AGID
Agenzia per l'Italia Digitale

FormezPA

FORMAZIONE AGID – FORMEZ SULLA TRANSIZIONE DIGITALE DELLA PA

Progetto Informazione e formazione per la transizione digitale della PA nell'ambito del progetto «Italia Login – la casa del cittadino»

(A valere sul PON Governance e Capacità Istituzionale 2014-2020)

UNIONE EUROPEA
Dipartimento della Funzione Pubblica
AGID Agenzia per l'Italia digitale

AGID
Agenzia per l'Italia Digitale

FormezPA

La sicurezza informatica nella PA

Webinar: Linee Guida «La sicurezza nel procurement ICT»

2 Dicembre 2021

Dario Basti
CERT-AgID

UNIONE EUROPEA

Dipartimento della Funzione Pubblica

AGID Agenzia per l'Italia digitale

Contesto

«*Abbiano inoltre registrato nel corso degli ultimi dodici mesi un incremento di attacchi veicolati tramite* ***l'abuso della supply chain****, ovvero tramite la compromissione di terze parti, il che consente poi a criminali e spie di colpire i contatti (clienti, fornitori, partner) dell'obiettivo, ampliando notevolmente il numero delle vittime e passando più facilmente inosservati*»

Linee guida - "La sicurezza nel procurement ICT"

Genesi e ambito del documento

Le «**Linee guida La sicurezza nel procurement ICT**» adottate con **Determinazione n. 220/2020** del 17 maggio 2020, rappresentano 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:

- AgID
- MiSE
- PCM Dip. Protezione Civile
- MEF
- Min. Esteri
- Min. Interno

- PCM-DIS
- Consip
- Min. Difesa
- Dip. PS
- Min. Giustizia

Linee guida - "La sicurezza nel procurement ICT"

Finalità del documento

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.

Linee guida - "La sicurezza nel procurement ICT"

A chi è rivolto il documento

Persone 

Dirigenti e funzionari delle pubbliche amministrazioni, RUP delle gare pubbliche, RTD - Responsabili della transizione al digitale (definiti dal CAD);

Amministrazioni 

Indicazioni vincolanti per i Ministeri, gli Enti centrali, le Regioni e le città metropolitane;
Suggerimenti, buone pratiche e procedure cui far riferimento per le restanti amministrazioni.

Fornitori 

Per far conoscere le problematiche legate alla sicurezza nel procurement ICT delle Pubbliche Amministrazioni.

Linee guida - "La sicurezza nel procurement ICT"

Struttura del documento

- **Capitolo 1** – Premessa
- **Capitolo 2** - Indicazioni per le amministrazioni
  - Paragrafo 2.1 - **Azioni da svolgere prima della fase di procurement**
  - Paragrafo 2.2 - **Azioni da svolgere durante la fase di procurement**
  - Paragrafo 2.3 - **Azioni da svolgere dopo la fase di procurement (in esecuzione e/o a posteriori**)
- **Capitolo 3** – Indicazioni per AgID
- **Capitolo 4** – Indicazioni per le Centrali di committenza
- **Capitolo 5** – Protezione dei dati personali
- **Appendice – A** – Requisiti Sicurezza Ammissibili

Linee guida - "La sicurezza nel procurement ICT"

2. Indicazioni per le amministrazioni

Azioni da compiere nelle varie fasi del processo di acquisizione, requisiti da capitolato, suggerimenti da declinare per le varie tipologie di acquisizione.

2.1 Azioni da svolgere prima della fase di procurement
(es. classificazione di sistemi/servizi per criticità, definizione metodologie generali, piani di contingenza, formazione, politiche per il personale, sensibilizzazione decisori, ecc.)

2.2 Azioni da svolgere in fase di procurement
(*scrittura documentazione di gara, formazione commissioni, scelta criteri per l'ammissione e l'assegnazione dei punteggi, ecc.*)

2.3 Azioni da svolgere dopo la stipula del contratto
(aspetti di cui tener conto in operatività o a posteriori, dopo la chiusura del contratto)

Linee guida - "La sicurezza nel procurement ICT"

2.1 Azioni da svolgere prima della fase di procurement - 1 di 3

AG1 - Promuovere competenza e consapevolezza

- ***Disporre*** *di risorse umane con competenze aggiornate di Procurement Management, Gestione Progetti, Risk Management –Sicurezza e protezione dati –*
- ***Definire*** *Percorsi Formativi e di Sensibilizzazione*
- ***Organizzare*** *eventi tematici, seminari sui rischi della 'non sicurezza'*

