Linee guida
La sicurezza nel procurement ICT

Aprile 2020

Sommario

1 Premessa

1.1 Genesi e ambito del documento

Il presente documento rappresenta il prodotto finale delle attività di un tavolo di lavoro promosso dal Nucleo per la Sicurezza Cibernetica (NSC) del Dipartimento Informazioni per la Sicurezza presso la Presidenza del Consiglio dei Ministri.

Al tavolo di lavoro, che ha operato dal novembre 2018 al febbraio 2019, hanno partecipato le seguenti pubbliche amministrazioni centrali:

- *Dipartimento Informazioni per la Sicurezza della PCM;*
- *Dipartimento della Protezione Civile della PCM;*
- *Ministero degli Affari Esteri;*
- *Ministero dell'Interno;*
- *Ministero della Giustizia;*
- *Ministero della Difesa;*
- *Ministero dell'Economia e delle Finanze;*
- *Ministero dello Sviluppo Economico;*
- *Agenzia per l'Italia Digitale;*

oltre alla società Consip, in veste di centrale di committenza delle pubbliche amministrazioni.

Obiettivo del tavolo di lavoro era definire indicazioni tecnico-amministrative per garantire, all'interno delle procedure per l'approvvigionamento di beni e servizi informatici delle pubbliche amministrazioni, la rispondenza di questi ad adeguati livelli di sicurezza.

Si ritiene infatti che - durante i processi di acquisizione - i fornitori, in relazione alla natura dei servizi offerti, possano accedere al patrimonio informativo delle pubbliche amministrazioni committenti, introducendo potenziali rischi informatici, con impatto in particolare su riservatezza, integrità, disponibilità, autenticità e non ripudio dei dati pubblici. Processi di acquisizione condotti senza attenzione agli aspetti di sicurezza possono vanificare, o comunque rendere meno efficaci, le misure prese dalle amministrazioni per tutelare il proprio patrimonio informativo. Di contro, la necessità di formalizzare e strutturare il rapporto con i fornitori può rappresentare, per le amministrazioni, un'opportunità per aggiornare o rivedere le proprie politiche di sicurezza, anche contando sulle competenze del fornitore stesso, che può contribuire in modo positivo a elevare le misure di protezione dell'amministrazione, come si vedrà nei paragrafi che seguono.

Per quanto sopra, il presente documento - che riguarda certamente il tema generale della sicurezza informatica - ha un ambito circoscritto, e si concentra sulla sicurezza nell'approvvigionamento di beni e servizi informatici, attività indicata nel seguito del testo con "procurement ICT".

È utile, in questa premessa, ricordare che la maggioranza dei contratti pubblici che riguardano l'ICT:

- derivano da una gara o rappresentano appalti specifici di accordi quadro;
- sono pluriennali (per cui un certo grado di avvicendamento del personale del fornitore è inevitabile);
- comprendono più di un'iniziativa progettuale, in genere numerosi progetti distinti, che vengono condotti in parte sequenzialmente, in parte in parallelo, non necessariamente dallo stesso gruppo di lavoro del fornitore;

Ai fini del presente documento, i contratti ICT si possono classificare come segue:

a) contratti di sviluppo, realizzazione e manutenzione evolutiva di applicazioni informatiche;

b) contratti di acquisizione di prodotti (hardware o software);

c) contratti per attività di operation e conduzione;

d) contratti per servizi diversi da a) e c) (es. supporto, consulenza, formazione, help desk, …);

e) contratti per forniture miste, combinazioni delle precedenti tipologie.

1.2 A chi è rivolto il documento

Il presente documento è diretto in primo luogo ai dirigenti e ai funzionari delle pubbliche amministrazioni, con particolare riferimento alle strutture che si occupano di acquisizioni informatiche, ai RUP delle gare pubbliche, ai responsabili della transizione al digitale (definiti dal CAD), ai responsabili dell'organizzazione, pianificazione e sicurezza. A questi soggetti sono rivolte le indicazioni pratiche, gli esempi e gli strumenti operativi contenuti nei paragrafi che seguono.

I contenuti del documento vanno intesi in termini di suggerimenti, buone pratiche e procedure cui allinearsi, anche sulla base della rilevanza e dei profili di criticità delle varie acquisizioni ICT da condurre, come illustrato nel dettaglio, per le varie indicazioni, nel capitolo 2.

Il documento è rivolto anche, con un diverso percorso di lettura, agli operatori di mercato e in particolare ai fornitori della pubblica amministrazione. Per questi ultimi è opportuno, tra l'altro, essere a conoscenza delle problematiche legate alla sicurezza nel procurement ICT delle pubbliche amministrazioni, in modo che siano pronti a recepire le richieste dei committenti senza impatti rilevanti sulle negoziazioni, e anzi con spirito di collaborazione. Si ritiene infatti che stabilire un lessico comune e condividere gli obiettivi di sicurezza possa rappresentare un vantaggio per i clienti ma anche per i fornitori, rendendo più efficienti le clausole dei contratti e aprendo nuovi spazi di mercato.

1.3 Finalità del documento

Il presente documento non costituisce un manuale tecnico, un compendio o uno studio accademico sulla tematica della sicurezza. Al contrario, nel testo si rimanda, per gli eventuali approfondimenti specialistici sulla materia, alla letteratura tecnica: riferimenti puntuali a studi, articoli e standard sono presenti nei paragrafi che seguono.

Allo stesso modo, non è scopo del presente documento fornire al lettore interpretazioni giuridiche, disamine o estensioni di norme e procedure vigenti in tema di appalti pubblici.

Le finalità del documento sono invece:

- illustrare in maniera semplice e immediatamente fruibile la problematica della sicurezza nel procurement ICT;
- mettere a sistema (tramite opportuni glossari e classificazioni), formalizzare definizioni e concetti legati alla sicurezza nel procurement ICT, rendendoli coerenti con la norma e con il contesto della pubblica amministrazione;
- presentare buone prassi, soluzioni già in uso, misure semplici da adottare (strumenti operativi, esempi pratici, riferimenti puntuali), per verificare il livello di sicurezza degli attuali processi di acquisizione ed eventualmente per alzare tale livello senza per questo aumentare in modo eccessivo la complessità dei processi e l'impegno necessario a condurli.

1.4 Definizioni

Accordo quadro	Gli Accordi quadro, aggiudicati da una centrale di committenza a più fornitori a seguito della pubblicazione di specifici bandi, definiscono le clausole generali (ad esempio corrispettivi unitari, SLA, …) che, in un determinato periodo temporale, regolano i contratti da stipulare. Nell'ambito dell'Accordo quadro, le amministrazioni provvedono poi, attraverso la contrattazione di appalti specifici, a negoziare i singoli contratti, personalizzati sulla base delle proprie esigenze (ad esempio quantità, caratteristiche specifiche, …).
Account management	Gestione account/credenziali accesso
Appalto specifico	Vedi Accordo quadro
Asset management	Gestione dei beni di proprietà di un'organizzazione
Audit	Processo indipendente di valutazione e verifica
Change management	Gestione del cambiamento
Code review	Processo di revisione del codice/istruzioni di programmazione.
Firmware	Programma, sequenza di istruzioni memorizzata sulla memoria non volatile di un componente elettronico.
Fleet management	Servizio di locazione operativa, gestione e manutenzione di un parco di apparecchiature hardware, ad esempio postazioni di lavoro.
Hardening	Processo che mira, attraverso operazioni di configurazione specifica di un dato sistema e dei suoi componenti, a minimizzare l'impatto di possibili vulnerabilità, migliorandone quindi la sicurezza complessiva.
Middleware	Software che svolge funzioni di integrazione tra diverse applicazioni e componenti software che sono stati sviluppati con tecnologie diverse e/o utilizzano architetture diverse.
Penetration test	Processo di valutazione della sicurezza di un sistema o di una rete attraverso la simulazione di un attacco.
Procurement ICT	Attività di approvvigionamento di beni e servizi informatici.
Procurement management	Gestione dei processi di approvvigionamento
Risk management	Gestione dei rischi
Vulnerability assessment	Processo di individuazione e classificazione delle vulnerabilità di sicurezza di un sistema o di una rete.
Web server	Applicazione software installata su un server che gestisce le richieste di pagine web provenienti dai browser dei client (Browser Web).
Wiping	Processo di cancellazione definitiva di dati contenuti su un supporto di memorizzazione, ad esempio da un Hard Disk.
Categorie di dati personali	
Dati giudiziari	Dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
Dati identificativi	Dati che possono identificare, direttamente o indirettamente una persona, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online.
Dati Sensibili	Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

1.5 Acronimi

BIA	Business Impact analysis
CVCN	Centro di valutazione e certificazione nazionale
CED	Centro Elaborazione Dati
CAD	Codice Amministrazione Digitale
CC	Common Criteria
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CMS	Content management system
CQ	Contratto Quadro
DPIA	Data Protection Impact Assessment
DBMS	Database Management System
DIS	Dipartimento delle informazioni per la sicurezza
EoL	End of Life (fine vita)
GDPR	General Data Protection Regulation - regolamento UE n. 679 del 2016
ICT	Information and Communications Technology
IOC	Indicator of Compromise
MEV	Manutenzione Evolutiva
NSC	Nucleo per la Sicurezza Cibernetica
OWASP	Open Web Application Security Project
PCM	Presidenza Consiglio Ministri
RTI	Raggruppamento Temporaneo di Impresa
RACI-VS	Responsible, Accountable, Consulted, Informed – Verifier, Signatory
RA	Risk Assessment
SGSI	Sistema di Gestione della Sicurezza delle Informazioni
SOC	Security Operational Center
SLA	Service Level Agreement - livelli di servizio
SIEM	Sistema di gestione delle informazioni e degli eventi di sicurezza
VPN	Virtual Private Network

1.6 Documenti di Riferimento

DR-1	ISO 22317 - Linee guida per Business Impact Analysis – https://www.iso.org/standard/50054.html
DR-2	ISO 27001 - Sistema di Gestione della Sicurezza delle Informazioni https://www.iso.org/isoiec-27001-information-security.html
DR-3	ISO 31000 Risk Management https://www.iso.org/iso-31000-risk-management.html
DR-4	Linee guida sviluppo software sicuro https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro
DR-5	Misure minime di sicurezza AgID https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict
DR-6	ISO 15408 Standard Common Criteria https://www.iso.org/standard/50341.html
DR-7	ISO 1005 Gestione Qualità – Linee Guida per i piano di qualità https://www.iso.org/standard/70398.html

2 Indicazioni per le amministrazioni

Il presente paragrafo contiene indicazioni, in termini di azioni da eseguire, che le pubbliche amministrazioni devono prendere in considerazione per le finalità di cui al 1.3. Alcune azioni sono di tipo organizzativo, altre funzionali, altre ancora di tipo operativo.

