REQUISITI DI SICUREZZA PER I FORNITORI

DOCUMENTO PUBBLICO

Redatto da:	DT, Resp. SGSI	In Data:	01/03/2024
Revisionato da	DT	In Data:	01/03/2024
Approvato da	AU	In Data:	01/03/2024

Rev.	Data	Causale	Redazione	Verifica	Firma
0	03/04/2017	Prima emissione	DT	AU	
1	13/01/2020	Aggiornamento e revision requisiti	DT	AU	
2	23/04/2020	Aggiornamento COVID	DT	AU	
3	20/05/2020	Aggiornamento requisiti di sicurezza	DT	AU	
4	01/03/2024	Rimozione requisiti COVID; Integrazione requisiti Cloud	DT	RSGA	

Sommario

1. Introduzione e ambito di applicazione

Nel presente documento viene presentato l'insieme dei requisiti di sicurezza di base di CELDA relativi all'ambito dei servizi erogati da un fornitore e di come CELDA intende assicurare la protezione degli asset della propria organizzazione accessibili da parte dei fornitori stessi, che essi siano primari e/o secondari.
I requisiti di sicurezza delle informazioni per mitigare i rischi associati all'accesso agli asset dell'organizzazione da parte dei fornitori sono concordati con i fornitori stessi e documentati.
Tutti i requisiti relativi alla sicurezza delle informazioni sono stabiliti e concordati con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, trasmettere o fornire informazioni e/o componenti dell'infrastruttura IT e/o, più in generale, delle attività di business di CELDA.
Gli accordi con i fornitori includono i requisiti per affrontare i rischi relativi alla sicurezza delle informazioni e delle comunicazioni dei servizi e prodotti inclusi nella filiera di fornitura per l'ITC.
CELDA ricorre unicamente a fornitori che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, nominando questi ultimi, ove previsto, responsabili del trattamento dei dati personali, come prescritto dall"art. 28 del Regolamento (UE) 2016/679.

CELDA fa appello a due macro-tipologie di fornitori di servizi:

1. da una parte alcune tipologie di servizi, tipicamente quelli ICT e che costituiscono un bene primario anche per CELDA;
2. dall'altra parte quelle tipologie di servizi, tipicamente NON ICT, necessari allo svolgimento delle attività quotidiane dell'azienda;

Lo scopo del presente documento è quindi quello di evidenziare e fornire delle linee guida di carattere generale per gestire le problematiche di sicurezza nell'affidamento a terzi di alcuni dei servizi di CELDA.

2. Requisiti di sicurezza delle informazioni e dei dati generali per i fornitori primari

R.001	Il fornitore deve adottare al proprio interno le procedure e politiche di sicurezza, con particolare riferimento alle modalità di accesso ai sistemi informativi, all'hardening (esempio installazione di soluzioni di end point security) dei dispositivi utilizzati dal fornitore, alla gestione delle informazioni, al trattamento dei dati (anche personali).
R.002	Il fornitore deve possedere la certificazione ISO/IEC 27001 e mantenerla per tutta la durata della fornitura.
R.003	(alternativa al precedente punto) se il fornitore non è certificato ISO/IEC 27001, almeno deve usare un Sistema di Gestione della Qualità.
R.004	Il fornitore deve autorizzare CELDA, con un preavviso di almeno 20 giorni solari, di svolgere attività di auditing secondo modalità concordate con il fornitore
R.005	Le soluzioni e i servizi di sicurezza proposti dal fornitore devono essere aggiornati dal punto di vista tecnologico, con riferimento all'evoluzione degli standard e del mercato; devono essere conformi alle normative e agli standard di riferimento applicabili; devono venire adeguati nel corso del contratto, senza oneri aggiuntivi, alle normative che l'UE o l'Italia rilasceranno in merito a servizi analoghi.
R.006	Il fornitore deve dotarsi delle misure minime di sicurezza per limitare il rischio di attacchi informatici
R.007	Il fornitore deve garantire il rispetto di quanto richiesto dalla normativa vigente in materia di