AG2 - Raccogliere buone prassi ed esperienze

- *Raccogliere al proprio interno casi di successo/insuccesso, in termini di sicurezza, riscontrati nelle precedenti acquisizioni ICT*

AG3 - Stabilire ruoli e responsabilità

- *Definire, all'interno della propria struttura, ruoli e responsabilità connesse con la sicurezza del procurement ICT, identificando profili idonei e assegnando incarichi formali (Matrice RACI-VS)*

Linee guida - "La sicurezza nel procurement ICT"

Esempio Matrice RACI-VS

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.

Linee guida - "La sicurezza nel procurement ICT"

2.1 Azioni da svolgere prima della fase di procurement - 2 di 3

AG4 - Effettuare una ricognizione dei beni informatici e dei servizi

- L'amministrazione deve **disporre di un inventario aggiornato** dei propri beni informatici ("asset")
- **Definire l'owner/responsabile di ogni asset** in termini di protezione dei requisiti generali di sicurezza (Riservatezza, Integrità, Disponibilità, Non Ripudio, Autenticità)
- **Costituire un analogo inventario/catalogo dei servizi** che l'amministrazione eroga al suo interno e nei confronti dei suoi utenti istituzionali (cittadini, imprese)
- **Mapping tra i due inventari (asset e servizi)**. Ad esempio quali beni informatici sono utilizzati per erogare quali servizi.
- **Aggiornamento continuo dei due inventari (asset, servizi)**

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

- ***Classificare i beni e i servizi individuati (AG4)*** *in termini di* ***criticità, rischi, minacce, vulnerabilità*** *(Risk Assessment - Business Impact Analisys periodici o a seguito di eventi che cambiano le condizioni operativi dell'amministrazione)*

Linee guida - "La sicurezza nel procurement ICT"

2.1 Azioni da svolgere prima della fase di procurement - 3 di 3

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

Organizzarsi in modo da poter svolgere efficaci azioni di audit *nei confronti dei propri fornitori*

- ***Definire processo e modalità di svolgimento delle attività di audit*** *ed esplicitarle nei capitolati di gare e/o contratti con i fornitori*
  - ***Stabilire****:*
    1. ***Obiettivi*** *(es. Verificare le misure di sicurezza adottate dal fornitore nell'erogazione delle sue prestazioni)*
    2. ***Periodicità*** *con la quale verranno eseguiti audit*
    3. ***Indicatori*** *(metodi e misure che saranno utilizzati)*

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).*

Linee guida - "La sicurezza nel procurement ICT"

CHECK LIST Azioni Generali

Attraverso la tabella mostrata, l'amministrazione pu ò verificare a che livello di preparazione si trovanel co ntesto 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 della singola amministrazione.

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)

Linee guida - "La sicurezza nel procurement ICT"

2.2 Azioni da svolgere durante la fase di procurement - 1 di 4

Il paragrafo **elenca 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.

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

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).

Linee guida - "La sicurezza nel procurement ICT"

Calcolo Criticità Acquisizione

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.

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	

Linee guida - "La sicurezza nel procurement ICT"

2.2 Azioni da svolgere durante la fase di procurement - 2 di 4

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

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

MEPA
aquistinretepa.it

Linee guida - "La sicurezza nel procurement ICT"

