisione interna).

19.2 Il mancato rispetto di tali obblighi da parte del Fornitore sarà considerato una violazione sostanziale dei termini del presente Contratto.

19.3 Se richiesto da un'autorità di regolamentazione, nell'ambito di un'ispezione normativa o di un'indagine forense sull'uso dell'AI/ML in qualsiasi parte del prodotto/servizio, il Fornitore deve assistere Citi nel rispondere alla richiesta dell'autorità di regolamentazione, inclusa la conduzione e/o la facilitazione della conduzione di audit degli algoritmi necessari per scoprire le operazioni effettive degli algoritmi che comprendono i modelli AI/ML.

19.4 Devono inoltre essere rispettati i seguenti principi:

Legalità. Il fornitore di AI/ML dovrà rispettare la normativa applicabile.

Finalità e proporzionalità. Il Fornitore non potrà unire i Contenuti o le Informazioni di Citi ai dati del Fornitore o a quelli di terze parti. Il Fornitore non utilizzerà Contenuti o Informazioni di Citi per addestrare AI/ML senza l'approvazione scritta di Citi. Il Fornitore AI/ML non utilizzerà i Contenuti o le Informazioni di Citi, se non nella misura necessaria per la fornitura dei Servizi.

20 RECLAMI DEI CLIENTI

20.1 Un reclamo è una comunicazione orale o scritta, che può essere ricevuta oralmente (di persona o per telefono) o per iscritto (via posta o tramite comunicazioni elettroniche quali e-mail, chat o social media, ecc.), che esprime insoddisfazione da parte di un Cliente, di un non Cliente, di un potenziale Cliente, di un client di Citi, di un potenziale Cliente o di un rappresentante autorizzato del Cliente (collettivamente, "Cliente") in merito a una Policy di Citi, un prodotto o un servizio offerto da o tramite Citi, un dipendente di Citi, un contraente di Citi o un fornitore di servizi terzo che agisce per conto di Citi, o una qualsiasi combinazione di quanto sopra.

20.2 I Fornitori devono rispettare la Citi Customer Complaint Handling Policy, ovvero la politica di gestione dei reclami dei clienti di Citi, nonché tutti gli standard e le procedure Citi applicabili relativi ai reclami. Il Fornitore notificherà per iscritto al proprio contatto commerciale principale presso Citi (o al suo delegato) entro ventiquattro (24) ore qualsiasi comunicazione scritta o orale di insoddisfazione o preoccupazione (ciascuna, un "Reclamo") ricevuta dal Fornitore da un qualsiasi Cliente (o non Cliente o potenziale Cliente, secondo la definizione di Reclamo adottata da Citi) o da qualsiasi Regolatore in relazione ai Servizi forniti dal Fornitore per conto di Citi, o altrimenti correlati a Citi. A meno che Citi non metta a disposizione del Fornitore tale sistema, il Fornitore svilupperà, implementerà e manterrà anche un sistema ("Sistema di monitoraggio") ragionevolmente soddisfacente per Citi per monitorare i Reclami e fornire a Citi, a sua discrezione, una copia dei rapporti o l'accesso al sistema. Il sistema di tracciamento:

- a. categorizza i reclami per tipo, data di ricezione e data in cui la notifica del reclamo è stata fornita a Citi,
- b. monitorizza il percorso di gestione del Reclamo fino alla conclusione/risoluzione, e
- c. provvede a tutte le altre questioni che Citi potrebbe ragionevolmente richiedere. Il sistema di tracciamento deve essere progettato per consentire al Fornitore di stabilire se riceve un numero eccessivo di Reclami riguardanti una questione specifica, in modo che il Fornitore (in consultazione con Citi) possa determinare se esiste un problema sistemico riguardante l'attività del Fornitore o la sua fornitura di Servizi e correggere tempestivamente i problemi.

