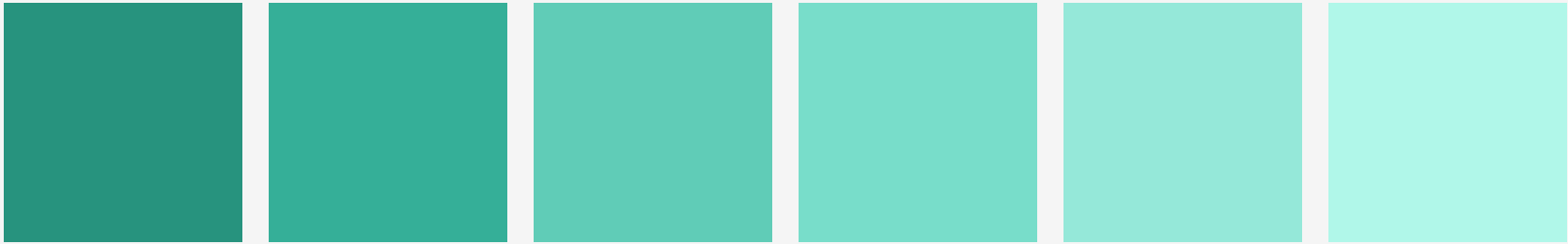
Linee guida sicurezza
PROCUREMENT ICT nella PA

Professore: **Milani Alfredo**

Studenti: **Baldassarrini Matteo**, **Luchini Chiara**



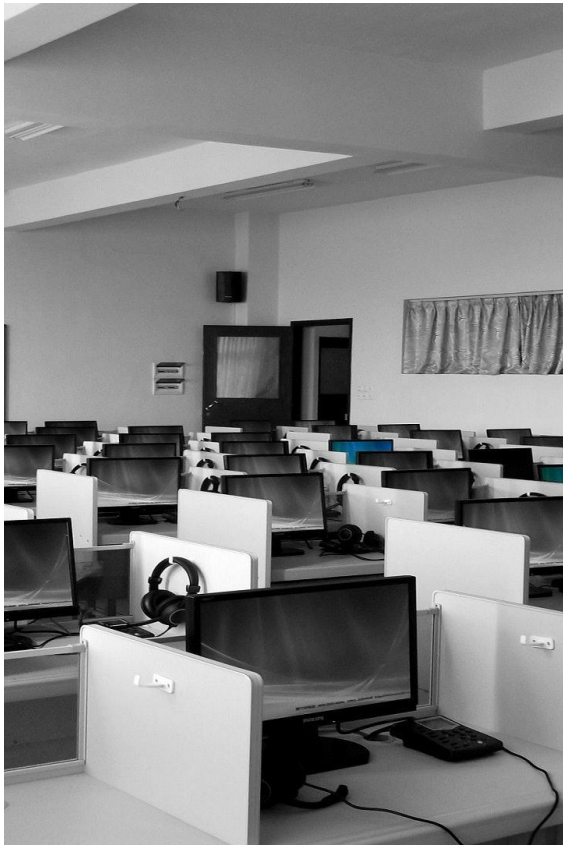
Genesi e Ambito del documento

Il documento che andremo a riassumere rappresenta il prodotto finale di diversi incontri svolti tra **Novembre 2018** e **Febbraio 2019**, promossi dal **Nucleo per la Sicurezza Cibernetica** (NSC) del **Dipartimento Informazioni per la Sicurezza** presso la **Presidenza del Consiglio dei Ministri**.

1. Il documento si concentra sulla sicurezza nell'approvvigionamento di beni e servizi informatici, attività indicata con il termine "**procurement ICT**" e riguarda principalmente i **contratti pubblici ICT**.

2. I contenuti del documenti sono intesi come procedure cui allinearsi anche sulla base dei gradi di criticità delle varie acquisizioni ICT e sono rivolti principalmente ai **dirigenti/funzionari** delle PA, ai **RUP** delle gare pubbliche, ai **responsabili** della **transizione al digitale** ed ai **responsabili dell'organizzazione, pianificazione e sicurezza**.