Esempio Azione AP2

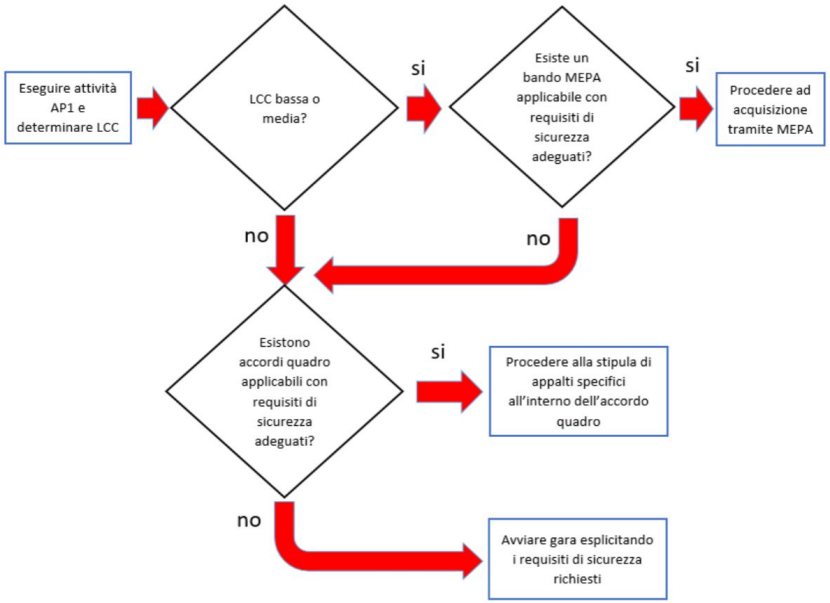

FIGURA 1: ESEMPIO DI AZIONE AP2

Linee guida - "La sicurezza nel procurement ICT"

2.2 Azioni da svolgere durante la fase di procurement - 3 di 4

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

Requisiti Indipendenti dalla tipologia di acquisizione (**Generici**):

- **Requisiti Minimi**
- **Standard Riservatezza**
- **GDPR**
- **Audit**

Requisiti specifici della fornitura

- **Appendice A – Requisiti Sicurezza Eleggibili**
  - Requisiti specifici per forniture di **servizi di sviluppo applicativo**
- Requisiti specifici per forniture di **oggetti connessi in rete**
  - Requisiti specifici per forniture di **servizi di gestione remota**

Linee guida - "La sicurezza nel procurement ICT"

2.2 Azioni da svolgere durante la fase di procurement - 4 di 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.

- Codice dei Contratti (D.Lgs. 50/2016 e s.m.i.) prevede, all'articolo 77 che i componenti della commissione siano iscritti all'**Albo ANAC** (Ad oggi non ancora operativo)

«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»

Per le acquisizioni classificate come critiche – si può applicare - comma 3-bis dell'art. 77 del Codice dei Contratti – «*La stazione appaltante individua ed inserisce nella commissione un esperto di Sicurezza Informatica*»

Linee guida - "La sicurezza nel procurement ICT"

2.2 CHECK LIST DELLE AZIONI IN FASE DI PROCUREMENT

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?	

Linee guida - "La sicurezza nel procurement ICT"

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** e dipendono dalla tipologia di fornitura (si veda la matrice azione - tipologia al seguente) 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.

TABELLA 6: MATRICE "AZIONE - TIPOLOGIA FORNITURA"

Azione	Tipologia di fornitura			
	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			

Linee guida - "La sicurezza nel procurement ICT"

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

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.

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 – (Inserimento nel capitolato e verifica continua in questa fase).

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 (VPN, Log).

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.

A5 - Stipulare accordi di autorizzazione - riservatezza - confidenzialità.

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. Definire (Modelli- Standard)

Linee guida - "La sicurezza nel procurement ICT"

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

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

*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/o che stia rispettando le specifiche tecniche puntuali presenti nel capitolato. (**Monitoraggio**)*

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 matrice Progetto-Fornitori e Ruoli-Utenze.

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. (ad esempio Produttore e Versioni web server, application server, CMS, DBMS), librerie, firmware, Bollettini Sicurezza, EoL).*

**Preventivamente inserita nel contratto/capitolato*

Linee guida - "La sicurezza nel procurement ICT"

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

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

Al termine di ogni singolo progetto l'amministrazione deve obbligatoriamente eseguire il deprovisioning delle utenze logiche fornitore, accessi fisici, VPN, Regole Firewall.

A10 – Aggiornare l'inventario dei Beni

Inserire l'eventuale hardware/software acquisito nell'inventario dei beni dell'amministrazione, nelle procedure di backup e di monitoraggio.

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.

A12 – Manutenzione e Aggiornamento 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)*

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 (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.

Linee guida - "La sicurezza nel procurement ICT"

Impatto per le amministrazioni

Nella **tabella**, tutte le azioni illustrate nei paragrafi precedenti sono classificate in base all'impatto e alla "**onerosità**" delle stesse per le amministrazioni. (**Impegno e risorse**).

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.

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.

AGID | Agenzia per l'Italia Digitale

GRAZIE PER L'ATTENZIONE