21 POLITICA DI TRADING E INVESTIMENTO PERSONALE

La politica di trading e investimento personale di Citi, ovvero la Citi Personal Trading and Investment Policy (PTIP), definisce le attività di trading e investimento consentite e vietate, i requisiti di pre-autorizzazione e i requisiti relativi alla tenuta, alla divulgazione e alla sorveglianza dei conti di intermediazione o di trading di una persona interessata. Stabilisce gli standard minimi per promuovere il rispetto delle leggi e dei regolamenti per prevenire un uso inappropriato della posizione o del rapporto di un individuo con Citi, inclusa la conoscenza dell'individuo riguardo (1) Informazioni sostanziali non pubbliche o informazioni riservate (collettivamente, denominate "MNPI") riguardanti Citi o una terza parte; o (2) informazioni riguardanti garanzie, derivazioni e posizioni di merci, transazioni e strategie.

Tutto il personale del Fornitore che necessita di un accesso regolare al MNPI nell'ambito delle proprie responsabilità lavorative presso Citi e che è designato come Persona Coperta e/o Persona con Accesso a Citi deve rispettare i requisiti previsti dal PTIP. Il personale del Fornitore deve ottemperare alle richieste dell'ICRM in merito alla divulgazione dei conti personali, all'autorizzazione preventiva delle attività commerciali personali, alle restrizioni commerciali personali e alla presentazione di dichiarazioni periodiche.

22 BILLING AND INVOICING STANDARDS

In relazione all'impegno di Citi per migliorare la tempestività del servizio e potenziare i controlli, tutti i Fornitori dovranno supportare i metodi preferiti di Citi per l'invio delle fatture, nonché le opzioni preferite di pagamento delle fatture, come dettagliato di seguito:

- Il Fornitore creerà file elettronici da trasmettere a Citi nel formato comunicato da Citi al Fornitore e/o utilizzerà lo strumento Citi iSupplier per inserire i dati di fatturazione/fatturato richiesti per la successiva trasmissione digitale a Citi.
- Il Fornitore fornirà a Citi tutte le informazioni bancarie necessarie e la documentazione di supporto per agevolare il pagamento elettronico al Fornitore e/o utilizzare l'offerta di pagamenti con carta virtuale di Citi (ove disponibile).

Nota: i termini di pagamento vengono calcolati a partire dalla data di ricezione della fattura da parte di Citi.

Per pagare puntualmente e rispettare gli impegni contrattuali, Citi richiede a tutti i Fornitori di includere i seguenti dati di fatturazione e di rispettare le linee guida associate al momento della fatturazione di beni o servizi a Citi:

1. L'entità aziendale Citi corretta, l'indirizzo di fatturazione e il nome del contatto aziendale Citi associato.
2. Numero di fattura, data di fattura e numero dell'ordine di acquisto.
3. Le fatture devono essere inviate alla sede Citi o all'indirizzo e-mail indicato nell'ordine di acquisto Citi.

4. I beni o servizi fatturati devono contenere dettagli chiari e descrittivi all'interno della fattura.
5. Includere solo gli addebiti correnti per la fattura specifica (non includere altri saldi di fatture in sospeso e non pagate).
6. Le fatture devono essere in lingua inglese, inclusa la documentazione giustificativa.

23 POLITICA SULLE ASSENZE OBBLIGATORIE

La Mandatory Absence Policy (Politica sulle assenze obbligatorie) di Citi richiede a individui che svolgono attività sensibili o ad alto rischio, in particolare quelle che riguardano i libri contabili e i registri dell'azienda, di allontanarsi periodicamente da queste mansioni. Questa interruzione forzata ha lo scopo di rafforzare i controlli interni creando opportunità di rilevare potenziali frodi, furti o altre condotte scorrette che potrebbero altrimenti rimanere nascoste. La policy è in linea con le aspettative di supervisione stabilite dal Federal Reserve Board degli Stati Uniti per quanto riguarda le assenze richieste per il personale in posizioni sensibili.