3. Le finalità del documento sono quelle di mostrare in modo semplice le **problematiche** legate alla sicurezza nel **Procurement ICT** e presentare buone prassi da adottare per verificare il **livello di sicurezza** degli attuali processi di acquisizione ed eventualmente per alzare tale livello senza aumentare la complessità dei processi e l'impegno necessario a condurli.



Procurement ICT

Questi tipi di **contratti** possono essere classificati nel seguente modo:

a) **contratti di sviluppo**, **realizzazione** e **manutenzione evolutiva** di applicazioni informatiche
b) **contratti di acquisizione** di prodotti hardware/software
c) **contratti per attività di operation** e **conduzione**
d) **contratti per servizi** diversi (supporto, consulenze, help desk ecc..)
e) **contratti per forniture miste**, combinazioni delle precedenti tipologie

CHIARA LUCHINI
MATTEO BALDASSARRINI

Indicazioni per le amministrazioni

Le azioni che le pubbliche amministrazioni devono eseguire sono di tipo organizzativo, funzionali e operativo e possono essere suddivise in 3 sotto categorie:

Azioni da svolgere prima della fase di acquisizione

Azioni da svolgere nel corso del procedimento di acquisizione

Azioni da svolgere dopo la stipula del contratto

CHIARA LUCHINI
MATTEO BALDASSARRINI

Azioni da svolgere prima della fase di acquisizione

Prima di attivare un procedimento di acquisizione, le amministrazioni devono aver svolto una serie di **azioni** per “prepararsi” ad effettuare i successivi passi in maniera sicura, minimizzando il rischio di trovarsi in **situazioni inaspettate** dovendo poi improvvisare.

Azioni Generali

Queste attività prendono il nome di **Azioni Generali** (AG) e vengono enumerate da 1 a 7.

La maggior parte di queste azioni sono **prassi** che le amministrazioni dovrebbero aver già svolto per altri obiettivi, risultando anche un modo per **verificare** e **sanare** eventuali carenze per quelle non prese in considerazione.

CHIARA LUCHINI
MATTEO BALDASSARRINI

Azioni Generali

AG1 - Promuovere competenza e consapevolezza

E' necessario che le amministrazioni possano disporre di **competenze aggiornate** in diversi aspetti come Procurement Management, gestione progetti ecc.. attraverso **percorsi didattici** appositi e nel caso non sia disponibile personale interno si può fare ricorso a **società di supporto/consulenza**. Allo stesso modo integrare attività per tutto il personale per avere una maggiore **consapevolezza** sulla **sicurezza nel Procurement ICT**.

AG2 - Raccogliere buone prassi ed esperienze

L'amministrazione deve raccogliere notizie su casi di **successo/insuccesso** riscontrati nelle precedenti acquisizioni, prendendole in considerazione come **prassi di successo** da tenere in conto per un miglioramento continuo di tale processo e allo stesso tempo deve essere in grado di diffondere **avvisi e allarmi** provenienti dagli organismi individuati dal legislatore a presidio della sicurezza cibernetica.

AG3 - Stabilire ruoli e responsabilità

Le amministrazioni devono definire **ruoli e responsabilità** connesse con la **sicurezza del procurement ICT**, identificando profili idonei e assegnando incarichi formali.

Azioni Generali

AG4 - Effettuare una ricognizione dei beni informatici e dei servizi

L'amministrazione deve disporre di un **inventario aggiornato** dei propri **beni informatici** e dei **servizi erogati** in modo tale da facilitare diverse attività come la gestione di Asset. Nel caso in cui non sia disponibile o incompleto si deve effettuare una **ricognizione** dei beni/servizi, e ad ogni elemento catalogato deve essere indicato un **responsabile** in termini di protezione dei requisiti generali di sicurezza.

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

L'amministrazione deve eseguire le attività di **Risk Assessment** e di **Business Impact Analisys** per classificare i beni e i servizi individuati in termini di criticità, rischi, minacce e vulnerabilità. Inoltre questa classificazione deve essere mantenuta aggiornata ripetendo tali procedure nel caso in cui l'amministrazione giudichi obsoleti gli ultimi studi condotti.