Il paragrafo è strutturato in 3 sotto paragrafi, che classificano le indicazioni fornite secondo il seguente criterio temporale:

- azioni da svolgere prima dell'acquisizione (prima della fase di procurement);
- azioni da svolgere nel corso del procedimento di acquisizione (durante la fase di procurement);
- azioni da svolgere dopo la stipula del contratto.

Le indicazioni fornite sono da ritenersi obbligatorie per le forniture ritenute critiche dall'amministrazione committente (vedi par. 2.2.1), mentre devono essere intese come semplici suggerimenti, da attuarsi compatibilmente con le risorse disponibili e in misura adeguata alle dimensioni - in termini di investimenti finanziari - del contratto stesso, per forniture non critiche. Nel documento verranno forniti criteri per classificare le forniture come "critiche" o "non critiche".

2.1 Azioni da svolgere prima della fase di procurement

Prima di attivare un procedimento di acquisizione, le amministrazioni devono aver svolto una serie di azioni di carattere generale e strategico, non legate alla singola acquisizione, per "prepararsi" a effettuare i successivi passi in maniera sicura. In estrema sintesi, le amministrazioni devono organizzarsi, dotarsi di strumenti, metodologie e competenze, definire una politica da seguire, stabilire regole, criteri, piani d'azione che poi utilizzeranno in fase di procurement. Detto in altri termini, si tratta di strutturare e formalizzare i futuri procedimenti di acquisizione, minimizzando il rischio di trovarsi - nell'operatività - in situazioni inaspettate e dover poi "improvvisare".

Per facilità di lettura, le azioni da svolgere vengono, qui nel seguito, enumerate da AG1 ad AG7 (l'acronimo AG sta per "azioni generali"). Si sottolinea che le amministrazioni non devono considerare queste azioni come ulteriori impegni rispetto ai normali procedimenti o un aggravio di complessità degli stessi. Al contrario, la maggior parte di queste azioni sono prassi che le amministrazioni dovrebbero già aver svolto per altri obiettivi: si tratta quindi di verificare e sanare eventuali carenze anche, ma non solo, per assicurare la sicurezza nel procurement ICT.

2.1.1 AG1 - Promuovere competenza e consapevolezza

È necessario che le amministrazioni possano disporre, tra le risorse umane che si occuperanno delle acquisizioni, di competenze aggiornate di Procurement Management, Gestione Progetti, Asset Management, Change Management, Risk Management, Sicurezza e Protezione dei Dati.

Ove le amministrazioni intendano mantenere internamente le competenze di cui sopra, occorre che il personale individuato venga formato attraverso opportuni percorsi didattici e di aggiornamento (ad esempio, una serie strutturata di corsi sui temi elencati). Una scelta alternativa, ove sia indisponibile

personale interno, è acquisire queste conoscenze dal mercato, facendo ricorso a società di supporto e consulenza specifica.

Allo stesso tempo, occorre che le amministrazioni mantengano al loro interno un adeguato livello di consapevolezza sulla tematica della sicurezza nel procurement ICT. Ciò si ottiene, ad esempio, organizzando eventi tematici, seminari e presentazioni sui rischi della "non-sicurezza" (cosa potrebbe accadere se…), destinati non solo alle risorse direttamente coinvolte nelle acquisizioni, ma ai decisori e più in generale a tutto il personale. Si suggerisce di inserire questo tipo di eventi nella normale attività di comunicazione dell'amministrazione verso i dipendenti (ad esempio, nel calendario della formazione obbligatoria sulla sicurezza dei luoghi di lavoro e sulla privacy).

2.1.2 AG2 - Raccogliere buone prassi ed esperienze

È opportuno che l'amministrazione raccolga al proprio interno notizie sui casi di successo/insuccesso, in termini di sicurezza, riscontrati nelle precedenti acquisizioni ICT, come buone prassi da tenere in conto al fine di un miglioramento continuo del processo di procurement. A livello più generale e inter-amministrazione, la raccolta di casi di successo e buone prassi può essere svolta da un soggetto centrale, vedi paragrafo 3.2.

L'amministrazione deve inoltre organizzarsi per essere in grado di ricevere e diffondere al proprio interno eventuali avvisi e allarmi provenienti dagli organismi individuati dal legislatore a presidio della sicurezza cibernetica, da gruppi specialistici e associazioni professionali che si occupano di sicurezza delle informazioni.

2.1.3 AG3 - Stabilire ruoli e responsabilità

Le amministrazioni devono definire, all'interno della propria struttura, ruoli e responsabilità connesse con la sicurezza del procurement ICT, identificando profili idonei e assegnando incarichi formali.

Come strumento operativo, si suggerisce di utilizzare matrici di tipo RACI-VS per mettere in relazione i ruoli definiti con le attività da svolgere nel corso dell'acquisizione e posteriormente alla stessa.

Nella tabella che segue si forniscono alcuni esempi, di tipo meramente esplicativo (servono solo per spiegare come usare, in questo contesto, le matrici RACI-VS). Sulle righe sono elencate le azioni suggerite in questo capitolo, mentre sulle colonne sono riportati alcuni ruoli tipici.

NB: i ruoli nominati in tabella non sono rappresentativi; nei casi reali di specifiche amministrazioni alcuni ruoli potrebbero non essere definiti, due o più ruoli potrebbero coincidere tra loro, o essere presenti con nomi diversi.

TABELLA 1: MATRICE RACI-VS DI ESEMPIO

	Ruoli									
Codice Azione/ Ruoli	Responsabile Asset - ICT	Responsabile Sicurezza - ICT	Responsabile Area ICT	Responsabile Procurement ICT	Responsabile Area Acquisizioni	Responsabile Audit	Responsabile Area Audit	Verificatore Esterno	Direttore Esecuzione Contratto	Direttore Generale
AG2	**C**	**C**	**I**	**R**	**A**	**I**	**I**	**V**		**S**
AG4	**R**	**C**	**A**	**I**	**I**	**I**	**I**	**V**		**S**
AG5	**C**	**R**	**A**	**I**	**I**	**I**	**I**	**V**		**S**

AG6	C	C	I	I	I	R	A	V	S	
AP1	C	C	C	R	A	I	I	V	S	
AP2	C	C	C	R	A	I	I	V	S	
A2	C	R	A	I	I	I	I	V	S	

R= Responsible: persona (o ruolo) che produce il risultato dell'attività.
A=Accountable: persona (o ruolo) che approva il risultato.
C=Consult: persona (o ruolo) che viene consultata nella produzione del risultato.
I=Inform: persona o il ruolo che viene informata sul risultato.
V=Verifier: persona o il ruolo che verifica che il risultato rispetti i criteri di accettazione.
S=Signatory: persona o il ruolo che approva la decisione del Verifier.

AI fine di assicurare l'effettiva osservanza del GDPR da parte dei soggetti coinvolti e nel rispetto del principio di responsabilizzazione ai sensi degli artt. 5, par. 2 e 24 GDPR, le amministrazioni sono tenute, inoltre, a definire puntualmente i compiti affidati al proprio responsabile della protezione dei dati personali e ai futuri fornitori che, trattando dati personali per conto dell'amministrazione, svolgeranno il ruolo di responsabili del trattamento ai sensi dell'art. 28 GDPR. Si rimanda, per questo tema, al successivo capitolo 5.

2.1.4 AG4 - Effettuare una ricognizione dei beni informatici e dei servizi

L'amministrazione deve disporre di un inventario aggiornato dei propri beni informatici (nel seguito, "asset"). Ove questo inventario non sia disponibile o sia ritenuto incompleto/inaffidabile/obsoleto, l'amministrazione deve effettuare una ricognizione (questa attività è definita "assessment") dei beni quali – a titolo di esempio - apparecchiature hardware, applicazioni, licenze d'uso, ecc.

L'inventario deve contenere, per ogni bene, il responsabile (definito "owner") in termini di protezione dei requisiti generali di sicurezza (Riservatezza, Integrità, Disponibilità, Non Ripudio, Autenticità).

Si suggerisce, ove non già presente o sia ritenuto non aggiornato, di costituire un analogo inventario anche dei servizi che l'amministrazione eroga al suo interno e nei confronti dei suoi utenti istituzionali (cittadini, imprese). Sarebbe utile anche una relazione tra i due inventari, ad esempio quali beni informatici sono utilizzati per erogare quali servizi. I due inventari devono essere oggetto di una sistematica manutenzione e aggiornamento.

Come già detto, l'utilità di questa azione esula dalla mera tematica della sicurezza nel procurement ICT. Pertanto, l'investimento necessario, in termini di giorni persona, per svolgere questa azione viene ripagato da benefici ben superiori alla sola sicurezza (si pensi, ad esempio, alla facilità di gestione di asset correttamente inventariati, oppure alla possibilità, a valle dell'assessment, di ottimizzare il parco licenze riducendone i costi).

2.1.5 AG5 - Classificazione di beni e servizi sotto il profilo della sicurezza

Successivamente all'azione AG4, l'amministrazione deve classificare i beni e i servizi individuati in termini di criticità, rischi, minacce, vulnerabilità. A tale scopo, ove non siano già state svolte per altri obiettivi, l'amministrazione deve eseguire le attività di Risk Assessment e di Business Impact Analisys. Per un approfondimento su queste attività, si rimanda alla consultazione dei seguenti documenti di riferimento (Rif: DR-1 – DR-2 – DR-3) del paragrafo 1.6.