	sicurezza cibernetica, anche in riferimento ai contenuti del GDPR.
R.008	Il fornitore deve garantire il rispetto di quanto richiesto dalle normative vigenti in materia di trattamento e protezione dei dati personali
R.009	Sulle reti messe a disposizione dal fornitore devono essere presenti di dispositivi di sicurezza perimetrale con funzioni di sicurezza (ad esempio Firewall e sistemi di Network Detection ed Event & Log Monitoring, SIEM, etc.) necessari a rilevare e contenere eventuali incidenti di sicurezza ICT.
R.010	Il fornitore deve prediligere l'utilizzo di protocolli cifrati e meccanismi di autenticazione nell'ambito dei servizi erogati.
R.011	Le strutture del fornitore, preferibilmente, dovranno essere dotate di rilevatore elettronico delle intrusioni e televisione a circuito chiuso (TVCC) nonché di un sistema di controllo degli accessi.
R.012	Il fornitore si impegna a trattare, trasferire e conservare le eventuali repliche dei dati oggetto di fornitura sempre all'interno del territorio dell'UE.
R.013	Il fornitore si impegna a sottoscrivere una clausola di non divulgazione (NDA) sui dati e sulle informazioni trattati per conto di CELDA.
R.014	Il fornitore deve attenersi alla politica di sicurezza della CELDA, con particolare riferimento all'accesso ai dati di CELDA, che avverrà esclusivamente sui sistemi di sviluppo e test.
R.015	Per l'accesso alle strutture della CELDA, il personale del fornitore dovrà essere munito di badge identificativo ed essere registrato nel software di gestione degli accessi. Non sarà consentito l'accesso se non in presenza di un referente CELDA.
R.016	Il fornitore deve assicurare che tutti i beni e i dati CELDA siano trasportati in modo sicuro.
R.017	Il fornitore, in caso di interventi on-site presso le strutture della CELDA, non è autorizzato a: connettersi alla rete dati di quest'ultima, scollegare, spegnere, modificare, rimuovere asset o qualsiasi tipologia di informazione/dato di quest'ultima.
R.018	In caso di intervento tecnico ordinario su qualsiasi tipo di asset su cui transitano o sono archiviati o sono trattati dati di CELDA, il fornitore dovrà prevenire quest'ultima con almeno 72h di anticipo.
R.019	In caso di intervento tecnico straordinario su di un qualsiasi asset su cui transitano o sono archiviati o sono trattati dati di CELDA, il fornitore dovrà prevenire quest'ultima con almeno 4h di anticipo, fornendo la motivazione di tale intervento ed una pianificazione per la sua gestione.
R.020	Il fornitore, al termine del rapporto tra le Parti ed ove non vige un obbligo di legge, dovrà rimuovere ogni informazione, dato, documento, sensibile e non, inerente alle attività svolte per conto di CELDA
R.021	In caso di affidamento di asset aziendali per interventi di manutenzione ordinari o straordinari, il Fornitore dovrà rispettare le clausole di Riservatezza e non divulgazione delle eventuali informazioni sensibili o meno contenute nell'asset.
R.022	Gestione delle interfacce e degli endpoint (API) di servizio: I fornitori devono implementare misure di sicurezza per proteggere le API attraverso cui gli utenti interagiscono con i servizi cloud, inclusa l'autenticazione robusta e la cifratura dei dati.
R.023	Segregazione dei clienti: Deve essere garantita la separazione efficace dei dati e delle risorse dei diversi clienti, per prevenire l'accesso non autorizzato ai dati e alle risorse.
R.024	Gestione delle vulnerabilità: I fornitori devono avere processi formali per la gestione tempestiva delle vulnerabilità nei sistemi cloud, compresa la valutazione periodica delle minacce e la rapida applicazione delle patch di sicurezza.
R.025	Trasferimento di informazioni e uso di crittografia: È richiesto l'uso di tecniche di crittografia e meccanismi di protezione adeguati durante il trasferimento di dati tra il cliente e il servizio

	cloud.
R.026	Gestione degli incidenti di sicurezza: Devono essere implementati processi per la gestione degli incidenti di sicurezza, inclusa la notifica tempestiva agli interessati.
R.027	Politiche per la protezione dei dati personali: Deve essere definita una chiara politica per la protezione dei dati personali, accessibile agli interessati.
R.028	Consentimento e scopo del trattamento: Il trattamento dei dati personali deve essere effettuato solo per gli scopi specificati e con il consenso esplicito degli interessati, quando richiesto.
R.029	Diritti degli interessati: I fornitori devono facilitare l'esercizio dei diritti degli interessati, come il diritto di accesso, rettifica, cancellazione e opposizione al trattamento dei dati personali.
R.030	Sub-processori: I fornitori devono selezionare sottoprocessori che offrano garanzie sufficienti in termini di misure tecniche e organizzative per la protezione dei dati personali.
R.031	Trasparenza e responsabilità: I fornitori devono essere trasparenti riguardo alle pratiche di trattamento dei dati e assumersi la responsabilità in caso di incidenti di sicurezza che coinvolgono dati personali.
R.032	I fornitori devono ottenere la certificazione o sottoporsi a audit periodici per dimostrare la conformità agli standard ISO 27017:2015 e ISO 27018:2019.

3. Sicurezza delle informazioni in caso di accesso limitato

(Rientrano in questa tipologia di attività, senza intento limitativo, i fornitori di cancelleria, gestione degli impianti degli edifici, fornitura di welness e welfare aziendale, altri fornitori accompagnati da personale CELDA)

L'osservanza della presente sezione costituisce requisito applicabile nel caso in cui il fornitore esegua lavori che comportino un accesso limitato alle informazioni CELDA e possano comportare un accesso limitato agli asset di CELDA ed ai dati ed informazioni da questa trattati.

Fatti salvi gli obblighi di riservatezza a cui possa essere soggetto, laddove il fornitore o personale temporaneo accedano alle informazioni di CELDA o dei clienti di CELDA (inclusi i dati personali) correlate a CELDA o ai suoi Clienti, il fornitore dovrà:

- fare in modo che tali informazioni (inclusi i dati personali) non vengano divulgate né consultate da personale temporaneo non impiegato direttamente nei lavori CELDA;
- mantenere (e provvedere affinché tutto il personale temporaneo interessato mantenga) tali informazioni (inclusi i dati personali) in condizioni di sicurezza e riservatezza (ad esempio, senza intento limitativo, mettendo in atto i sistemi e le procedure necessari per salvaguardare la sicurezza di tutte le informazioni appartenenti a, o sotto il controllo di, CELDA nella misura in cui siano in possesso o sotto il controllo del fornitore in conformità alle migliori prassi di settore e implementare tali sistemi e processi in modo rigoroso).

4. Sicurezza delle informazioni generali

Il fornitore avrà cura di trasmettere prontamente a CELDA gli estremi del proprio referente per la sicurezza ed ogni eventuale variazione degli stessi.