Tutto il personale del Fornitore che ha accesso ai dati sensibili e che nell'ambito delle proprie responsabilità lavorative presso Citi è designato come soggetto "sensibili" deve rispettare i requisiti previsti dalla Mandatory Absence Policy. I soggetti sensibili sono tenuti ogni anno a pianificare e completare per intero un periodo di assenza obbligatorio, seguendo tutte le regole e le restrizioni della policy. Durante questo periodo, non devono eseguire, istruire, autorizzare o approvare attività sensibili, né devono rispondere in modo sostanziale a comunicazioni, comprese le interazioni con i clienti, salvo reindirizzare richieste di copertura. Se il periodo di assenza deve essere interrotto dopo che è iniziato, i responsabili o i contatti commerciali di Citi devono annullarlo nei sistemi di conformità per l'accesso al sistema da ripristinare, dopodiché il lavoratore deve riprogrammare un nuovo periodo di assenza.

APPENDICE - DEFINIZIONI

Air-Gap è una misura di sicurezza in cui un computer, sistema o rete è fisicamente separato da altri computer, sistemi o reti. Un'architettura di backup dei dati con air-gap limita l'esposizione a un attacco informatico e consente il ripristino dei dati fino a un momento prima dell'inizio dell'attacco.

La **legge applicabile** include: (a) le leggi e i regolamenti statali sul pignoramento e (b) le regole, le linee guida e altri comunicati emessi da varie agenzie federali degli Stati Uniti, compreso l'Office of the Comptroller of the Currency (a volte indicati come Red Flag Guidelines and Regulations) che implementano la sezione 114 del Fair and Accurate Credit Transactions Act del 2003

La **zona di disponibilità** è quella in cui il fornitore di servizi cloud ha un gruppo di data center logici. Una zona di disponibilità consiste in uno o più data center discreti provvisti di alimentazione, rete e connettività ridondanti in una regione cloud.

Per **intelligenza artificiale (IA)** si intende un metodo, un sistema o un approccio quantitativo ('tecniche') che emula l'intelligenza umana tramite programmi informatici per elaborare stime, previsioni, raccomandazioni o decisioni in modi che vanno oltre i classici approcci statistici, matematici, econometrici o finanziari. Ciò include tutte le categorie IA stabilite di seguito, nonché le variazioni dell'AI, ad esempio: IA generativa, IA agentica, modelli linguistici di grandi dimensioni, modelli di IA Algenerica (GPAI), ecc.

Le categorie di IA includono:

- **IA statica:** tecniche di IA addestrate manualmente offline o i cui parametri sono programmati in modo esplicito e quindi utilizzati per effettuare stime, previsioni, raccomandazioni o decisioni.
- **IA dinamica:** tecniche che, a differenza della "IA statica", possono aggiornare automaticamente e periodicamente i parametri, nella produzione
- **IA automatica:** tecniche di "IA dinamica" che sono inoltre in grado di modificare automaticamente la loro struttura di base (ad esempio, iperparametri, variabili di input).
- **AI cognitiva:** tecniche in grado di prendere autonomamente decisioni e agire di conseguenza, anche su materie per le quali non sono state specificatamente formate.

Machine Learning (ML) è il sottoinsieme dell'IA che ricava rappresentazioni o inferenze dai dati, senza programmare esplicitamente ogni rappresentazione dei parametri o passaggio del computer, ad esempio attraverso i modelli Random Forest e gli approcci basati su reti neurali. Al contrario, le tecniche di intelligenza artificiale che non fanno parte del sottoinsieme dell'apprendimento automatico ML includono tecniche quali la logica fuzzy e tecniche di analisi delle dipendenze complesse per l'elaborazione del linguaggio naturale.

Il Business Activity Owner (BAO) è un dipendente Citi responsabile dell'esecuzione e della gestione attiva di determinate attività associate ai rapporti con il fornitore.

Introduttore aziendale è un fornitore incaricato da Citi di agire per conto di Citi al fine di identificare nuove opportunità commerciali o gestire i rapporti con i clienti esistenti.

Regalo aziendale: qualsiasi articolo di valore (diverso da un intrattenimento aziendale) dato o ricevuto da un dipendente di Citi in relazione all'attività di Citi o all'attività della parte esterna, generalmente escludendo gli oggetti di valore pari o inferiore a 25 USD.

Informazioni Citi: informazioni che Citi possiede o è obbligata a proteggere durante l'archiviazione, l'elaborazione, la trasmissione o lo smaltimento in formato sia digitale che non digitale.