Anche questa classificazione va mantenuta aggiornata, eventualmente ripetendo RA e BIA quando l'amministrazione giudichi obsoleti gli ultimi studi condotti (ad esempio a valle di un evento che cambi le condizioni operative dell'amministrazione).

2.1.6 AG6 - Definire una metodologia di audit e valutazione del fornitore in materia di sicurezza

Le amministrazioni devono organizzarsi in modo da poter svolgere efficaci azioni di audit nei confronti dei propri fornitori, anche individuando al loro interno competenze e responsabilità. Devono definire il processo e le modalità di svolgimento delle attività di audit: processo e modalità devono essere esplicitate nei capitolati di gara o nei contratti di fornitura, come dettagliato nel successivo paragrafo 2.2.

Tra le modalità da definire, occorre stabilire almeno:

- gli obiettivi del processo di audit (tra questi, nelle forniture critiche sotto l'aspetto della sicurezza, c'è l'obiettivo di verificare le misure di sicurezza adottate dal fornitore nell'erogazione delle sue prestazioni);
- la periodicità con la quale verranno eseguiti gli audit;
- gli indicatori, metodi e misure che saranno utilizzati, anche con riferimento all'oggettività dei risultati dell'audit.

Gli indicatori, metodi e misure di cui all'ultimo punto potranno essere utilizzati anche per valutare il fornitore, sotto il profilo della sicurezza, nelle procedure di acquisizione che l'amministrazione dovrà gestire (si veda il paragrafo 2.2).

2.1.7 AG7 - Definire una metodologia di audit interno in materia di sicurezza

In coerenza con l'azione precedente, le amministrazioni devono organizzarsi anche per effettuare audit interni, che avranno l'obiettivo di verificare la corretta adozione, nel tempo, di tutte le misure di sicurezza e la conformità alle normative vigenti in materia (ad esempio il GDPR).

2.1.8 Check list delle azioni generali

Uno strumento operativo molto semplice che si propone alle amministrazioni è la seguente tabella. Rispondendo alle domande della tabella, l'amministrazione può verificare a che livello di preparazione si trova nel contesto della sicurezza nel procurement ICT (ad esempio confrontando la somma delle risposte rispetto al massimo possibile), e quali azioni deve ancora compiere per migliorare la sua posizione. Un raffinamento di questo strumento si ottiene imputando a ciascuna domanda un peso differente a seconda dell'importanza di ciascuna azione nel contesto dell'amministrazione.

TABELLA 2: CHECK LIST DELLE AZIONI GENERALI

Azione	Domande	Risposte Si (1), No (0), Parziale(0,5)
AG1	Esiste un piano aggiornato di formazione sui temi della sicurezza?	
	È definito un calendario di eventi per sensibilizzare il personale sui rischi della "non sicurezza"?	
AG2	Esiste un archivio di buone prassi ed esperienze?	
AG3	Sono formalizzati gli incarichi e le responsabilità sulla sicurezza nelle acquisizioni?	
	Sono definite matrici RACI-VS per le attività di gestione della sicurezza nelle acquisizioni?	
AG4	Esiste un inventario aggiornato dei beni informatici dell'amministrazione?	

	Esiste un inventario aggiornato dei servizi erogati dall'amministrazione?	
AG5	Sono disponibili studi aggiornati di RA e BIA nell'ambito dell'amministrazione?	
AG6	È definita una metodologia di audit dei fornitori sul tema della sicurezza?	
AG7	È definita una metodologia di audit interno sul tema della sicurezza?	
	Valutazione complessiva	(somma punteggi)

2.2 Azioni da svolgere durante la fase di procurement

In questo paragrafo vengono elencate le azioni che le amministrazioni devono compiere, sul tema della gestione della sicurezza, nel corso del procedimento di acquisizione, che comprende anche la scrittura della documentazione di gara.

Rispetto alle azioni precedenti, che erano generali e di tipo strategico-organizzativo, queste azioni sono operative, dipendono dalle caratteristiche della singola acquisizione (sia per l'oggetto della fornitura che per il procedimento di acquisizione), e in alcuni casi sono alternative tra loro.

Le azioni da seguire sono illustrate nei paragrafi che seguono, che forniscono anche casi d'uso pratici, riferimenti ed esempi. Le azioni sono denominate AP1 – AP4, ove AP è acronimo per "azioni procurement".

2.2.1 AP1 - Analizzare la fornitura e classificarla in base a criteri di sicurezza

Quando sorge una necessità di acquisire beni o servizi ICT, le amministrazioni devono determinare il livello di criticità dell'acquisizione in esame. Per fare ciò, l'amministrazione deve verificare anzitutto su quali beni e servizi avrà impatto l'acquisizione in esame (con riferimento alla classificazione di cui al paragrafo 2.1.5). Si noti che "avere impatto" non significa solo che l'acquisizione determina una modifica sul bene o sul servizio, ma anche - ad esempio - che l'acquisizione è funzionale al mantenimento in operatività del bene o servizio in questione.

In generale, la criticità del bene o servizio impattato si riflette sulla criticità dell'acquisizione. Ad esempio, ove l'acquisizione impatti su un servizio pubblico erogato dall'amministrazione ai cittadini, oppure su un bene e servizio richiesto da norme di carattere generale o speciale, l'acquisizione dovrà essere considerata critica. Possono tuttavia essere definiti altri criteri, ad esempio:

- la dimensione complessiva in termini finanziari dell'acquisizione (un possibile criterio è definire "critiche" le acquisizioni di importo oltre una certa soglia);
- la durata temporale del contratto da stipulare (anche in questo caso, si potrebbero definire "critiche" le acquisizioni di durata oltre una certa soglia)
- la sede ove verrà installato il bene da acquisire o saranno erogate le prestazioni del fornitore (ad esempio, se è necessario consentire al fornitore di accedere a locali ove si svolgono attività critiche dell'amministrazione, oppure ove sono conservati informazioni critiche).

Tuttavia le singole amministrazioni possono definire all'atto della programmazione la criticità dell'affidamento.

Uno strumento operativo molto semplice che si propone alle amministrazioni è la seguente tabella. L'amministrazione deve attribuire, tramite i pesi di colonna 2, l'importanza di ciascuna domanda,

aggiungere eventuali righe per ulteriori criteri (altro), rispondere e calcolare la criticità complessiva dell'acquisizione.

Come semplificazione, si può pensare di riportare la criticità complessiva a una scala a tre valori "**alta**", "**media**", "**bassa**", confrontando il risultato del calcolo con il massimo valore possibile.

TABELLA 3: CALCOLO CRITICITÀ DELL'ACQUISIZIONE

Domande	**Peso** (da definire a cura dell'amministrazione)	**Risposte** Si (1), No (0), Parzialmente (0,5)	**Punteggi pesati** (prodotto delle precedenti due colonne)
L'acquisizione impatta su beni e/o servizi critici dell'amministrazione?	esempio: 5		
L'importo, o più in generale l'investimento complessivo dell'acquisizione supera la soglia minima di criticità?	esempio: 2		
La durata del contratto da stipulare supera la soglia minima di criticità?	esempio: 1		
La sede ove verranno erogate le prestazioni da acquisire è critica?	esempio: 3		
Altro (da definire…)			
		Criticità complessiva	

2.2.2 AP2 - Scegliere lo strumento di acquisizione più adeguato, tenendo conto della sicurezza

L'amministrazione deve tenere conto dei risultati dell'azione AP1 per scegliere lo strumento di acquisizione di cui avvalersi, tra quelli disponibili e in accordo con il codice degli appalti e il resto della normativa applicabile, ivi compresa la disciplina in tema di obblighi di utilizzo di strumenti di acquisto e di negoziazione previsti dalle vigenti disposizioni in materia di contenimento della spesa.

A titolo di mero esempio, l'amministrazione potrebbe effettuare acquisizioni di bassa criticità sul MEPA, o comunque verificando che il bando MEPA di riferimento contenga requisiti di sicurezza adeguati all'acquisizione da effettuare.

Al contrario, per acquisizioni classificate di alta criticità, l'amministrazione potrebbe ad esempio verificare che eventuali accordi quadro disponibili (come oggetto e capienza) prevedano requisiti di sicurezza adeguati per quel grado di criticità: in caso la verifica sia negativa, l'amministrazione potrebbe scartare l'opzione di servirsi del suddetto accordo quadro. NB: occorre ricordare che, per la loro stessa natura, gli accordi quadro sono strumenti di tipo "generalista", pertanto potrebbero contenere requisiti di sicurezza adeguati alla maggioranza dei casi ma non per specifiche iniziative dell'amministrazione.

Come esempio esplicativo, nella figura che segue è riportata una possibile applicazione dell'azione AP2, dove LCC sta per "livello di criticità complessiva" della fornitura. Si ribadisce che si tratta di un mero esempio e non di regole generali.