All'inizio del contratto, il fornitore provvederà a comunicare per iscritto al referente di CELDA, le aree geografiche in cui vengono erogati i servizi principali, viene assegnato il personale temporaneo interessato o vengono trattate o archiviate le informazioni CELDA. Durante il contratto, il fornitore dovrà inoltre comunicare ogni proposta di modifica dell'area geografica al referente di CELDA, affinché questa possa valutare nuovamente gli eventuali rischi a carico delle informazioni.

Il fornitore provvederà affinché tutti i contratti con i subappaltatori interessati includano clausole scritte che impongano il rispetto, da parte dei subappaltatori stessi, dei requisiti di sicurezza per i fornitori di CELDA, nella misura in cui risultino applicabili.

Queste condizioni devono essere stipulate tra il fornitore e il suo subappaltatore prima che quest'ultimo o un suo addetto possano accedere ai sistemi CELDA e alle informazioni CELDA.

Il fornitore non potrà avvalersi delle informazioni CELDA per finalità diverse da quelle per cui tali informazioni gli sono state trasmesse da CELDA e unicamente nella misura necessarie per consentirgli di dare esecuzione al contratto.

Il fornitore avrà l'obbligo di trattare o utilizzare le informazioni CELDA secondo modalità coerenti con i requisiti di sicurezza, nonché in conformità alla legislazione vigente in materia.

Il fornitore avrà cura di informare il referente di CELDA, qualora si trovi ad essere soggetto a procedure di fusione, acquisizione o cambiamento di proprietà, affinché ci sia possibile valutare nuovamente gli eventuali rischi a carico di CELDA, delle informazioni CELDA o delle informazioni dei clienti di CELDA.

Con cadenza almeno annuale e ogni volta che sopraggiungano variazioni alle forniture o alla modalità con cui vengono fornite, il fornitore dovrà riesaminare i presenti requisiti di sicurezza al fine di accertarne la conformità a tutti i requisiti di sicurezza applicabili.

Il fornitore dovrà gestire in condizioni di sicurezza tutti i Beni materiali CELDA e/o gli asset CELDA assegnatigli dalla stessa CELDA.

Quando inutilizzati, i beni materiali CELDA e gli Articoli CELDA dovranno essere immagazzinati in condizioni di sicurezza. Tali materiali includono, senza intento limitativo, token di accesso remoto, computer portatili CELDA, apparecchiature di rete, server e documentazione.

I beni materiali CELDA non potranno essere allontanati dal luogo di lavoro senza previa autorizzazione.

In relazione all'approvvigionamento delle forniture, il fornitore dovrà attuare procedure formali di gestione degli incidenti riguardanti la sicurezza con responsabilità definite e trattamento "riservato" di tutte le informazioni relative a tali incidenti.

Il fornitore provvederà ad informare il referente di CELDA, entro un ragionevole lasso di tempo da quando giunga a conoscenza di un qualsiasi incidente:

- che comporti perdite materiali, corruzione, danneggiamento o uso improprio di informazioni CELDA, Beni materiali CELDA, articoli CELDA oppure un accesso improprio o non autorizzato ai sistemi CELDA e alle informazioni CELDA, oppure una violazione degli obblighi del fornitore ai sensi dei presenti requisiti di sicurezza;
- che abbia come conseguenza l'incapacità di effettuare le forniture in conformità al contratto;
- causato da azioni che violano i requisiti del presente documento sulla sicurezza.

Dietro ragionevole richiesta, il fornitore trasmetterà sollecitamente a CELDA una relazione scritta contenente un piano di ripristino che includa un calendario e le misure da porre in atto al fine di evitare il reiterarsi dell'incidente.

Il fornitore dovrà garantire un pronto intervento a fronte di ogni rischio identificato a carico della riservatezza, integrità o disponibilità delle informazioni CELDA o dei processi o sistemi del fornitore.

CELDA avrà facoltà di condurre valutazioni dei rischi relativamente a qualsiasi aspetto pertinente del servizio (ad esempio i subappaltatori coinvolti nel servizio) allo scopo di identificare ulteriori rischi a carico di CELDA per effetto dell'approvvigionamento delle forniture, a seconda dei casi. CELDA potrà quindi precisare le opportune contromisure aggiuntive atte a contrastare tali rischi. Gli eventuali costi associati all'attuazione delle contromisure saranno oggetto di accordo tra le parti.

Il fornitore dovrà dotarsi di processi e politiche sulla sicurezza e mantenere una documentazione (di cui copie da mettere a disposizione in lingua inglese) che attestino la conformità ai presenti requisiti di sicurezza, mettendo inoltre a disposizione di CELDA l'accesso alle prove.

Il fornitore disporrà affinché siano in atto procedure e controlli atti a proteggere il trasferimento di informazioni CELDA tramite l'impiego di servizi di comunicazione e-mail, voce, fax e video (accertandosi ad esempio che durante le riunioni in videoconferenza tutti i partecipanti siano autorizzati a discutere di informazioni CELDA).

Il fornitore avrà l'obbligo di implementare procedure atte a contrastare le minacce alla sicurezza dirette o mirate a CELDA o contro un soggetto terzo operante al servizio di CELDA al fine di tutelare adeguatamente le informazioni CELDA.

Il fornitore provvederà affinché le attività lavorative remote aventi attinenza con informazioni CELDA e sistemi CELDA siano soggette a regolari controlli sulla sicurezza nell'ambito dell'organizzazione del fornitore stesso, quali, a titolo di esempio e senza intento limitativo, l'autenticazione avanzata da applicare all'accesso remoto da parte degli utenti.