Le classificazioni delle informazioni di Citi includono:

Riservate sono le informazioni relative alle attività di Citi e/o alle parti correlate che non fanno riferimento a individui e richiedono un elevato livello di protezione. La compromissione della riservatezza, dell'integrità o della disponibilità di tali informazioni potrebbe avere un grave impatto sulle operazioni, sullo stato finanziario, sul franchising o sui clienti aziendali di Citi.

Le **informazioni di identificazione personale riservate** sono informazioni personali su un individuo che potrebbero facilitare attività illecite come furto di identità, frode creditizia o altre frodi finanziarie contro tale individuo. La compromissione della riservatezza, dell'integrità o della disponibilità di queste informazioni potrebbe avere un impatto significativo sugli individui, incluso, a scopo esemplificativo, perdite finanziarie o frodi.

- Gli elementi dei dati personali che, se combinati con altri dati personali, costituiscono PII riservate includono nome individuale o informazioni di contatto (indirizzo, telefono o indirizzo e-mail) in combinazione con:
 - Elementi di dati di transazione che potrebbero comportare movimenti di fondi o che possono essere utilizzati per commettere furti di identità o frodi, come ad esempio:
 - Numero della carta di credito/debito.
 - Valore di verifica della carta (CVV) o PIN
 - Dati del rapporto di credito (punteggio di credito)
 - Data di nascita completa
 - Prestazioni del lavoratore (valutazione/feedback) o informazioni sulla retribuzione
 - Registrazioni video comprendenti registrazioni in CCTV e presso gli sportelli ATM.
- Alcuni elementi di dati personali isolati dovrebbero costituire PII riservate:
 - Un numero di previdenza sociale degli Stati Uniti o un numero di identificazione emesso soltanto dal governo (che sia equivalente nell'uso e/o nello stato di protezione legale al numero di previdenza sociale degli Stati Uniti), numero del passaporto, numero della patente o numero di identificazione utilizzato per la dichiarazione dei redditi.

Interne sono le informazioni che non riguardano un individuo, destinate a scopi commerciali e che richiedono un livello moderato di protezione. La compromissione della riservatezza, dell'integrità o della disponibilità di queste informazioni potrebbe avere un **impatto limitato** su un team o un gruppo di lavoro.

- Le **Informazioni di identificazione personale (PII)** sono ogni tipo di informazione che:
 - Identificano o possono essere utilizzate per identificare un individuo o un nucleo familiare (come nome, firma, indirizzo, identificatore nazionale univoco come

numero di previdenza sociale, codice di registrazione di residenza, data di nascita, numero della patente di guida).

- Si riferiscono, descrivono, possono essere associate o potrebbero essere ragionevolmente collegate (direttamente o indirettamente) a un individuo o famiglia;
- Possono essere utilizzate per autenticare un individuo o fornire l'accesso a un account (ad esempio
- nome utente, indirizzo email, password, PIN, numero di identificazione, risposte a domande di sicurezza); o si riferiscono ad un individuo e che potrebbero essere sensibili (come informazioni mediche o sanitarie personali, numero di conto, valore del conto).
- Le informazioni personali includono anche le informazioni sanitarie protette Protected Health Information (secondo quanto definito dall'Health Insurance Portability and Accountability Act degli Stati Uniti), le informazioni personali sensibili e le informazioni sul credito (definite da varie direttive sulla protezione dei dati/privacy e da varie leggi sul segreto bancario).

Pubbliche sono le informazioni liberamente disponibili al di fuori di Citi o destinate al pubblico utilizzo, come comunicati stampa di Citi o articoli apparsi sui giornali che riguardano Citi.

Limitate sono le informazioni limitate all'uso da parte di persone o gruppi specifici che sono le più sensibili per Citi o le sue affiliate e richiedono il massimo livello di protezione. La compromissione della riservatezza, dell'integrità o della disponibilità di queste informazioni potrebbe avere un **grave impatto (a livello dell'intera azienda, di più regioni, di più settori)** sulle operazioni, sullo stato finanziario, sul franchising o sui clienti aziendali di Citi.