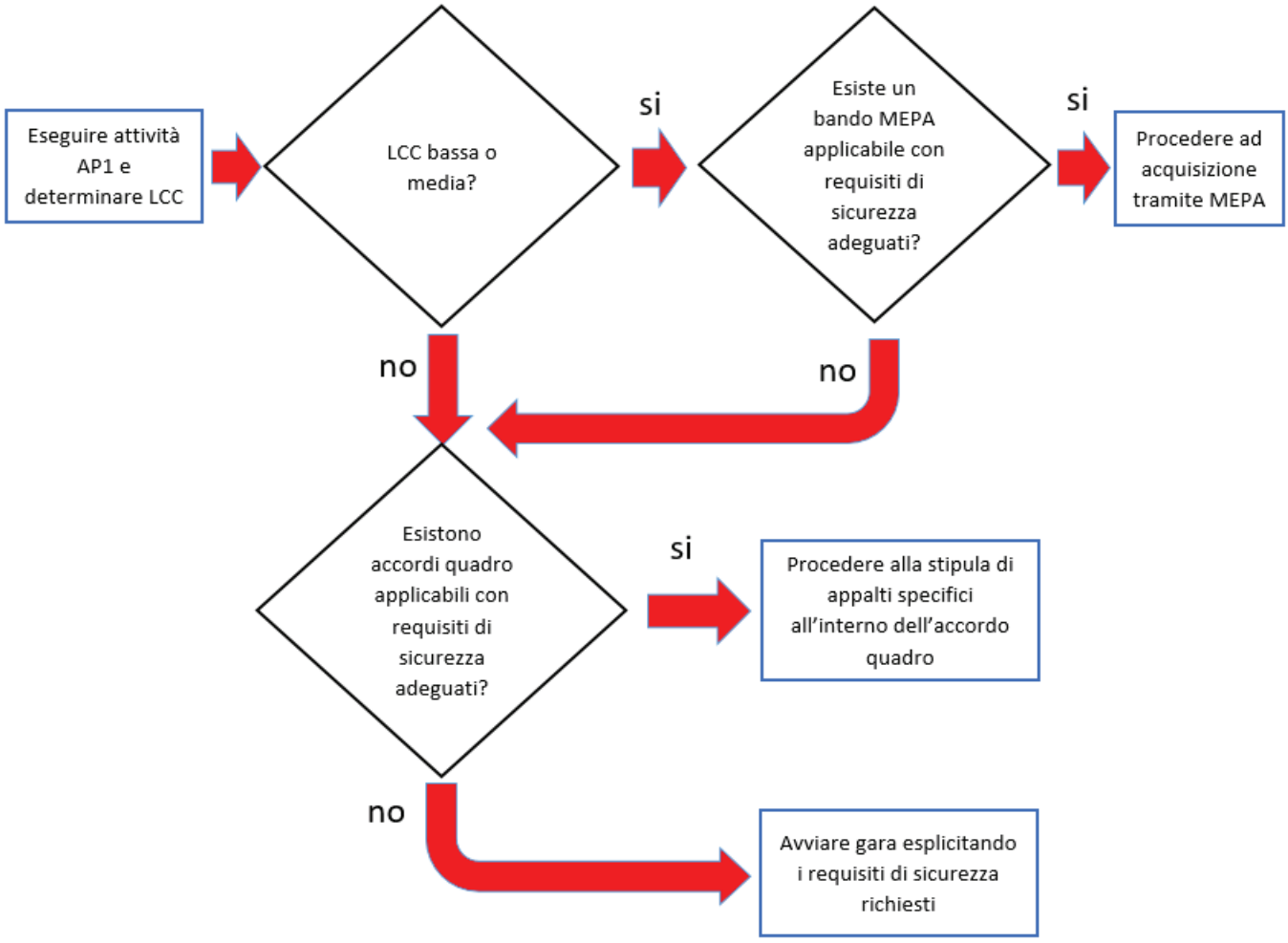

FIGURA 1: ESEMPIO DI AZIONE AP2

2.2.3 AP3 - Scegliere i requisiti di sicurezza da inserire nel capitolato

Ove l'amministrazione, a seguito dell'azione AP2, abbia scelto di procedere tramite gara, essa deve inserire nel capitolato gli opportuni requisiti di sicurezza, differenziando i requisiti che l'offerta del fornitore deve prevedere obbligatoriamente (mandatori) da quelli opzionali, che determinano eventualmente un premio nel punteggio tecnico. L'amministrazione dovrà tener conto anche dei requisiti di sicurezza quando sceglierà gli indicatori di qualità e le penali da inserire nel contratto.

Alcuni requisiti di sicurezza sono indipendenti dalla tipologia di acquisizione, e riguardano ad esempio:

- gli aspetti "minimi" di sicurezza del bene e/o servizio da acquisire (riferimento DR-6).
- le obbligazioni cui i fornitori devono attenersi per poter operare all'interno del perimetro di sicurezza dell'amministrazione (ad esempio standard di riservatezza per la gestione delle informazioni/dati da parte del fornitore; specifici standard sul trattamento di dati personali ai sensi del GDPR);
- le obbligazioni per rendere possibile ed efficace il monitoraggio della fornitura;
- le obbligazioni per rendere possibile ed efficace attività di audit (vedi paragrafo 2.1.7).

Altri requisiti di sicurezza sono invece specifici delle diverse tipologie di fornitura, in particolare sono connessi al bene o prestazione da acquisire. Si rimanda all'appendice A – Requisiti di sicurezza eleggibili, che contiene un elenco (non esaustivo ma valido per la maggior parte delle forniture pubbliche) di requisiti di sicurezza. Si raccomanda alle amministrazioni di attingere da questo elenco, piuttosto che scrivere ex-novo il testo dei propri requisiti di sicurezza, anche per omogeneizzare i vari capitolati pubblici e favorire un lessico comune tra committenti e fornitori.

Sarà cura di AgID (vedi paragrafo 3.1) estendere e aggiornare l'elenco dei requisiti anche tenendo presente eventuali segnalazioni di incompletezza, errori o obsolescenza che giungeranno dalle amministrazioni.

2.2.4 AP4 - Garantire competenze di sicurezza nella commissione di valutazione

Nel caso di gara, l'amministrazione deve tenere conto, nella scelta delle commissioni giudicatrici, dell'esigenza che almeno uno dei commissari abbia competenze in tema di sicurezza. Questa raccomandazione vale soprattutto nelle acquisizioni classificate "critiche" a seguito dell'azione AP1.

La necessità che la commissione abbia competenze specifiche sulla sicurezza, comunque, può essere mitigata scrivendo i requisiti di sicurezza in maniera chiara, oggettiva e quanto più possibile "chiusa", vale a dire lasciando meno spazio possibile all'offerta tecnica del fornitore e – di conseguenza – alla valutazione soggettiva della commissione.

Ove l'amministrazione affidi lo svolgimento della gara a una centrale di committenza, sarà quest'ultima a dover svolgere l'azione AP4. La disponibilità, presso le centrali di committenza locali, di competenze sul tema sicurezza è uno dei criteri per la scelta dell'affidamento.

Si rammenta che il Codice dei Contratti (D.Lgs. 50/2016 e s.m.i.) prevede, all'articolo 77, che i componenti della commissione giudicatrice, per gare che si aggiudicano con il criterio dell'offerta economicamente più vantaggiosa, siano iscritti all'Albo nazionale gestito dall'ANAC, di cui all'articolo 78 del Codice stesso.

Secondo la delibera ANAC n. 648 del 18 luglio 2018, punto 17, l'Albo citato doveva entrare in operatività il 15 gennaio 2019. Nel comunicato del 9 gennaio 2019, ANAC ha spostato il termine al 16 aprile 2019. Alla data di scrittura delle presenti Linee Guida, l'Albo non è ancora operativo, causa il numero insufficiente di iscrizioni.

A regime, quando l'Albo ANAC sarà operativo e conterrà una sottosezione dedicata a esperti di sicurezza informatica (al momento non prevista) l'azione AP4 si svolgerà in questo modo:

- nel caso di acquisizioni classificate critiche a seguito dell'azione AP1, l'amministrazione specificherà, nel disciplinare, che uno dei componenti della commissione sarà selezionato nella sottosezione degli esperti in sicurezza informatica dell'Albo ANAC;
- nel caso di acquisizioni non critiche, sarà facoltà dell'amministrazione specificare eventuali vincoli sulla formazione della commissione, tenendo presente le indicazioni del Codice dei Contratti.

Al momento, vista la già citata assenza di una sottosezione dell'Albo dedicata a esperti di sicurezza informatica, si ritiene si possa applicare il comma 3-bis dell'art. 77 del Codice dei Contratti, che si riporta di seguito:

"*In caso di indisponibilità o di disponibilità insufficiente di esperti iscritti nella sezione ordinaria dell'Albo (…), la commissione è nominata, anche solo parzialmente, dalla stazione appaltante competente ad effettuare la scelta del soggetto affidatario del contratto tenuto conto delle specifiche caratteristiche del contratto da affidare e delle connesse competenze.*"

Pertanto, in caso di acquisizioni classificate critiche a seguito dell'azione AP1, sarà la stazione appaltante a scegliere, applicando il comma 3-bis citato, un esperto di sicurezza informatica e inserirlo tra i componenti della commissione giudicatrice.

Si suggerisce comunque alle amministrazioni di invitare i propri esperti di sicurezza ad iscriversi all'Albo citato, compatibilmente con la disponibilità e le attività già a carico di detti esperti.

2.2.5 Check list delle azioni in fase di procurement

Il più semplice strumento operativo che si suggerisce per automatizzare le azioni dei paragrafi precedenti è la check list che segue, utile all'amministrazione per ricapitolare le decisioni prese e verificare di aver svolto puntualmente gli adempimenti necessari in questa fase.

TABELLA 4: CHECK LIST DELLE AZIONI IN FASE DI PROCUREMENT

Azione	Domande	Risposte
AP1	Come è stata classificata l'acquisizione in oggetto? (es. alta, media o bassa criticità)	
AP2	Quale strumento di acquisizione è stato scelto? (es. MEPA, accordo quadro, nuova gara, …)	
AP3	Nel capitolato di gara sono stati inseriti tutti i requisiti di sicurezza necessari?	
	È stato necessario definire requisiti non presenti nelle tabelle dell'appendice A, o modificarne alcuni? In caso, le variazioni sono stati comunicate ad AgID?	
AP4	La commissione giudicatrice ha competenze in tema di sicurezza?	
	I requisiti di sicurezza presenti nel capitolato sono scritti in maniera chiara, oggettiva e "chiusa", facilitando così il compito della commissione giudicatrice?	

2.3 Azioni da svolgere dopo la stipula del contratto (in esecuzione e/o a posteriori).

Le azioni elencate in questo paragrafo sono generalmente di tipo operativo, dipendono dalla tipologia di fornitura (si veda la matrice azione - tipologia al successivo paragrafo 2.3.15) e sono in connessione con le azioni di cui ai paragrafi 2.1 e 2.2, nel senso che non possono essere svolte in modo efficace se, prima e durante la fase di acquisizione, non sono state eseguite le azioni ad esse propedeutiche. Ad esempio, l'azione A10 deve essere preceduta dalla azione AG4.

Si tratta, per la quasi totalità, di verifiche del soddisfacimento di requisiti definiti in fase di acquisizione e presenti nel capitolato di gara, oppure di dichiarazioni presenti nell'offerta tecnica del fornitore. Per quanto riguarda le azioni da svolgere dopo la chiusura del contratto, alcune sono collegate alla tipologia del contratto stesso, altre sono più generali e si riconducono alle azioni di cui al paragrafo 2.1.