Alla risoluzione o scadenza del contratto, il fornitore provvederà, e farà in modo che il personale temporaneo e i subappaltatori provvedano, a distruggere in sicurezza e in conformità dei

requisiti di sicurezza, tutte le informazioni CELDA possedute o controllate dal fornitore o dai suoi subappaltatori, salvo diversamente specificato da CELDA, o imposto in forza di un obbligo legislativo o regolamentare. Le informazioni archiviate devono essere poste al di fuori della possibilità di accesso nel corso delle attività aziendali correnti.
Il fornitore dovrà conservare le informazioni CELDA per tutto il tempo necessario a svolgere il servizio, ma non oltre un massimo di due anni, tranne che un diverso periodo di conservazione sia stato specificato da CELDA o sia imposto in osservanza di requisiti legislativi o regolamentari.
Il fornitore dovrà garantire la disponibilità, qualità, integrità e capacità adeguata di offrire la prestazioni di sistema richieste o le forniture con una disponibilità senza interruzioni, assicurando che:

- sia in atto un piano di backup;
- i dati di sistema critici siano protetti (se del caso);
- venga applicata una soluzione alternativa, se ciò costituisce un requisito concordato;
- il sistema o servizio possa essere ripristinato dopo un guasto o un incidente di grave entità;
- il piano venga messo in pratica almeno con cadenza annuale;
- le copie di backup delle informazioni e del software, a seconda dei casi, vengano effettuate e testate regolarmente in conformità ad una politica di backup concordata allo scopo di garantire il ripristino dei dati senza alterazioni.

5. Sicurezza del personale temporaneo

Il personale temporaneo interessato riceverà l'autorizzazione di Accesso unicamente previo completamento della formazione alla sicurezza di CELDA e dei presenti requisiti di sicurezza.
Il corso CELDA sulla sicurezza delle informazioni potrà essere sostituito da una formazione equivalente organizzata dai fornitori sullo stesso tema, salvo approvazione da parte di CELDA.
In seguito, la formazione obbligatoria dovrà essere oggetto di mantenimento.
Il fornitore avrà l'obbligo di conservare i registri della formazione, i quali saranno messi a disposizione per le verifiche condotte da CELDA.
Il fornitore provvederà affinché tutto il personale temporaneo firmi l'accordo di riservatezza del fornitore stesso prima di avviare i lavori negli edifici di CELDA o sui sistemi CELDA o di accedere alle informazioni CELDA. Questi accordi di riservatezza devono essere conservati dal fornitore e messi a disposizione per le verifiche di CELDA nell'ambito delle procedure di audit.
Il fornitore si impegna ad intervenire in caso di violazioni alle politiche e procedure di sicurezza attraverso processi formali quali, se opportuno, azioni disciplinari.

Il fornitore dovrà attivare un servizio riservato di linea telefonica diretta, disponibile al suo intero personale, nella misura consentita dalla legge, che dovrà essere utilizzato dal personale temporaneo qualora riceva istruzioni di agire in modo incongruo rispetto ai presenti requisiti di sicurezza e in violazione degli stessi. Le relative relazioni dovranno essere trasmesse al referente di CELDA.

Quando le forniture cessino di essere assegnate al personale temporaneo, il fornitore provvederà affinché l'accesso alle informazioni CELDA venga revocato e ogni bene, articolo o informazione di CELDA in possesso del personale temporaneo venga restituito al team operativo CELDA competente o distrutto in ottemperanza dei presenti requisiti di sicurezza.

Laddove possibile, il fornitore attiverà una procedura di uscita controllata che includa una richiesta scritta al responsabile operativo di CELDA per la rimozione degli accessi e dell'identità.

Il personale temporaneo dovrà essere informato che l'accordo di riservatezza sottoscritto resta in vigore e che le informazioni CELDA acquisite tramite il lavoro sulle forniture non devono essere divulgate.

Nell'ambito della concessione dell'accesso, il fornitore dovrà conservare ed esibire i registri di tutto il personale temporaneo che necessita di accesso o che sta effettuando forniture CELDA, indicando nominativo, ubicazione dei lavori, indirizzo e-mail professionale e numero di telefono aziendale diretto e interno (se necessario) e/o numero di telefono cellulare, data di richiesta del numero di identificazione utente (UIN, User Id Number) (se posseduto), data di assegnazione del progetto CELDA, data di completamento della formazione obbligatoria, data in cui hanno lasciato il progetto CELDA e una dichiarazione di controllo preliminare all'assunzione. Il referente per la sicurezza del fornitore dovrà accertarsi in permanenza che l'autorizzazione venga rilasciata unicamente al personale temporaneo interessato.

6. Politica e requisiti generici di sicurezza

L'osservanza delle clausole contenute in questa sezione ha carattere vincolante se il fornitore ha accesso a "informazioni sensibili" (come da definizione), oppure svolge funzioni di sviluppo, installazione, manutenzione e supporto di reti o fornisce servizi professionali di IT.

Il fornitore dovrà essere in possesso di certificazione ISO27001 o conformarsi ai requisiti di sicurezza della certificazione ISO27001 o di politiche di sicurezza allineate alla ISO27001 e/o avere avviato la procedura di ottenimento della certificazione ISO27001 entro un lasso di tempo concordato con CELDA. In assenza di tale certificazione, il fornitore dovrà dimostrare a CELDA di essere in grado di gestire in

maniera consona e sicura le informazioni ed i dati a lui affidati e, in ogni caso, essere dotato di un Sistema di Gestione della Qualità ISO9001.