- Le **PII sensibili** sono informazioni personali che secondo leggi specifiche necessitano di ulteriore protezione e che potrebbero essere potenzialmente utilizzate per discriminare illegalmente o causare in altro modo ingiustizie o danni a un individuo. La compromissione della riservatezza, dell'integrità o della disponibilità di queste informazioni potrebbe avere un impatto significativo sull'individuo (tra i quali, a scopo esemplificativo, perdite finanziarie, frode o impatto discriminatorio).
- Dati che si riferiscono specificamente a: razza, religione, credenze religiose o filosofiche, etnia, appartenenza politica od opinioni, appartenenza sindacale, informazioni su precedenti criminali o reati, dati genetici, dati biometrici o dati relativi all'orientamento o all'attività sessuale di un individuo.
- Informazioni sanitarie personali (PHI) che includono informazioni relative alla cartella clinica o alle condizioni mentali o fisiche dell'individuo.

Il **Cliente** è un qualsiasi cliente di Citi, incluse persone fisiche e persone giuridiche quali imprese, istituzioni, organizzazioni ed entità legali.

La **Regione Cloud** è quella in cui il fornitore di servizi cloud raggruppa uno o più data center.

Apparecchiature, sistemi e servizi di comunicazione sono qualsiasi hardware, software o applicazione utilizzata nella trasmissione di comunicazioni elettroniche scritte, vocali o video. I canali eComm includono a scopo esemplificativo: computer, computer portatili, tablet, dispositivi mobili o telefoni cellulari, compresi "Bring Your Own Device" (BYOD), BlackBerry, telefono, fax (servizi di fax), accesso intranet e internet, servizi Wi-Fi, servizi di posta elettronica, servizi di messaggistica istantanea quali Microsoft Lync, Skype e messaggi Bloomberg, siti web e applicazioni con funzioni di comunicazione incorporate, piattaforme per video riunioni o

collaborazione come Zoom o Microsoft Teams, e servizi di social media, servizi interattivi di condivisione delle informazioni, chat room di terze parti, bacheche elettroniche e blog.

Per **Contenuto** si intendono le informazioni riservate di Citi e qualsiasi altro dato, rapporto, statistica o informazione di qualsiasi tipo (a) forniti o resi disponibili direttamente o indirettamente al fornitore da o per conto di Citi o delle sue affiliate o da o per conto dei suoi o dei loro clienti, clienti o fornitori di servizi, (b) creati, prodotti tramite i Servizi, o (c) derivati da uno qualsiasi dei precedenti.

Il **Contratto** è un documento legale scritto firmato da due o più parti che include un'offerta, un'accettazione, un corrispettivo, le obbligazioni delle parti e uno scopo legittimo. Gli esempi dei contratti possono includere gli accordi quadro per prodotti e servizi, le specifiche di lavoro/ordini di lavoro, le modifiche e gli addenda, gli orari, gli ordini o qualsiasi altro documento scritto firmato da un'entità Citi e da un fornitore. Un accordo di non divulgazione (Non-Disclosure Agreement, NDA) è altresì considerato un contratto ai fini di questi Standard.

Test Denial of Access (DOA): convalida la dotazione di personale DEL Fornitore e il supporto ai processi operativi di Citi che possono essere ripristinati all'interno dell'RTO definito.

Test Denial of Service (DOS): convalida che le componenti dell'applicazione e dell'infrastruttura sottostante del fornitore che supportano l'attività di Citi possano essere ripristinate all'interno dell'RTO definito.

Per **"Materiali di deposito"** si intendono le seguenti sottosezioni (i)-(vi), collettivamente, in relazione, ove applicabile, al software concesso in licenza a Citi per il funzionamento nell'ambiente Citi o ai materiali utilizzati dal Fornitore per i Servizi ospitati forniti a Citi:

- (i) Una versione esatta e duplicata del Codice Sorgente per il software utilizzato per lo sviluppo, il funzionamento, la manutenzione e il supporto del software concesso in licenza o dei Servizi Ospitati stabiliti nel contratto applicabile con Citi (e tutte le versioni successive di tale software o Servizi Ospitati) e tutta la Documentazione per tale software (indipendentemente dal fatto che Citi possa già disporre di una copia di parti di tale Codice Sorgente) ("**Deposito del Codice Sorgente**");
- (ii) Il codice sorgente di qualsiasi software di terze parti su cui il Fornitore ha diritti riguardo lo sviluppo, il funzionamento, la manutenzione e il supporto del software concesso in licenza o dei Servizi ospitati;
- (iii) Una copia con licenza di tutti gli strumenti software, quali debugger, assembleri e compilatori necessari per convertire il codice sorgente incluso nei materiali depositati in formato eseguibile, necessario per far funzionare, mantenere e supportare il software o i servizi ospitati;
- (iv) Nella misura non già prevista sopra, qualsiasi Documentazione che fornisca quanto segue: (A) descrizioni e operazioni generali dei Materiali di Deposito; (B) architettura e funzioni di base del programma; (C) informazioni sul flusso di dati; (D) mappa dettagliata della memoria e relativo elenco; (E) mappe delle porte di input/output; e (F) altri dettagli che consentirebbero a un programmatore con competenze ordinarie nei linguaggi di programmazione applicabili di utilizzare e modificare il Codice Sorgente incluso nei Materiali di Deposito;
- (v) Tutte le altre informazioni tecniche relative al software o ai Servizi Ospitati che sarebbero ragionevolmente necessarie per consentire a Citi, o a una terza parte competente per conto di Citi, di utilizzare, gestire, modificare e migliorare il software o i Servizi Ospitati; e
- (vi) Un elenco di tutti i software e le tecnologie di terze parti utilizzati in relazione al software o ai Servizi ospitati, inclusi dettagli ragionevoli riguardanti il loro utilizzo nel software e le

informazioni sul contatto del fornitore di tale software o tecnologia. Citi riconosce e accetta che i Materiali di Deposito non contengono alcun codice sorgente di terze parti, salvo quanto stabilito nella sottosezione (ii); e

(vii) per quanto riguarda i Servizi Ospitati:

- a. una replica ridotta dell'ambiente di produzione ospitato nel cloud o dei materiali specifici dell'ambiente correlati al cloud e di altre informazioni necessarie per replicare l'ambiente di produzione di Citi, inclusi (a scopo esemplificativo ma non esaustivo): infrastruttura come codice, script Terraform, risorse cloud, modelli di formazione cloud, file di configurazione, tenant cloud, abbonamenti cloud, immagini macchina, immagini Docker e infrastruttura come codice sorgente del software; e
- b. una copia dei dati di Citi contenuti nel software.

Comunicazioni elettroniche: messaggi o informazioni inviate, ricevute o utilizzate dal Personale tramite mezzi elettronici, trasmesse via cavo o tramite segnali wireless. Le comunicazioni elettroniche includono, a titolo esemplificativo ma non esaustivo, messaggi di testo, e-mail, messaggi peer-to-peer o istantanei, post di blog, post sui social media, messaggi inviati tramite applicazioni di messaggistica quali WhatsApp, WeChat, Line, Signal o Viber, e includono allegati, screenshot, file vocali o video registrati, audio o video in diretta e file creati, ricevuti, scaricati, archiviati, trasmessi, eliminati o utilizzati tramite apparecchiature, sistemi e servizi di comunicazione elettronica.

ID funzionale: ID generico, come ADMIN o ROOT, che viene utilizzato da una persona o da un processo per accedere a un sistema di sicurezza. Un'iniziativa chiave dell'Identity and Access Management (IAM) garantisce che Citi disponga di controlli specifici definiti per proteggere dai rischi legati all'uso di ID funzionali.

Processi Critici per il Franchising/Applicazioni Critiche per il Franchising (Franchise Critical Application, FCA): processi/applicazioni identificati da Citi come essenziali per il corretto svolgimento delle proprie Funzioni Aziendali Critiche di Franchising

Frode: un atto intenzionale, una dichiarazione errata o un'omissione concepita per ingannare gli altri, con la conseguenza che la vittima subisce una perdita o l'autore del reato ottiene un guadagno

Servizi ospitati: comprendono tutte le Applicazioni installate e tutte le strutture e gli ambienti gestiti o utilizzati dal fornitore per fornire i Servizi ospitati, tutte le applicazioni e gli altri software, i database, i siti web, i server, l'hardware, le reti, le telecomunicazioni e le altre apparecchiature, e altre tecnologie installate o utilizzate nell'ambiente dei Servizi ospitati, e, in ciascun caso, tutti gli aggiornamenti e i servizi di assistenza, ma ad eccezione di tutti i contenuti e i sistemi di Citi.