Ad ogni azione deve essere associato, anche formalmente, il ruolo o la struttura dell'amministrazione che ha la responsabilità dell'azione stessa (si veda, a questo proposito, il paragrafo 2.1.3).

2.3.1 A1 - Gestire le utenze dei fornitori

L'amministrazione deve fornire, ai dipendenti del fornitore che hanno necessità di accedere alle infrastrutture dell'amministrazione stessa, utenze nominative in accordo con le politiche di sicurezza definite (in via generale per tutte le forniture, o nel singolo contratto). Questa azione rientra nell'attività che in letteratura tecnica si chiama Account Management.

Gli accessi del fornitore dovranno poter essere tracciati e verificati (l'effettivo tracciamento potrà essere svolto o meno, a seconda della situazione e della criticità delle prestazioni erogate dal fornitore).

2.3.2 A2 - Gestire l'utilizzo di dispositivi di proprietà del fornitore

Le caratteristiche di sicurezza (ad esempio la crittografia dei dati) che i dispositivi del fornitore (computer, portatili, tablet, ecc.) devono rispettare per accedere alla rete dell'amministrazione devono essere specificate come requisiti nel capitolato tecnico (si veda R1 in Appendice A), in quanto probabilmente comportano un costo per il fornitore, che deve poterne tener conto nella formulazione della sua offerta economica.

Pertanto, l'azione A2 consiste nella sistematica verifica di conformità dei dispositivi rispetto a quanto richiesto nel capitolato. Ove il capitolato escluda la possibilità, da parte del fornitore, di utilizzare propri dispositivi per accedere a dati e reti dell'amministrazione, l'azione A2 consiste nella verifica che questo divieto venga rispettato. Non è superfluo ricordarlo, perché si ha contezza di contratti che prevedono regole di questo tipo, che però vengono vanificate da assenza di controlli periodici e puntuali (il controllo, a volte, viene demandato allo stesso fornitore).

2.3.3 A3 - Gestire l'accesso alla rete dell'amministrazione

L'accesso alla rete locale dell'amministrazione da parte del fornitore deve essere configurato con le abilitazioni strettamente necessarie alla realizzazione di quanto contrattualizzato, vale a dire consentendo l'accesso esclusivamente alle risorse necessarie. L'accesso dall'esterno mediante VPN deve essere consentito, solo se strettamente necessario, utilizzando account VPN personali configurati e abilitati opportunamente. Gli accessi dovranno poter essere tracciati per eventuali successivi audit (si veda l'azione AG6).

2.3.4 A4 - Gestire l'accesso ai server/database

Nelle forniture di sviluppo e manutenzione, l'utilizzo dei dati dell'amministrazione per la realizzazione di quanto contrattualizzato deve essere consentito esclusivamente su server/database di sviluppo nei quali sono stati importati i dati necessari per gli scopi del progetto. Pertanto, questa azione consiste nel gestire l'accesso ai server e ai DB in modo da rispettare questa regola generale, tracciando le eventuali eccezioni che dovessero verificarsi.

Ove il tipo di fornitura e/o il contesto particolare determini la necessità di regole diverse per l'accesso ai server e ai DB, queste devono essere definite nei documenti contrattuali (ad esempio sotto forma di in uno specifico requisito) e l'azione A4 consisterà nel verificare il rispetto di quanto definito.

2.3.5 A5 - Stipulare accordi di autorizzazione - riservatezza - confidenzialità

Nei tipici contratti pluriennali multi-iniziativa, l'amministrazione deve stipulare accordi di autorizzazione (clearance) e riservatezza con ogni singolo fornitore prima dell'avvio di ogni progetto. L'azione A5 consiste nella gestione documentale di tali accordi. Si suggerisce all'amministrazione di definire modelli standard per questi accordi, eventualmente derivandoli da buone prassi comuni (vedi azione AG2).

Inoltre, ogni fornitore dovrà presentare all'amministrazione l'elenco dei dipendenti che saranno impiegati sul singolo progetto e far sottoscrivere a ogni dipendente dichiarazioni di riservatezza/confidenzialità. L'azione A5 include quindi anche la raccolta, verifica e conservazione delle dichiarazioni consegnate dal fornitore.

2.3.6 A6 - Verificare il rispetto delle prescrizioni di sicurezza nello sviluppo applicativo

In forniture di tipologia sviluppo applicativo e/o manutenzione evolutiva che sono state classificate critiche, l'amministrazione deve aver definito - nel capitolato tecnico o in qualche suo allegato - requisiti in termini di sicurezza.

Questi requisiti possono essere:

1) **di tipo generico**, che lasciano al fornitore la libertà di scegliere la tecnologia e la metodologia da impiegare, dichiarandoli nella propria offerta tecnica (che va poi valutata dalla commissione giudicatrice);

2) **specifiche tecniche puntuali**, ad esempio piattaforma e linguaggio di programmazione da utilizzare; metodologie di sviluppo basata sul rispetto dei principi di "Security and Privacy by Design"; DBMS, middleware e librerie consentite, periodicità delle verifiche, della revisione del codice e dei vulnerability assessment. A tale fine far riferimento alle linee guida AgID sullo sviluppo del software sicuro (Rif. DR-4, paragrafo 1.5).

Nel caso 1), l'azione A6 consiste nel verificare sistematicamente, nel corso dell'intero contratto, che il fornitore stia effettivamente utilizzando le tecnologie e le metodologie che ha dichiarato nell'offerta tecnica, e sulla base delle quali ha ottenuto il proprio punteggio tecnico.

Nel caso 2), l'azione A6 consiste nel verificare sistematicamente, nel corso dell'intero contratto, che il fornitore stia rispettando le specifiche tecniche puntuali presenti nel capitolato.

Si suggerisce che queste verifiche, in quanto richiedono un impegno non trascurabile, vengano svolte nell'ambito delle attività di monitoraggio del contratto. Esse saranno condotte internamente all'amministrazione se questa possiede le necessarie competenze, oppure saranno affidate a un monitore esterno tramite un opportuno contratto per servizi di questo tipo. Potranno anche rientrare nelle attività di audit di cui al paragrafo 2.1.6.

Nel caso di contratti non soggetti a monitoraggio, l'amministrazione dovrà svolgere l'azione A6 nell'ambito della gestione del contratto stesso, affidandone la responsabilità al direttore dell'esecuzione o a una struttura tecnica che riferisca a quest'ultimo.

2.3.7 A7 - Monitorare le utenze e gli accessi dei fornitori

Come estensione dell'azione A1, nel caso di contratti pluriennali che prevedono lo sviluppo di più progetti e sia consentito il turn-over del personale dei fornitori, l'amministrazione deve creare e mantenere costantemente aggiornata una matrice Progetto-Fornitori e Ruoli-Utenze che aiuti a monitorare e verificare l'impiego da parte del fornitore di personale con qualifica e formazione adeguata e la corretta rimozione dei permessi (deprovisioning) delle utenze.

2.3.8 A8 - Verificare la documentazione finale di progetto

Alla fine di ogni singolo progetto (che come specificato in precedenza non coincide necessariamente col termine del contratto), l'amministrazione deve verificare che il fornitore rilasci la seguente documentazione:

- documentazione finale e completa del progetto;
- manuale di installazione/configurazione;
- report degli Assessment di Sicurezza eseguiti con indicazione delle vulnerabilità riscontrate e le azioni di risoluzione/mitigazione apportate.
- "libretto di manutenzione" del prodotto (software o hardware), con l'indicazione delle attività da eseguire per mantenere un adeguato livello di sicurezza del prodotto realizzato o acquistato. In particolare, nel libretto di manutenzione deve essere indicato:
  - produttore e versione dei prodotti software utilizzati (ad esempio web server, application server, CMS, DBMS), librerie, firmware;
  - indicazioni per il reperimento dei Bollettini di Sicurezza dei singoli produttori di hardware/software;
  - indicazioni sul processo di installazione degli aggiornamenti sicurezza;
  - documento di EoL (documento che contiene indicazione dei prodotti utilizzati e relativo fine vita/rilascio aggiornamenti sicurezza).

Si tratta, anche in questo caso, di una verifica operativa di un impegno che dev'essere preventivamente inserito nel contratto o nel capitolato (vedi paragrafo 2.2.3).

2.3.9 A9 - Effettuare la rimozione dei permessi (deprovisioning) al termine di ogni progetto

Al termine di ogni singolo progetto l'amministrazione deve obbligatoriamente eseguire le seguenti attività:

- deprovisioning delle utenze logiche del fornitore;
- deprovisioning degli accessi fisici del fornitore;
- deprovisioning delle utenze VPN;
- deprovisioning delle regole Firewall;
- richiedere dichiarazione di avvenuta cancellazione dei dati sui dispositivi utilizzati dal fornitore durante il progetto.

2.3.10 A10 - Aggiornare l'inventario dei beni

Nel caso di progetti realizzativi e di acquisizioni, l'amministrazione deve:

- inserire l'eventuale hardware acquisito nell'inventario dei beni dell'amministrazione (vedi paragrafo 2.1.4);

- inserire l'eventuale software realizzato o acquisito (insieme al relativo middleware e alle librerie a corredo) nell'inventario dei beni dell'amministrazione;
- inserire gli oggetti di cui ai punti precedenti nel sistema di backup / disaster recovery dell'amministrazione ed eventualmente anche in un sistema di monitoraggio web server / servizi (es: Uptime Robot, SIEM);
- verificare che la documentazione e le procedure operative che riguardano la sicurezza vengano aggiornate, nel corso del contratto, a ogni cambiamento, fornendo una tempestiva comunicazione interna della variazione.

2.3.11 A11 - Distruzione del contenuto logico (wiping) dei dispositivi che vengono sostituiti

Nelle acquisizioni di attività di conduzione CED o di gestione di parchi di PC (fleet management), occorre verificare che l'hardware dismesso, si tratti di server o di postazioni di lavoro, venga cancellato e distrutto in modo sicuro, evitando rischi che dati critici possano restare erroneamente memorizzati sull'hardware dismesso.