Per i servizi erogati in cloud, i fornitori devono ottenere la certificazione o sottoporsi a audit periodici per dimostrare la conformità agli standard ISO 27017:2015 e ISO 27018:2019.

Se previsto, CELDA potrà periodicamente aggiornare politiche, linee guida e requisiti correlati alla sicurezza e altre disposizioni obbligatorie.
CELDA integrerà gli aggiornamenti in questione nell'ambito di una versione riveduta dei presenti requisiti di sicurezza mediante una richiesta di modifica contrattuale notificata per iscritto al fornitore da CELDA. Gli eventuali costi associati all'introduzione dei nuovi requisiti di sicurezza saranno oggetto di accordo tra le parti.
Il fornitore metterà a disposizione di CELDA copie delle Certificazioni di sicurezza e una dichiarazione di applicabilità relativa ai servizi erogati a sostegno delle prove di messa in conformità rispetto a questo piano

7. Sicurezza fisica - Strutture di CELDA

L'osservanza delle clausole contenute nella presente sezione ha carattere vincolante se il fornitore effettua forniture presso le Strutture di CELDA.
Tutti i membri del personale temporaneo impegnato presso le strutture di CELDA dovranno essere in possesso di una tessera che li identifichi come “fornitore autorizzato” e/o “OSPITE” e/o altro documento analogo fornito da CELDA.
Questa tessera dovrà essere utilizzata permanentemente da ciascun membro del personale temporaneo come strumento di verifica dell'identità presso le strutture di CELDA e dovrà includere una immagine fotografica chiaramente visibile e fedelmente rappresentativa del suo portatore.
Il personale temporaneo potrà essere ugualmente dotato di una scheda di accesso elettronico e/o di una tessera per visitatori a durata limitata, che dovranno essere utilizzate nel rispetto delle istruzioni vigenti localmente.
Solo server conformi agli standard CELDA, PdL CELDA e dispositivi verificati potranno essere connessi direttamente (mediante inserimento di cavo nella porta LAN o connessione wireless) ai domini CELDA.
Il fornitore non potrà (e, quando opportuno, disporrà affinché il personale temporaneo non possa) collegare un’apparecchiatura non approvata da CELDA a un qualsiasi dominio CELDA

senza l'autorizzazione preliminare del referente di CELDA.
Il referente di CELDA fornirà l'autorizzazione scritta contestualmente all'avvio del processo di concessione della politica di sicurezza interna di CELDA da parte del referente CELDA del fornitore.
Nessuna informazione CELDA potrà essere rimossa dalle strutture CELDA e nessuna apparecchiatura o nessun software potranno essere rimossi o installati presso le strutture CELDA senza l'autorizzazione preliminare di CELDA.
Le linee guida in materia di protezione fisica e di lavori all'interno delle Strutture di CELDA dovranno essere rigorosamente rispettate, ad esempio predisponendo un accompagnamento in caso di attraversamento delle zone protette. Ogni ulteriore ordine o istruzione impartito da CELDA ad un rappresentante del fornitore si intenderà trasmesso direttamente al fornitore.
Laddove il fornitore sia autorizzato a concedere al personale temporaneo un accesso non accompagnato alle aree interne alla proprietà di CELDA, il firmatario autorizzato non CELDA e il personale temporaneo dovranno aderire a tutte le raccomandazioni impartite da CELDA.

8. Sicurezza fisica - Strutture del fornitore

L'osservanza delle clausole contenute nella presente sezione ha natura vincolante se il fornitore effettua le forniture da strutture non CELDA e include l'insieme di personale temporaneo, subappaltatori e dipendenti, subappaltatori e agenti del fornitore.
L'accesso alle strutture non CELDA (siti, edifici o aree interne) in cui vengono effettuate le forniture o in cui vengono archiviate o trattate le informazioni CELDA dovrà avvenire mediante una tessera di identificazione fornita da un fornitore autorizzato. Questa tessera dovrà essere utilizzata permanentemente da ciascun individuo come strumento di verifica dell'identità presso le strutture in questione e dovrà includere una immagine fotografica chiaramente visibile e fedelmente rappresentativa del suo portatore. I singoli individui potranno essere provvisti di una tessera di accesso elettronico autorizzato al solo scopo di accedere alle strutture di interesse o, in alternativa, di un accesso di sicurezza tramite tastiera con procedure di controllo delle autorizzazioni e della distribuzione e di modifica dei codici ad hoc o periodica.
Il fornitore provvederà affinché l'accesso ai siti, agli edifici o alle aree interne in cui vengono eseguite le forniture o in cui vengono archiviate o trattate le informazioni CELDA, venga avvenga tramite autorizzazione e aderisca ai processi e procedure di sicurezza. Tale obbligo si intende esteso ai subappaltatori con accesso fisico a queste aree (ad esempio, società di controllo ambientale, manutenzione e vigilanza).
Su richiesta dell'azienda CELDA o del proprietario del progetto CELDA, il fornitore disporrà affinché il personale temporaneo interessato venga isolato in maniera sicura dal resto del

personale del fornitore.

Le zone protette all'interno delle strutture del fornitore (ad esempio le sale per comunicazioni di rete), saranno segregate e protette mediante adeguati controlli all'ingresso per fare in modo che possa accedervi unicamente il personale temporaneo autorizzato. L'accesso effettuato a queste aree da parte del personale temporaneo deve essere sottoposto a regolari verifiche e la concessione dei diritti d'accesso a queste aree deve essere rinnovata almeno con cadenza annuale.