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 definendo il processo e le modalità di svolgimento di tali attività. Per le modalità si devono stabilire gli **obiettivi** del processo di audit, la **periodicità** con la quale verranno eseguiti e le **misure** che saranno utilizzate.

Azioni Generali

07

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

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

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)

CHIARA LUCHINI
MATTEO BALDASSARRINI

Azioni da svolgere durante la fase di procurement

Questo tipo di azioni sono dette “**Azioni Procurement**” (AP) e sono quelle che le amministrazioni devono compiere per la gestione della sicurezza **nel corso** del procedimento di acquisizione.

In totale sono **4** e il loro svolgimento dipende dalle caratteristiche della singola acquisizione e in alcuni casi sono alternative tra loro.

Azioni Procurement

AP1 - Analizzare la fornitura e classificarla in base ai 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 verificando su quali beni e servizi avrà **impatto** tale acquisizione e tenendo d'occhio quando necessario, anche **altri criteri** di criticità. (Es: Costo > Soglia ecc..)

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**.

AP3 - Scegliere i requisiti di sicurezza da inserire nel capitolato

Se a seguito dell'azione **AP2**, è stato scelto di procedere tramite **gara**, l'amministrazione deve inserire nel capitolato gli opportuni **requisiti di sicurezza**, differenziando i requisiti che l'offerta del fornitore deve prevedere **obbligatoriamente** da quelli **opzionali**, che determinano eventualmente un premio nel punteggio tecnico.

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.

Ove l'amministrazione affidi lo svolgimento della gara a una **centrale di committenza**, sarà quest'ultima a dover svolgere l'azione **AP4**.

CHIARA LUCHINI
MATTEO BALDASSARRINI

Azioni post stipula contratto

Da svolgere in esecuzione e/o a posteriori

Queste 13 azioni sono di tipo **operativo**, dipendono dalla fornitura e sono connesse con le azioni svolte nelle fasi precedenti per svolgere in modo efficace.

A1- Gestire utenze fornitori

L'amministrazione deve fornire ai dipendenti che ne necessitano delle utenze nominative in accordo con le politiche di sicurezza. Gli accessi potranno essere tracciato e verificati.

A2- Gestire utilizzo dispositivi del fornitore

Consiste nel verificare la conformità dei dispositivi rispetto alle caratteristiche di sicurezza definite come requisiti poiché possono comportare un costo per il fornitore.

A3- Gestire accesso alla rete

L'accesso alla rete locale dell'amministrazione deve essere configurato in modo da consentire l'accesso solo alle risorse necessarie. L'accesso dall'esterno con VPN deve essere consentito solo quando necessario e utilizzando account personali configurati e abilitati.

A4- Gestire l'accesso ai server/database

L'utilizzo dei dati dell'amministrazione deve essere consentito esclusivamente su server/database di sviluppo nei quali sono stati importati i dati necessari per gli scopi del progetto.

CHIARA LUCHINI
MATTEO BALDASSARRINI

Azioni post stipula contratto

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.

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

In forniture di tipo sviluppo applicativo e/o manutenzione evolutiva che sono state classificate critiche, l'amministrazione deve aver definito requisiti in termini di sicurezza. Questi possono essere:

- di tipo generico
- specifiche tecniche puntuali

A7- Monitorare le utenze e gli accessi dei fornitori

L'amministrazione deve mantenere costantemente aggiornata una matrice Progetto-Fornitori e Ruoli-Utenze che aiuti a monitorare e verificare l'impiego di personale con qualifica e formazione adeguata e la corretta rimozione dei permessi delle utenze.

A8- Verificare la documentazione finale di progetto

Alla fine di ogni progetto l'amministrazione deve controllare che il fornitore rilasci:

- documentazione finale e completa del progetto
- manuale di installazione/configurazione
- report degli Assessment di Sicurezza
- "libretto di manutenzione" del prodotto

CHIARA LUCHINI
MATTEO BALDASSARRINI

Azioni post stipula contratto

A9- Effettuare la rimozione (deprovisioning) dei permessi 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.