Anche in questo caso, scrivere il requisito nel capitolato non è sufficiente: va definito un processo di verifica strutturato. Il processo può prevedere:

- la consegna di un verbale di avvenuta distruzione da parte del fornitore,
- nel caso di sistemi critici, un'eventuale azione ispettiva che può ad esempio far parte delle attività di monitoraggio.

2.3.12 A12 - Manutenzione - aggiornamento dei prodotti

Per mantenere un adeguato livello di sicurezza, i prodotti software/hardware acquistati o realizzati devono essere correttamente manutenuti in base alle indicazioni del fornitore nel "Libretto di Manutenzione" (vedi azione A8).

In aggiunta a quanto sopra, gli amministratori di sistema devono obbligatoriamente eseguire gli aggiornamenti ogni qualvolta sui siti dei produttori vengono rilasciati patch e correzioni per problemi di vulnerabilità.

2.3.13 A13 - Vulnerability Assessment

L'amministrazione deve eseguire, su beni e servizi classificati critici ed esposti sul web, un Vulnerability Assessment. La periodicità e la tipologia di assessment dipenderà dal grado di criticità del bene e servizio (vedi azione AG5). Come indicazione orientativa, si suggerisce di svolgere assessment a cadenza almeno annuale, e ogni volta che si apportano modifiche alla configurazione software/hardware.

2.3.14 Matrice applicabilità Azione - Requisito

La maggior parte delle azioni da svolgere dopo la stipula del contratto sono in relazione 1 a N con i requisiti di sicurezza di cui all'Appendice A. Di seguito, una tabella di corrispondenza, di scopo esplicativo senza pretesa di esaustività.

TABELLA 5: MATRICE "AZIONE - REQUISITI"

Azione	Requisiti Appendice A
A1	R1, R20, R27, R31, R40
A2	R1, R5, R9, R19

A3	R1, R12, R13, R14, R20, R25, R34, R35, R36, R39
A4	R1, R20
A5	R7, R15, R18
A6	Da R20 a R23, più i requisiti di sicurezza specifici dello sviluppo applicativo richiesto
A7	Gli stessi requisiti di A1
A8	Da R20 a R23, R38
A9	R1, R20, R23, R40
A10	R23, R33, R38, R45
A11	R1, R4, R5
A12	R23, R45
A13	R4, da R8 a R14, R32, R33

2.3.15 Matrice applicabilità Azione - Tipologia Fornitura

Con riferimento alla classificazione delle forniture riportata nel paragrafo 1.1, si riporta di seguito la matrice di applicabilità azione - tipologia fornitura:

TABELLA 6: MATRICE "AZIONE - TIPOLOGIA FORNITURA"

	Tipologia di fornitura			
Azione	a) sviluppi e MEV	b) acquisizione di prodotti	c) operation/conduzione	d) servizi diversi da a) e c)
A1	X		X	
A2	X	X	X	X
A3	X	X	X	X
A4	X		X	
A5	X		X	X
A6	X	X	X	X
A7	X	X	X	
A8	X			
A9	X			
A10	X	X		
A11		X		
A12	X	X	X	
A13	X			

2.4 Impatto delle azioni per le amministrazioni

Nella tabella che segue, le azioni illustrate nei paragrafi precedenti sono classificate in base all'impatto e alla "onerosità" delle stesse per le amministrazioni, vale a dire in base a quanto l'amministrazione deve investire, in impegno e risorse, per effettuarle.

NB: i valori riportati nella colonna 2 della tabella sono tipici, nel senso che rappresentano - statisticamente - la situazione della grande maggioranza delle amministrazioni: non è tuttavia da escludere la possibilità che, in casi particolari, il livello di impatto effettivo di una o più azioni sia più alto o più basso del valore di colonna 2. Ad esempio, ove il personale di un'amministrazione sia già formato sui temi della sicurezza, l'azione AG1 potrà avere un livello di impatto basso; allo stesso modo, in situazioni ove ci sia un uso massiccio e poco disciplinato di dispositivi di proprietà del fornitore, l'azione A2 potrebbe avere livello di impatto medio o anche alto.

TABELLA 7: IMPATTO DELLE AZIONI PER LE AMMINISTRAZIONI

Azione	Livello di impatto	Note
AG1	Medio	Comporta attività di formazione.

AG2	Basso	Solo modifiche organizzative.
AG3	Basso	Solo modifiche organizzative, e una tantum.
AG4	Alto	Comporta un assessment, potrebbe essere oneroso ove il patrimonio ICT dell'amministrazione sia esteso e le informazioni su di esso siano obsolete.
AG5	Alto	Comporta attività di BIA e di RA. Possibile rivolgersi a società esterne.
AG6	Basso	Azione una tantum.
AG7	Basso	Azione una tantum.
AP1	Basso	L'azione può essere facilitata usando strumenti come la tabella 3.
AP2	Basso	L'azione può essere facilitata seguendo un processo di scelta strutturato come in figura 1.
AP3	Basso	L'azione può essere facilitata usando le tabelle dell'Appendice A.
AP4	Medio	Può comportare attività di formazione.
A1	Basso	Modifiche organizzative e strutturazione di processi già presenti.
A2	Basso	Essenzialmente modifiche organizzative.
A3	Basso	Essenzialmente modifiche organizzative.
A4	Basso	Essenzialmente modifiche organizzative.
A5	Basso	Essenzialmente modifiche organizzative.
A6	Basso	Modifiche organizzative e strutturazione di processi già presenti.
A7	Basso	Modifiche organizzative e strutturazione di processi già presenti.
A8	Medio	Prevede verifica di documenti, pertanto il livello d'impatto dipende dalla complessità di questi ultimi.
A9	Basso	Essenzialmente modifiche organizzative.
A10	Medio	Vedi note per AG4 e AG5.
A11	Medio	Possibile l'uso di strumenti specifici.
A12	Alto	Sono possibili costi aggiuntivi per manutenzione e aggiornamento di prodotti.
A13	Alto	Può comportare l'acquisizione di servizi esterni.

Come si nota dalla tabella, la maggior parte delle azioni sono di "basso impatto", in quanto esse si configurano come semplici mutamenti organizzativi o strutturazione di processi già presenti. Dato il basso impatto, non si ravvisano motivi per cui le amministrazioni non possano attrezzarsi da subito per svolgere tale azioni. Potrebbero, al più, costituire eccezione P.A. di dimensioni estremamente ridotte, ad esempio piccolissimi comuni con personale minimo, che peraltro difficilmente intraprendono acquisizioni ICT critiche sotto l'aspetto della sicurezza.

Le azioni di "medio impatto" prevedono investimenti sulle risorse interne dell'amministrazione, e potrebbero determinare necessità di incentivi, straordinari o meccanismi premianti per il personale. Pertanto le amministrazioni devono strutturarsi per svolgere queste azioni nei tempi e nelle modalità compatibili con il budget a disposizione, considerando comunque che i costi da sostenere sono interni, riguardando il personale, e non sono necessariamente da imputare alla spesa per l'informatica.

Le azioni di "alto impatto" potrebbero coinvolgere risorse esterne all'amministrazioni (ad esempio monitori), per cui potrebbero determinare costi aggiuntivi (esterni, da imputare prevalentemente al settore informatico) per l'amministrazione stessa. Non si ritiene pertanto di poter imporre alle amministrazioni, di qualunque grandezza e tipologia, di svolgere obbligatoriamente da subito queste azioni. Le P.A. dovranno valutare tempi e modi per la loro progressiva adozione, ad esempio effettuandole in occasione di un'acquisizione ICT effettivamente critica, tenendo comunque conto che i costi esterni sostenuti rappresentano un investimento, che verrà ripagato già nel breve periodo dall'innalzamento della sicurezza complessiva e dunque dal minore rischio per l'amministrazione stessa. Le P.A. devono inoltre tener presente che, sebbene alcune azioni vadano ripetute nel tempo, l'impatto maggiore si ha la prima volta che esse vengono eseguite, mentre le successive (aggiornamento) il loro impatto è nettamente inferiore.

3 Indicazioni per AgID

Il tavolo di lavoro ha identificato, anche sulla base dei risultati di una rilevazione condotta nell'ambito delle organizzazioni coinvolte nei lavori (vedi paragrafo 1.1), quali, tra le esigenze delle amministrazioni pubbliche sul tema della sicurezza nel procurement ICT, potrebbero essere soddisfatte da una struttura centrale di indirizzo, supporto e mediazione quale l'AgID.

Nei paragrafi che seguono vengono elencati i compiti che l'Agenzia potrebbe svolgere in modo istituzionale, eventualmente formalizzandoli in una futura edizione del Piano Triennale.

3.1 Presidiare la tematica "sicurezza nel procurement ICT"

Il presente documento, come detto, si configura come una delle linee guida AgID ai sensi dell'art. 71 del CAD, ed ha pertanto la valenza giuridica prevista dal Codice stesso.

L'Agenzia è responsabile della manutenzione e dell'aggiornamento di questo documento, con modalità e tempistica da definirsi, comunque in coerenza con le prescrizioni dell'art. 71 del CAD.

Almeno per i primi 6 mesi dalla pubblicazione di questo documento, l'AgID ne promuove la diffusione e il recepimento. Ciò avverrà tramite seminari, presentazioni ed eventi per illustrarne il contenuto alle amministrazioni. Sarà fornito anche un supporto a richiesta, ad esempio tramite una casella di posta elettronica, presidiata da AgID, per spiegazioni e chiarimenti sui contenuti del documento.

Al termine del primo periodo, le domande/risposte raccolte formeranno una FAQ o la base per altri strumenti automatici di supporto per le amministrazioni, che saranno messi a disposizione su una pagina specifica del sito web di AgID, dedicata appunto al tema della sicurezza nel procurement ICT. Inoltre i riscontri ottenuti nel primo periodo saranno utilizzati per una revisione del documento (in particolare, per estendere e modificare l'appendice A, che al momento contiene solo alcuni esempi, e che dovrebbe invece diventare una sorta di "massimario" per i requisiti di sicurezza nei capitolati).