I **dati di verifica dell'identità (IVD)** sono definiti come domande di sicurezza (SQ) o domande di autenticazione Knowledge Based Authentication (KBA). Le domande di sicurezza vengono generalmente definite dall'applicazione e ricevono risposta dall'utente finale. Esempi sono il nome da nubile della madre, il luogo di nascita, il gelato preferito, ecc. Entrambi i tipi di domande devono essere trattati come dati di autenticazione.

Sicurezza delle informazioni o "IS" (Information Security): lo stato in cui un computer o sistema informatico è protetto da accessi o attacchi non autorizzati e, a causa di tale stato, a) il computer o il sistema informatico continua a essere disponibile e operativo; b) l'integrità del computer o del sistema informatico è mantenuta; e c) l'integrità e la riservatezza delle informazioni memorizzate, elaborate o trasmesse attraverso il computer o il sistema informatico sono mantenute.

Per **minaccia IS** si intende un atto o un'attività (nota o sospetta) eseguita su o tramite un computer o un sistema informatico che potrebbe mettere a repentaglio o influire negativamente sui sistemi informatici di quel o di un altro computer o sistema informatico.

Per **vulnerabilità dei sistemi informativi** si intende qualsiasi vulnerabilità in un computer o sistema informatico che può essere sfruttata da una o più minacce dei sistemi informativi.

Per attività **non legate al cliente/non generatrici di ricavi** si intendono le attività critiche per l'azienda non associate ad attività generatrici di ricavi, tra cui attività legali, di supervisione, normative e attività aziendali di continuità.

Accordo di non divulgazione (Non-Disclosure Agreement, NDA): un accordo tra Citi e un fornitore per cui lo scambio, l'uso e la divulgazione delle informazioni sono disciplinati dai termini dell'accordo.

Per **software open source** si intende il codice source o un programma informatico compilato in cui il codice source è disponibile al pubblico in generale per l'utilizzo o la modifica rispetto al suo design originale.

Personale: indica, sia che sia dichiarato direttamente sia che sia derivato dal contesto, fornitori e affiliati, direttori, funzionari, dipendenti, agenti, revisori dei conti, consulenti, fornitori di servizi e appaltatori (escluso il personale Citi). Il personale del fornitore comprende anche direttori, funzionari, dipendenti, agenti, revisori dei conti, consulenti o altri rappresentanti di qualsiasi Subappaltatore."

Inventario dei documenti: un elenco dettagliato che include i tipi di documenti, la posizione, le date, ecc. dei documenti di Citi ed è necessario all'entità per gestire correttamente i propri documenti attraverso il ciclo di vita delle informazioni.

Il vincolo di conservazione delle informazioni è un requisito imposto ai registri e alle informazioni che ne sospende la modifica o l'eliminazione finché non viene revocata dall'autorità che ha emesso la sospensione.

La **capacità di ripristino** è il volume, la quantità o la velocità di consegna dei prodotti e dei servizi del Fornitore, espressa come percentuale della normale consegna di prodotti e servizi.

La **durata del ripristino** è la durata massima, in giorni di calendario, durante la quale il Fornitore è in grado di sostenere le operazioni mentre è in modalità di ripristino.

L'**Obiettivo del punto di ripristino** è il momento nel passato, espresso in ore, in cui i dati devono essere ripristinati dopo un'interruzione dell'attività. Si tratta del periodo massimo entro il quale i dati di un servizio IT potrebbero andare persi a causa di un incidente grave. L'RPO è solo una misura del periodo di tempo massimo in cui i dati potrebbero andare persi in caso di un incidente grave che colpisce un servizio IT. Non è una misura diretta di quanti dati potrebbero essere persi, ad esempio, fino al termine dell'elaborazione del giorno precedente.