Il fornitore dovrà fare uso di sistemi di sicurezza CCTV e relativi supporti di registrazione sia in risposta a incidenti di sicurezza come strumento di videosorveglianza o come deterrente, sia come ausilio nella possibile cattura di individui colti nell'atto di commettere un reato.

Le immagini CCTV registrate (su nastro o in formato digitale) dovranno essere conservate per 24h. Questo periodo potrà tuttavia essere prorogato nelle situazioni seguenti:

- laddove le prove video CCTV debbano essere conservate per accertamenti peritali o indagini penali;
- se previsto come requisito necessario di ottemperanza ad una legge.

Ove utilizzati, tutti i nastri utilizzati per la registrazione delle immagini riprese dalle videocamere CCTV devono essere riposti in un armadio chiuso, con la chiave conservata e controllata in condizioni di sicurezza. L'accesso all'armadio deve essere limitato unicamente al personale autorizzato.

Tutti i registratori video e video digitali CCTV devono essere ubicati in punti appartati per evitare l'accesso non autorizzato e la possibilità di visioni "casuali" dei relativi schermi CCTV.

L'area locale che circonda le strutture del fornitore utilizzate per i prodotti e/o i servizi, a seconda dei casi, dovrà essere regolarmente ispezionata dal fornitore per verificare l'assenza di rischi e minacce.

Il fornitore dovrà verificare il livello di protezione dei cavi di alimentazione e telecomunicazione che trasmettono i dati o supportano i servizi informativi o i servizi radio/satellitari utilizzati nell'approvvigionamento delle forniture al fine di evitare l'interruzione delle operazioni aziendali.

Dovranno essere implementate le seguenti misure di tutela della sicurezza fisica commisurate alla criticità aziendale delle rispettive operazioni:

- le sedi stradali, le schermature dei cavi, i passi d'uomo o le scatole da incasso a marciapiede attraversati da cavi di importanza critica per l'azienda devono essere protetti;
- l'accesso al vano cavi o agli armadi delle risalite cavi all'interno degli edifici operativi deve essere limitato mediante l'uso di appositi lettori di controllo elettronici o una efficace gestione delle chiavi;

- i collegamenti per le comunicazioni computerizzate e le relative apparecchiature poste all'interno degli impianti informatici devono essere protetti a livello fisico e ambientale;
- i collegamenti per comunicazioni radio e satellitari e le relative apparecchiature devono essere protetti adeguatamente.

A completamento delle misure di sicurezza elettronica e fisica presso le sedi dei fornitori si reputa necessario integrare servizi di sicurezza presidiati nelle seguenti circostanze:

- la sede ha una particolare importanza operativa;
- le informazioni CELDA trattate possono avere conseguenze sul marchio e sulla reputazione;
- elevato volume di informazioni CELDA trattate (ad esempio, esternalizzazione di processi aziendali);
- requisiti contrattuali dei clienti;
- presenza di rischi/minacce specifici del sito;
- il fornitore è in possesso di informazioni CELDA con un elevato livello di sensibilità.

Per tutelare le apparecchiature CELDA (quali, ad esempio, server o switch) installate presso le strutture dei fornitori da minacce e pericoli di natura ambientale, nonché dal rischio di accessi non autorizzati, tali apparecchiature devono essere collocate in un'area protetta e segregata dalle apparecchiature utilizzate da qualsiasi sistema di organizzazioni non CELDA. Il livello di segregazione deve far sì che la sicurezza delle apparecchiature CELDA non possa essere compromessa né deliberatamente, né accidentalmente, per effetto di un accesso accordato a organizzazioni non CELDA e potrebbe ad esempio, assumere la forma di pareti divisorie, armadi con chiusura a chiave o ingabbiature metalliche.

Misure di prevenzione e rilevamento dovranno essere adottate allo scopo di prevenire guasti agli impianti causati dall'interruzione di servizi essenziali o altri fattori di influenza ambientali:

- incendi;
- gas;
- nubifragi;
- interruzioni di energia.

Per consentire il rilevamento delle seguenti circostanze dovranno essere installati appositi allarmi, collegati ad una postazione presidiata in permanenza:

- incendi;
- gas;
- interruzioni di energia;
- guasto al gruppo di continuità (UPS);

- guasto al sistema di controllo di umidità e temperatura/aria condizionata.

A protezione delle zone contenenti informazioni CELDA e strutture di elaborazione delle informazioni dovranno essere eretti perimetri di sicurezza (barriere quali pareti, recinzioni, cancelli ad apertura mediante tessera o reception presidiata).
Per evitare l'accesso non autorizzato o aggressioni deliberate, i punti d'accesso come le zone di consegna e di carico e altri punti da cui potrebbero entrare nei locali persone non autorizzate dovranno essere controllati e se possibile isolati dalle installazioni informatiche.
Assicurarsi che l'accesso fisico alle aree da cui si accede alle informazioni CELDA avvenga unicamente mediante carte di prossimità o a microprocessore (o sistemi di sicurezza equivalenti) e che il fornitore conduca verifiche interne periodiche per accertare il rispetto di tali disposizioni.
Il fornitore disporrà il divieto di scattare fotografie o acquisire in altro modo immagini delle informazioni CELDA o delle informazioni dei clienti di CELDA. In circostanze eccezionali per cui possa presentarsi la necessità per motivi aziendali di acquisire tali immagini, sarà necessario ottenere dal referente di CELDAl'esenzione temporanea da questa clausola in forma scritta.
A tutela delle informazioni CELDA, il fornitore dovrà mettere in atto una politica aziendale di blocco dei computer e pulizia dello spazio di lavoro per i dipendenti che lasciano la propria postazione.