AgID monitorerà l'applicazione delle linee guida con un questionario annuale indirizzato – a campione – alle amministrazioni, ove verranno richieste informazioni sugli strumenti adottati e sui risultati conseguiti.

3.2 Veicolare best practice tra le PA

Come anticipato al paragrafo 2.1.2, AgID fungerà da punto di raccolta e diffusione di casi di studio - tratti dalle esperienze positive e negative delle amministrazioni - sul tema della sicurezza nel procurement ICT.

Sarà creato un Forum, moderato da AgID, cui le amministrazioni si potranno iscrivere e postare la loro esperienza, le criticità che hanno riscontrato, le soluzioni che hanno adottato, le scelte cui sono pervenute. AgID supervisionerà il Forum, approverà i contributi delle amministrazioni, eventualmente effettuando opportune azioni a tutela della privacy e della libera concorrenza (es. rimozione di nomi e marchi di prodotti), deriverà statistiche e trend.

AgID metterà in contatto amministrazioni con esigenze e problematiche simili (ove l'Agenzia ne venga a conoscenza e le suddette amministrazioni offrano disponibilità) eventualmente partecipando agli incontri tra le amministrazioni interessate o mediando in posizione di terzietà.

Il Forum, come le FAQ, un archivio di modelli contrattuali, e altri strumenti di collaboration, saranno resi disponibili per l'accesso sul sito istituzionale dell'Agenzia, in una pagina dedicata alla sicurezza nel procurement ICT.

3.3 Introdurre la tematica nei pareri

I pareri resi da AgID sui contratti pubblici ai sensi dell'art. 14bis comma 2 lettera f) del CAD diverranno anche uno strumento di verifica e ausilio alle amministrazioni per il recepimento delle indicazioni delle Linee Guida sulla sicurezza nel procurement ICT.

A oggi i pareri, oltre alla tradizionale valutazione di congruità tecnico-economica, contengono anche uno specifico paragrafo dedicato alla coerenza tra le caratteristiche dell'iniziativa in esame e le indicazioni del Piano Triennale (es. uso delle piattaforme immateriali, sviluppo applicativo anche sotto forma di API, riuso e apertura delle basi dati, ...). Allo stesso modo, sarà introdotto nei pareri un paragrafo "Sicurezza nel procurement". In tale paragrafo, l'iniziativa in esame verrà analizzata e classificata in base alla rispondenza ai criteri metodologici e procedurali definiti nelle Linee Guida; in caso di non rispondenza o di rispondenza parziale a detti criteri, il parere suggerirà opportune modifiche all'iniziativa in esame per garantire un livello minimo di sicurezza non solo all'iniziativa stessa, ma più in generale alla linea progettuale e ai servizi istituzionali dell'amministrazione cui l'iniziativa afferisce.

Questa innovazione nei pareri sarà presentata tramite una specifica circolare AgID, ove verranno schematizzate le informazioni sul tema della sicurezza che l'amministrazione dovrà inserire nella richiesta di parere, ad esempio una check-list che elenchi come vengono applicate nell'iniziativa in esame le indicazioni delle Linee Guida.

3.4 Introdurre la tematica nel monitoraggio

In termini complementari al punto precedente, la tematica sicurezza sarà introdotta anche nelle attività di monitoraggio dei contratti ai sensi dell'art. 14bis comma 2 lettera h) del CAD. Com'è noto, il monitoraggio rappresenta un'attività strumentale al governo dei progetti pubblici, e si raccorda con i pareri costituendone una sorta di prosecuzione temporale (i pareri intervengono in fase ex-ante, mentre il monitoraggio avviene in itinere ed ex-post alle iniziative delle amministrazioni).

Il monitoraggio, peraltro, ha una visibilità sui progetti delle PA che può essere superiore a quella dei pareri: le circolari AgID sul monitoraggio indirizzano infatti le seguenti amministrazioni:

- amministrazioni centrali dello Stato;
- regioni e provincie autonome e gli enti a loro collegati, ovvero enti pubblici vigilati ai sensi degli art. 22, c. 1, lettera a); art. 22, c. 2, 3 del D.Lgs. 33/2013);
- ASL, Aziende Ospedaliere e ospedali universitari;
- città metropolitane.

La normativa prevede inoltre che siano sottoposti a monitoraggio le iniziative che, indipendentemente dalle dimensioni economiche:

- si riferiscano a servizi che interessino la sicurezza dello Stato, la difesa nazionale, l'ordine e la sicurezza pubblica, lo svolgimento di consultazioni elettorali nazionali ed europee;
- abbiano un rilevante impatto sotto il profilo organizzativo o dei benefici che si prefiggono di conseguire;
- che l'Agenzia ritenga necessario sottoporre a monitoraggio.

Sulla base di quanto sopra, si ritiene che il monitoraggio costituisca uno strumento efficace per la verifica della sicurezza nel procurement ICT. Si propone di inserire, tra l'elenco degli indicatori di monitoraggio, uno o più indicatori specifici sul tema sicurezza nel procurement, e di aggiornare di conseguenza gli schemi di RAC (rapporto di avanzamento, di chiusura, relazione ex post).

3.5 Adeguare la tempistica delle gare Consip a esigenze di sicurezza

Presidiare la tematica della sicurezza significa anche verificare che siano costantemente disponibili, per le amministrazioni, adeguati (e sicuri) strumenti di acquisizione di prodotti e servizi ICT.

A tale scopo, AgID propone di tener conto anche di questo obiettivo nel pianificare, di concerto con la Consip, la tempistica delle gare che interessano sistemi e progetti critici sotto l'aspetto della sicurezza, evitando ad esempio situazioni in cui convenzioni e/o accordi quadro siano esauriti e i successivi non siano ancora disponibili perché le relative gare sono ancora da aggiudicare.

4 Indicazioni per le centrali di committenza

Si premette che le indicazioni elencate nei paragrafi precedenti si applicano, in generale, anche alle centrali di committenza. In particolare, le azioni AP2, AP3 e AP4 sono da ritenersi obbligatorie, per le centrali di committenza, quando queste svolgano iniziative di acquisizione ICT nell'interesse di Ministeri, Enti centrali, Regioni e città metropolitane.

In aggiunta, si ritiene che le centrali di committenza, per il ruolo che hanno nelle acquisizioni pubbliche di beni e servizi, possono fungere da enti attuatori di miglioramenti/evoluzioni per gli aspetti di sicurezza delle forniture ICT. Anche sulla base dei risultati della rilevazione citata al paragrafo precedente, si propone alle centrali di committenza di:

- instaurare una collaborazione con il CVCN per il recepimento tempestivo, nelle gare curate dalle centrali di committenza, delle raccomandazioni in materia di sicurezza ICT;
- inserire clausole di compliance alle indicazioni in materia di sicurezza sulle gare in corso che passi attraverso anche i comitati di governo (per le gare che li prevedono);
- prevedere, per le gare che comprendono gestione di sistemi o fornitura di servizi di sicurezza, non solo flussi informativi sugli eventi critici verso l'amministrazione contraente, ma anche verso gli organismi individuati dal legislatore a presidio della sicurezza cibernetica;
- per le gare che prevedono centri servizi o servizi web, qualora si ritenga applicabile la misura, verificare la sicurezza tramite vulnerability assessment e penetration test. Il governo di queste verifiche potrebbe essere a cura di un organismo centrale (CVCN, CSIRT, CERT, altri) in collaborazione col comitato di governo della fornitura;
- sensibilizzare i fornitori al fine di anticipare le tendenze e le possibili problematiche di sicurezza che possono presentarsi (consultazioni di mercato mirate alla sicurezza);
- costruire, in accordo con ANAC, un elevato livello di cultura e formazione delle Commissioni di valutazione delle gare in ambito sicurezza (vedi paragrafo 2.2.4);
- svolgere un ruolo di omogeneizzatore/armonizzatore degli approcci di sicurezza e delle tecnologie di sicurezza erogati nell'ambito delle forniture della PA.

5 Protezione dei dati Personali

Come già accennato nei precedenti paragrafi, è fondamentale che le amministrazioni pongano attenzione alla protezione dei dati personali, sia nella fase preliminare al *procurement* sia in quella successiva alla stipula contrattuale, nel rispetto del principio di responsabilizzazione di cui agli artt. 5, par. 2 e 24 GDPR.

I principi della protezione dei dati fin dalla progettazione e per impostazione predefinita, di cui all'art. 25 GDPR, sono centrali nel contesto degli appalti pubblici e devono essere attuati sin dalle fasi prodromiche, attraverso strumenti, metodologie e competenze finalizzati a gestire adeguatamente i rischi che derivano dai trattamenti di dati personali.

Con particolare riferimento a quanto previsto dall'art. 28 GDPR, qualora le pubbliche amministrazioni intendano avvalersi di fornitori per compiere attività che presuppongono trattamenti di dati personali, le stesse sono tenute a individuare tali soggetti ricorrendo unicamente a coloro che "presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato" (art. 28, par. 1 GDPR). Tale individuazione da parte delle pubbliche amministrazioni, in qualità di titolari del trattamento, deve avvenire tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà degli interessati, nel rispetto dell'art. 24 GDPR.

Nell'ambito del capitolato di gara o degli altri strumenti di cui l'amministrazione decida di avvalersi, devono essere adeguatamente individuate le misure di sicurezza sia organizzative sia tecniche da applicare ai singoli trattamenti di dati personali, ai sensi dell'art. 32 GDPR, e la corretta ripartizione delle relative responsabilità tra amministrazione in qualità di titolare del trattamento e fornitore in qualità di responsabile del trattamento, evitando, in particolare, la previsione di sproporzionati esoneri di responsabilità specialmente in caso di contratti standard con margini di negoziazione pressoché nulli in capo al titolare del trattamento.

Una volta individuato il fornitore che tratterà i dati personali per conto dell'amministrazione nello svolgimento delle attività contrattualmente delegate, l'amministrazione deve nominarlo responsabile del trattamento ai sensi e per gli effetti degli artt. 4, n. 8 e 28 GDPR.