L'**Obiettivo dei tempi di ripristino** è la durata in ore trascorsa tra l'interruzione di un servizio e il ripristino di prodotti e servizi.

"Evento di rilascio" significa uno o più dei seguenti:

- (i) Il fornitore (A) diventa insolvente o ammette la propria incapacità di pagare i propri debiti in generale alla scadenza; (B) diventa soggetto, volontariamente o involontariamente, a un procedimento ai sensi di una qualsiasi legge nazionale o estera in materia di fallimento o insolvenza che non viene completamente sospeso entro sette (7) giorni lavorativi o non viene licenziato o lascia il posto entro quarantacinque (45) giorni dalla presentazione; (C)

effettua una cessione generale a beneficio dei creditori; o (D) ha un curatore, un fiduciario, un custode o un agente simile nominato per ordine di un qualsiasi tribunale di giurisdizione competente per prendere in carico o vendere una qualsiasi parte sostanziale della sua proprietà o attività.

La divisione **Resource Management Organization (RMO)** è responsabile della gestione globale delle risorse end-to-end per Citi, tra cui sourcing strategico, operazioni Purchase to Pay, ufficio del personale e framework di gestione dei fornitori.

Il **Responsabile dell'approvvigionamento RMO** è una persona all'interno della Resource Management Organization (RMO) che è responsabile della negoziazione delle condizioni commerciali del Contratto, dei requisiti e dei prezzi, tra cui l'RFP e altre attività di selezione dei fornitori, l'amministrazione dei termini e delle condizioni del Contratto e i requisiti di accreditamento della valutazione finanziaria.

Per **Effetto negativo grave o catastrofico** sugli individui si intende che l'impatto potrebbe ragionevolmente comportare effetti negativi significativi per l'individuo, tra cui una perdita finanziaria, la perdita del lavoro o la perdita o difficoltà nell'ottenere un impiego, la perdita dei diritti umani, l'umiliazione personale o pubblica o l'ingiusta detenzione in carcere.

Subappaltatore: un subappaltatore è una quarta parte (persona o entità), assunta da una terza parte per eseguire alcuni o tutti i servizi o le attività che Citi ha appaltato alla terza parte.

Guida

Q1: È necessario segnalare tutti i subappaltatori della Terza Parte?

A1: Devono essere segnalati solo i subappaltatori relativi al servizio in esecuzione. Esempi di servizi o attività eseguiti da un subappaltatore includono, a scopo esemplificativo:

*Un subappaltatore che esegue servizi tecnologici o di software che supportano direttamente o indirettamente il servizio/le attività che Citi ha appaltato alla Terza Parte; oppure

*Un subappaltatore i cui servizi includono l'accesso a informazioni riservate di Citi o di livello più elevato; oppure

*Un subappaltatore che ha un'interazione diretta o indiretta con qualsiasi cliente Citi esistente/potenziale; oppure

*Un subappaltatore che non è scortato e svolge servizi di distruzione o archiviazione di documenti Citi all'interno o all'esterno di qualsiasi sede di Citi; oppure

*Un subappaltatore che supporta funzioni o servizi bancari fondamentali quali pagamenti, riscossione, prestito, ecc.

Fornitore: ai fini del presente documento "Requisiti di Citi per i Fornitori", per "Fornitore" si intende esclusivamente una terza parte esterna che ha stipulato un accordo commerciale per fornire prodotti o servizi direttamente a un'entità Citi o per supportare un'entità Citi nel raggiungimento dei propri obiettivi aziendali. Una terza parte esterna è definita come un'entità non Citi. I Fornitori possono anche essere clienti di un'entità Citi o supportare le interazioni con clienti di Citi; tuttavia, gli accordi basati esclusivamente sulla loro condizione di clienti di Citi non sono considerati rapporti di fornitura nell'ambito del presente documento.

Informazioni transitorie: un documento è la versione finale e più completa delle informazioni che Citi è obbligata a conservare per motivi legali, normativi o aziendali approvati. Tutte le altre informazioni sono classificate come "Informazioni transitorie".