9. Sicurezza di rete

L'osservanza delle clausole contenute nella presente sezione ha carattere vincolante se il fornitore realizza, sviluppa o supporta reti CELDA o infrastrutture di rete.
In relazione alle forniture, il fornitore avrà l'obbligo di attuare misure concordate di sicurezza in tutti i componenti forniti, in modo tale da salvaguardare il carattere di riservatezza, disponibilità e integrità delle reti CELDA e/o delle infrastrutture delle sue Aziende "sorelle". Il fornitore metterà a disposizione di CELDA la documentazione completa relativa all'implementazione della sicurezza di rete correlata alle forniture e si impegnerà al fine di:

- soddisfare ogni requisito legale e normativo;
- impedire al meglio delle proprie capacità che soggetti non autorizzati (ad esempio, pirati informatici) accedano a elementi di gestione della rete e ad altri elementi accessibili tramite le reti CELDA e/o delle sue Aziende "sorelle";
- adoperarsi al meglio delle proprie capacità al fine di contenere il rischio di uso improprio delle reti CELDA e/o delle sue Aziende "sorelle" tale da causare perdite potenziali di proventi o interruzioni di servizio, da parte di individui autorizzati ad accedervi;
- adoperarsi al meglio delle proprie capacità al fine di individuare le violazioni della

sicurezza effettivamente perpetrate, attivando la rapida correzione degli eventuali problemi che ne conseguano, nonché l'identificazione degli individui che hanno ottenuto l'accesso e delle modalità seguite per ottenerle;

- ridurre al minimo il rischio di errata configurazione delle reti CELDA, ad esempio concedendo il numero minimo di autorizzazioni necessarie per adempiere al ruolo oggetto del contratto.

Il fornitore dovrà adottare tutte le misure ragionevoli allo scopo di mettere in sicurezza tutte le interfacce presenti nei componenti forniti, senza presupporre che questi vengano fatti funzionare in un ambiente sicuro.

Il fornitore avrà l'obbligo di comunicare al referente per la sicurezza di rete CELDA i nominativi, gli indirizzi (e altri dati che CELDA avrà facoltà di richiedere) di tutti i membri del personale temporaneo che di volta in volta sarà direttamente coinvolto nell'installazione, manutenzione e/o gestione delle forniture prima che intraprendano tali operazioni.

Il fornitore trasmetterà al referente per la sicurezza di rete CELDA un prospetto (opportunamente aggiornato) di tutti i componenti attivi contenuti nelle forniture con indicazione delle rispettive fonti.

Il fornitore comunicherà gli estremi dei membri del suo personale che assicurano il collegamento con il team per la gestione delle vulnerabilità (CERT) in relazione alla discussione sulle vulnerabilità individuate da CELDA e dal fornitore nelle forniture. Il fornitore comunicherà puntualmente a CELDA informazioni sulle vulnerabilità, e adempierà ai ragionevoli obblighi ad esso notificati di volta in volta dal referente per la sicurezza di rete CELDA, a proprie spese. Il fornitore informerà CELDA in ordine alle vulnerabilità con sufficiente anticipo, in modo da consentire l'introduzione di controlli di mitigazione prima che il fornitore stesso divulghi pubblicamente le vulnerabilità.

Il fornitore dovrà concedere al referente per la sicurezza di rete CELDA e a chi da esso di volta in volta designato un accesso completo e incondizionato alle strutture in cui le forniture vengono sviluppate, prodotte o fabbricate perché vi possano condurre test e/o valutazioni di conformità alla sicurezza. Il fornitore sarà peraltro tenuto a collaborare (e disporrà affinché l'intero personale temporaneo interessato faccia altrettanto) in tali verifiche della conformità.

Il fornitore dovrà accertarsi che tutti i componenti riguardanti la sicurezza contenuti nelle forniture, così come di volta in volta identificati da, o comunicati a CELDA, vengano valutati esternamente a spese del fornitore e con la ragionevole soddisfazione di CELDA.

In relazione alle informazioni trasmesse o ottenute da CELDA e accompagnate dalla dicitura "STRETTAMENTE RISERVATO" o la cui natura riservata sia facilmente riconoscibile, il fornitore dovrà provvedere affinché:

- l'accesso ad esse venga consentito unicamente al personale temporaneo appositamente autorizzato da CELDA per la visione e il trattamento e venga conservato un registro di tali accessi;
- esse vengano trattate, utilizzate e archiviate con estrema cura e criptate prima dell'archiviazione mediante PGP o WinZip 9 e in condizioni che assicurino un elevato grado di resistenza alla compromissione accidentale (ossia, adottando il più efficace algoritmo di crittografia disponibile o utilizzando una valida password) e che rendano rilevabile con grande probabilità l'azione o il tentativo di compromissione;
- una volta trasmesse, esse vengano sottoposte a misure di sicurezza adeguate mediante crittografia con Secure Email, PGP o WinZip 9; e
- non vengano, salvo autorizzazione scritta di CELDA, esportate al di fuori dello spazio economico europeo.