Il quadro di garanzie in materia di protezione dei dati personali si applica anche alle acquisizioni di *Software as a Service* (SaaS), di *Product as a Service* (PaaS) e di *Internet as a Service* (IaaS).

Appendice A – Requisiti di sicurezza eleggibili

Nelle tabelle che seguono sono elencati alcuni requisiti di sicurezza che le amministrazioni possono inserire nei propri capitolati di gara. L'elenco non è esaustivo, ha solo lo scopo di offrire alcuni esempi significativi e di favorire un lessico comune nell'esprimere requisiti di sicurezza.

Per ragioni di sintesi, il testo di alcuni requisiti (ad esempio di R1) è stato generalizzato in modo da renderlo un modello per una "famiglia di requisiti", da declinare ed eventualmente suddividere in più requisiti elementari, a seconda del contesto della singola acquisizione.

TABELLA 8: REQUISITI GENERALI (INDIPENDENTI DALLA TIPOLOGIA DI FORNITURA)

R1	Il fornitore deve adottare al proprio interno le procedure e politiche di sicurezza definite dall'amministrazione committente, con particolare riferimento alle modalità di accesso ai sistemi dell'amministrazione, all'hardening (esempio installazione di soluzioni di end point security) dei dispositivi utilizzati dal fornitore, alla gestione dei dati dell'amministrazione.
R2	Il fornitore deve possedere la certificazione ISO/IEC 27001 e mantenerla per tutta la durata della fornitura.
R3	(alternativo al precedente) Anche se il fornitore non è certificato ISO/IEC 27001, almeno deve usare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) aggiornato nel tempo e/o predisporre un piano di qualità secondo lo standard ISO 10005
R4	Il fornitore deve far eseguire annualmente un audit sul proprio sistema di sicurezza, a proprie spese e da una società specializzata scelta previa approvazione della stazione appaltante. NB: Qualora applicabile, tale attività si incrocia con il requisito R2 (le verifiche dell'Ente Certificatore hanno cadenza pressoché annuale).
R5	L'amministrazione può, con un preavviso di 20 giorni solari, richiedere ulteriori attività di auditing secondo modalità concordate con il fornitore. Le risultanze di tali audit verranno comunicate all'amministrazione.
R6	L'amministrazione, direttamente o tramite terzi incaricati, può eseguire verifiche relative alla conformità della prestazione dei servizi rispetto a quanto stabilito nel capitolato tecnico oltre che nell'offerta tecnica se migliorativa.
R7	Il personale del fornitore che presta supporto operativo nell'ambito dei servizi di sicurezza dovrà possedere certificazione su specifici aspetti della sicurezza.
R8	Il fornitore deve disporre di una struttura per la prevenzione e gestione degli incidenti informatici con il compito d'interfacciarsi con le analoghe strutture dell'amministrazione e con le strutture centrali a livello governativo.
R9	Il fornitore deve dotarsi delle misure minime di sicurezza per limitare il rischio di attacchi informatici (riferimento DR-5)
R10	Il SOC del fornitore deve sovrintendere alla gestione operativa e continuativa degli incidenti informatici sui servizi erogati nell'ambito della fornitura.
R11	Il fornitore deve garantire il rispetto di quanto richiesto dalla normativa vigente in materia di sicurezza cibernetica, anche in riferimento ai contenuti del GDPR, mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenuto conto dello stato dell'arte e dei costi di attuazione nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, e adottando procedure tecniche e organizzative volte alla gestione di eventuali violazioni di dati personali
R12	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, ecc.) necessari a rilevare e contenere eventuali incidenti di sicurezza ICT e in grado di gestire gli IoC (Indicator of Compromise).
R13	Il fornitore deve usare protocolli cifrati e meccanismi di autenticazione nell'ambito dei servizi erogati.
R14	Qualora il fornitore subisca un attacco, in conseguenza del quale vengano compromessi sistemi del committente da lui gestiti, deve farsi carico delle bonifiche del caso, e riportare i sistemi in uno stato di assenza di vulnerabilità.
R15	Il fornitore si impegna a trattare, trasferire e conservare le eventuali repliche dei dati oggetto di fornitura, ove autorizzate dalle amministrazioni, sempre all'interno del territorio dell'UE.
R16	Il fornitore deve dare disponibilità a far parte di un Comitato di Direzione Tecnica, eventualmente aperto anche a soggetti terzi, che tratti il tema della sicurezza, sia nell'ottica di favorire la risoluzione di temi aperti sia per introdurre eventuali varianti al contratto per fronteggiare nuove minacce o altro.
R17	Il fornitore deve condividere le informazioni necessarie al fine di garantire il corretto monitoraggio della qualità e della sicurezza, eventualmente pubblicando le stesse nel portale della fornitura.
R18	Il fornitore si impegna a sottoscrivere una clausola di non divulgazione (NDA) sui dati e sulle informazioni dell'amministrazione.
R19	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.

TABELLA 9: REQUISITI SPECIFICI PER FORNITURE DI SERVIZI DI SVILUPPO APPLICATIVO

R20	Il fornitore deve attenersi alla politica di sicurezza dell'amministrazione committente, con particolare riferimento all'accesso ai dati dell'amministrazione, che avverrà esclusivamente sui sistemi di sviluppo e test.
R21	In fase di analisi, il fornitore deve definire le specifiche di sicurezza (non funzionali) a partire dai requisiti espressi dall'amministrazione.

R22	In fase di progettazione codifica, il fornitore deve implementare le specifiche di sicurezza nel codice e nella struttura della basedati.
R23	Al termine del progetto, il fornitore deve rilasciare tutta la documentazione necessaria all'amministrazione per gestire correttamente quanto rilasciato anche sotto l'aspetto della sicurezza.

TABELLA 10: REQUISITI SPECIFICI PER FORNITURE DI OGGETTI CONNESSI IN RETE

R24	Supporto di protocolli sicuri e cifrati (HTTPS, SSH v2, ecc.).
R25	Filtraggio di indirizzi IP.
R26	Supporto di protocolli di autenticazione (ad esempio RADIUS, IEEE 802.1X, ecc.).
R27	Gestione di più profili con privilegi diversi.
R28	Funzionalità di "richiesta creazione o cambio della password al primo accesso".
R29	Blocco dell'utenza dopo un numero definito (fisso o variabile) di tentativi falliti di accesso.
R30	Gli accessi degli utenti devono essere registrati su un archivio (log) non cancellabile con il reset.
R31	Gestione dei log di sistema (accessi, allarmi, ecc.).
R32	Il fornitore (anche in collaborazione con il produttore della tecnologia) deve offrire processi, unità organizzative e strumenti dedicati alla gestione di vulnerabilità scoperte sui prodotti oggetto della fornitura.
R33	Per gli apparati proposti deve essere disponibile documentazione tecnica (schede tecniche, manuali, guide operative) relativa alla corretta configurazione e gestione degli aspetti di sicurezza.

TABELLA 11: REQUISITI SPECIFICI PER FORNITURE DI SERVIZI DI GESTIONE REMOTA

R34	I meccanismi di autenticazione devono essere basati su meccanismi di crittografia asimmetrica, a chiave pubblica; la lunghezza delle chiavi va impostata sulla base della criticità della comunicazione da cifrare (ad esempio 256 bit per le meno critiche, 512 bit per le più critiche). La gestione e distribuzione delle chiavi e dei certificati è a carico del fornitore.
R35	Autorizzazione: sulla base delle credenziali fornite dall'utente, si devono individuare i diritti e le autorizzazioni che l'utente possiede e permetterne l'accesso alle risorse limitatamente a tali autorizzazioni.
R36	Confidenzialità nella trasmissione dei dati: le comunicazioni tra la componente di gestione remota centralizzata e la componente locale installata presso la sede dell'amministrazione devono essere cifrate.
R37	Fornire meccanismi che permettano di garantire l'integrità di quanto trasmesso (ad esempio meccanismi di hashing).
R38	Il fornitore deve descrivere nel dettaglio le soluzioni tecniche utilizzate (dispositivi hardware e software impiegato, modalità operative, politiche di sicurezza, …) per soddisfare i requisiti di sicurezza dell'amministrazione committente.
R39	In fase di attivazione del servizio, il fornitore deve concordare con l'amministrazione le modalità operative e le politiche di sicurezza, i livelli di gravità degli incidenti, le attività e le contromisure che dovranno essere svolte per contrastare le minacce.
R40	Il fornitore dovrà attenersi alle politiche di sicurezza definite dalla committente, con particolare riferimento alla definizione di ruoli e utenze per l'accesso ai sistemi gestiti.
R41	In caso di necessità, da parte degli operatori, di accesso a Internet, il fornitore deve utilizzare un proxy centralizzato e dotato di configurazione coerente con la politica di sicurezza definita dall'amministrazione.
R42	In caso di rilevazione di un incidente di gravità elevata (con scala da definire a inizio fornitura), il fornitore deve dare immediata notifica, tramite canali concordati con l'amministrazione, dell'incidente rilevato e delle azioni da intraprendere, al Responsabile della Sicurezza indicato dall'amministrazione e agli organismi individuati dal legislatore a presidio della sicurezza cibernetica.
R43	Per ogni incidente di sicurezza, il fornitore s'impegna a consegnare all'amministrazione, entro il giorno successivo, un report che descriva la tipologia di attacco subito, le vulnerabilità sfruttate, la sequenza temporale degli eventi e le contromisure adottate.
R44	Su richiesta dell'amministrazione, il fornitore deve consegnare i log di sistema generati dai dispositivi di sicurezza utilizzati, almeno in formato CSV o TXT. Tali log dovranno essere inviati all'amministrazione entro il giorno successivo a quello in cui è avvenuta la richiesta.
R45	Il fornitore deve monitorare la pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi utilizzati per erogare i servizi e nelle infrastrutture gestite. Entro il giorno successivo al rilascio dell'upgrade/patch/hotfix, il fornitore deve avviare una valutazione, da rilasciarsi entro un numero giorni da stabilirsi, propedeutica all'installazione delle stesse sui dispositivi di sicurezza, che ad esempio identifichi la possibilità di applicare la patch immediatamente, o la necessità di apportare MEV o integrazioni prima di procedere alle installazioni.