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;
- inserire l'eventuale software realizzato o acquisito;
- inserire gli oggetti di cui ai punti precedenti nel sistema di backup / disaster recovery e eventualmente un sistema di monitoraggio web/server e servizi;
- verificare che la documentazione e le procedure operative che riguardano la sicurezza vengano aggiornate e comunicate le variazioni.

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 occorre verificare che l'hardware dismesso venga cancellato e distrutto in modo sicuro, evitando che dati critici possano restare erroneamente memorizzati sull'hardware dismesso.

CHIARA LUCHINI
MATTEO BALDASSARRINI

Azioni post stipula contratto

A12 - Manutenzione - aggiornamento dei prodotti

Gli amministratori di sistema devono obbligatoriamente eseguire gli aggiornamenti ogni qualvolta sui siti dei produttori vengono rilasciate patch e correzioni per problemi di vulnerabilità.

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 ma indicativamente si suggerisce di svolgere un assessment almeno annualmente.

La maggior parte delle azioni da svolgere dopo la stipula del contratto sono in relazione con i requisiti di sicurezza che le amministrazioni possono inserire nei propri capitolati di gara, quest'ultimi sono elencati a fine documento.

Impatto delle azioni

La maggior parte delle azioni che vengono considerate a **“basso impatto”** non sono state riportate poiché esse configurano semplici mutamenti organizzativi o strutturazione di processi già presenti. Ciò che interessa sono le azioni a **“ medio impatto”** e ad **“alto impatto”** in quanto esse potrebbero prevedere investimenti sulle risorse interne o coinvolgere risorse esterne all’amministrazione così da avere costi aggiuntivi.

Azione	Livello di impatto	Note
AG1	Medio	Comporta attività di formazione.
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.
AP4	Medio	Può comportare attività di formazione.
A8	Medio	Prevede verifica di documenti, pertanto il livello di impatto dipende dalla complessità di questi ultimi.
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.

CHIARA LUCHINI
MATTEO BALDASSARRINI

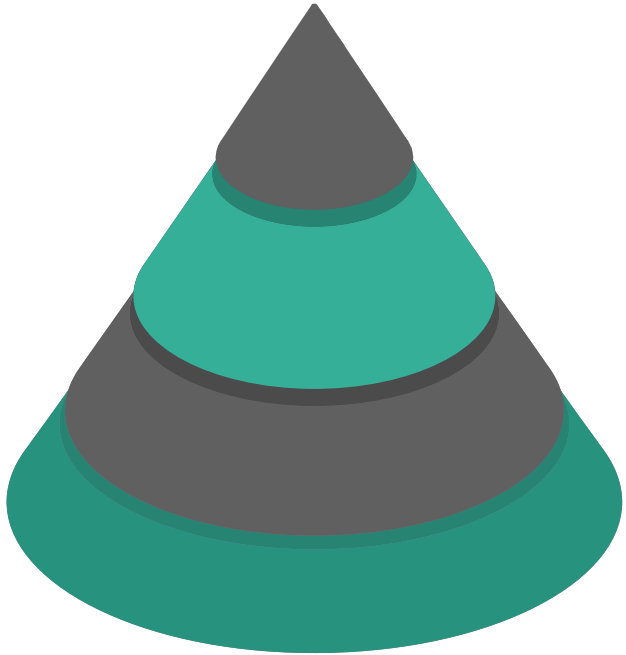
Indicazioni per le centrali di committenza

Le indicazioni elencate nelle slides precedenti si applicano anche alle **centrali di committenza**

Azioni AP2, AP3 e AP4

Sono da ritenersi obbligatorie quando queste svolgono iniziative di **acquisizione ICT** nell'interesse di Ministeri, Enti centrali, Regioni e città metropolitane.

Inoltre si ritiene che le centrali di committenza possono fungere anche da enti attuatori di **miglioramenti** per gli aspetti di sicurezza delle **forniture ICT**.



CHIARA LUCHINI
MATTEO BALDASSARRINI

Protezione dei dati Personali

É 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 **GDPR**.

I principi della protezione dei dati fin dalla progettazione e per impostazione predefinita, 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.

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”

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).*

CHIARA LUCHINI
MATTEO BALDASSARRINI

Grazie per l’attenzione