Il fornitore dovrà comunicare sollecitamente, e in ogni caso entro il termine di 7 giorni lavorativi, al referente per la sicurezza di rete CELDA i dettagli completi delle caratteristiche e funzionalità proprie delle forniture (o che sono pianificate nella tabella di marcia per le forniture) progettate per, o che potrebbero essere progettate per, l'intercettazione legale o altre forme di intercettazione del traffico delle telecomunicazioni che di volta in volta:

- il fornitore conosce; o che
- il referente per la sicurezza di rete CELDA ritiene ragionevolmente di conoscere e ne dà pertanto comunicazione al fornitore. Tali dettagli dovranno includere tutte le informazioni ritenute ragionevolmente necessarie per consentire al referente per la sicurezza di rete CELDA di comprendere appieno la natura, composizione e portata di tali caratteristiche e/o funzionalità.

Allo scopo di mantenere abilitato l'accesso ai sistemi e/o alle reti CELDA, il fornitore dovrà comunicare immediatamente a CELDA ogni eventuale modifica apportata al proprio metodo di accesso tramite i firewall, fornendo ad esempio la traduzione degli indirizzi di rete.
Non è consentito l'utilizzo di strumenti di monitoraggio in grado di visualizzare informazioni relative alle applicazioni.
La funzionalità IPv6 inclusa nei sistemi operativi deve essere disabilitata sugli host (dispositivi degli utenti finali, server) collegati ai domini di rete CELDA e quando non necessaria.
Il fornitore è tenuto a rispettare, e disporrà affinché le forniture rispettino, le politiche CELDA eventualmente vigenti e i requisiti di sicurezza. Ogni inosservanza dovrà essere concordata all'atto della firma del contratto o in sede di controllo delle modifiche.
Il fornitore provvederà affinché il personale temporaneo venga sottoposto a controlli pre-impiego adeguati rispetto al livello di accesso.

10. Sicurezza di rete del fornitore

L'osservanza delle clausole contenute nella presente sezione ha carattere vincolante se la rete del fornitore verrà utilizzata ai fini dell'approvvigionamento delle forniture (sono incluse reti LAN, WAN, Internet, wireless e radio).

In relazione alle forniture, il fornitore avrà l'obbligo di attuare misure concordate di sicurezza in tutte le reti, in modo tale da salvaguardare il carattere di riservatezza, disponibilità e integrità delle informazioni CELDA. Le misure dovranno:

- soddisfare ogni requisito legale e normativo;
- impedire nella misura del possibile che soggetti non autorizzati (ad esempio, pirati informatici) accedano alla rete;
- contenere nella misura del possibile il rischio di uso improprio delle reti tale da causare potenziali perdite di proventi o interruzioni di servizio, da parte di individui autorizzati ad accedervi;
- individuare nella misura del possibile ogni violazione della sicurezza effettivamente perpetrata, attivando la rapida correzione degli eventuali problemi che ne conseguano, nonché l'identificazione degli individui che hanno ottenuto l'accesso e delle modalità seguite per ottenerle.

11. Sicurezza in Cloud

In risposta alla crescente adozione dei servizi cloud e all'importanza critica della sicurezza dei dati in tali ambienti, [Nome dell'Azienda] stabilisce i seguenti requisiti di sicurezza applicabili a tutti i fornitori di servizi in cloud. Questi requisiti sono conformi agli standard internazionali ISO 27017:2015 per la sicurezza dei servizi cloud e ISO 27018:2019 per la protezione dei dati personali ospitati in cloud.

Misure Tecniche ed Organizzative

I fornitori devono adottare misure tecniche ed organizzative avanzate per garantire la sicurezza dei dati nel cloud, includendo:

- Cifratura dei dati in transito e a riposo utilizzando algoritmi riconosciuti come sicuri.
- Autenticazione forte e gestione delle identità per controllare l'accesso ai dati e ai servizi.
- Segregazione efficace dei dati dei clienti per prevenire l'accesso non autorizzato o la commistione dei dati.

Privacy by Design e by Default

Le soluzioni cloud devono essere progettate e configurate per massimizzare la privacy degli utenti, limitando la raccolta e l'utilizzo dei dati al minimo necessario e garantendo che le impostazioni predefinite offrano il massimo livello di privacy.

Valutazioni d'Impatto sulla Protezione dei Dati (DPIA)

Prima del lancio di qualsiasi servizio cloud o di significative modifiche a un servizio esistente, i fornitori devono condurre una DPIA per identificare e mitigare i rischi per i diritti e le libertà degli individui.

Contratti e Accordi di Lavorazione
I fornitori di servizi cloud devono stipulare contratti che includano obblighi specifici per la protezione dei dati, conformemente all'articolo 28 del GDPR. Tali contratti devono delineare chiaramente le responsabilità dei fornitori nel trattamento dei dati personali.

Notifica di Violazione dei Dati
In caso di violazione dei dati personali, i fornitori devono avere procedure in atto per notificare tempestivamente l'incidente a [Nome dell'Azienda] e, se necessario, alle autorità di controllo e agli interessati, in linea con gli articoli 33 e 34 del GDPR.

Diritti degli Interessati
I servizi cloud devono permettere agli utenti di esercitare facilmente i loro diritti in materia di protezione dei dati, come il diritto di accesso, rettifica, cancellazione e opposizione al trattamento dei dati personali.

Monitoraggio e Revisione
Le pratiche di privacy e sicurezza dei servizi cloud saranno soggette a monitoraggio e revisione periodica per verificare la conformità al GDPR e ad altre normative applicabili, oltre che per identificare e mitigare nuovi rischi.

[EOF]