SAPIENZA
UNIVERSITÀ DI ROMA

Acquisto servizi/applicativi sicuro

SAPIENZA
UNIVERSITÀ DI ROMA

Sommario

ACRONIMI

Acronimi e definizioni	
ABAC	Attribute Based Access Control - Sistema di controllo accessi basato sugli attributi, l'accesso a una risorsa è determinato dal controllo di diversi attributi, o combinazione di essi, assegnati agli utenti.
BC	Business Continuity - processi e procedure eseguite nell'ambito dell'organizzazione per assicurare l'operatività delle funzioni base durante e a seguito di un incidente e governare i diversi aspetti tecnico/amministrativi.
Dati Personali e particolari	"dati personali" sono definiti come qualsiasi informazione riguardante una persona fisica identificata o identificabile; "dati particolari" dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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.
MFA	Multi Factor Authentication -autenticazione a più fattori è quella tecnologia che permette di riconoscere, attraverso più di due metodi di autenticazione, la persona che effettua l'accesso ad un sistema
OWASP	Open Web Application Security Project un progetto open-source che ha l'obiettivo di realizzare linee guida, strumenti e metodologie per lo sviluppo di codice sicuro
PT	Penetration Test – processo operativo eseguito mediante simulazione di attacco per determinare criticità di un sistema.
RBAC	Role Based Access Control - Sistema di controllo accessi basato sui ruoli in cui le entità del sistema che sono identificate e controllate rappresentano posizioni funzionali in una organizzazione o processi.
Sistema	Applicazione/Servizio che deve essere disponibile agli aventi diritto in termini di esercizio e disponibilità dell'informazione.
SSL	Secure Sockets Layer protocollo crittografico delle comunicazioni
TLS	Transport Layer Security protocollo crittografico evoluto
VA	Vulnerability Assessment - processo finalizzato a identificare e classificare i rischi e le vulnerabilità del sistema informatico.

1. Scopo del documento

Il presente documento rappresenta un vademecum di carattere generale per richiedere e verificare la messa in sicurezza di applicativi e servizi acquisiti da fornitori esterni, a garanzia della protezione dei dati personali, per impostazione predefinita nel rispetto del GDPR Regolamento (UE) 2016/679, e della continuità dei servizi.

Sapienza può acquisire i propri servizi da fornitori esterni ed erogarli come soluzioni in **cloud certificati** oppure **on-premises** all'interno della propria infrastruttura ICT.

Si fa riferimento alle indicazioni contenute nelle linee guida per gli acquisti ICT per le Pubbliche Amministrazioni, per la progettazione dei servizi digitali e dei siti della PA, nel rispetto ai principi di accessibilità ed usabilità.

2. Requisiti generali di Ateneo

La sicurezza delle applicazioni è funzionale alla protezione delle informazioni che esse trattano ed alla continuità dei servizi erogati. I dati devono essere accessibili solo agli utenti nel rispetto dei ruoli prefissati e del principio di riservatezza. Devono essere messe in atto misure tecniche e organizzative adeguate a proteggere i dati/servizi da uso, modifica, divulgazione, perdita, distruzione o danno accidentali, accessi non autorizzati o illegali (GDPR Regolamento (UE) 2016/679- Considerando 39, 75, 77, 78, 79, 83, 87; Art. 5, 9, 32).
Per i servizi e software, acquisiti da fornitori esterni a Sapienza, è necessario richiedere e verificare, tramite dichiarazione di conformità, il rispetto di quanto previsto ai punti successivi.

2.1. Protezione degli accessi

L'accesso per scopi amministrativi, e di gestione, alle macchine server su cui sono ospitati gli applicativi, ed agli applicativi stessi, deve essere riservato alle sole utenze autorizzate e preventivamente profilate. L'accesso ai sistemi deve essere permesso previa autenticazione e autorizzazione in base ai ruoli strettamente assegnati.
L'accesso alle informazioni attraverso le funzioni dell'applicativo deve essere garantito agli utenti solo previa autenticazione e secondo le autorizzazioni loro concesse ed esclusivamente per la visibilità ai dati ed alle funzioni permesse dai ruoli assegnati.
Gli accessi da remoto su soluzioni on-premises devono essere garantiti solo attraverso protezione del canale di comunicazione ed autenticazione dell'utenza attraverso connessioni in VPN.

2.2. Pubblicazione informative privacy e conservazione del consenso

Nel caso di servizi che prevedano il trattamento di dati personali, è necessario esporre e conservare le informative sulla privacy, o l'indicazione esplicita del consenso espresso, per la

raccolta e gestione dei dati, personali e particolari, degli interessati e le indicazioni sul trattamento dei dati effettuato dall'applicativo.
Il modello dell'informativa sulla privacy può essere reperito nel sito del Settore Privacy nella sezione "Informative" raggiungibile al link https://www.uniroma1.it/it/pagina/settore-privacy

2.3. Utilizzo di dominio "uniroma1.it" e protezione del canale di comunicazione

Nel caso di pubblicazione di applicazioni web è necessario la registrazione di un dominio "uniroma1.it", di secondo livello o terzo livello secondo le indicazioni date dal CEW (Comitato Editoriale Web) di Sapienza.
La richiesta della registrazione del dominio ed il rilascio del certificato può essere presentata al Centro InfoSapienza o al referente di rete della struttura in caso di dominio terzo livello.
La Pubblica Amministrazione, come indicato dal CAD (Codice Amministrazione Digitale) e dalle linee attuative di AGID (Agenzia per l'Italia digitale), nei propri servizi erogati attraverso la rete, deve utilizzare canali di comunicazione che consentono autenticazione, integrità dei dati e confidenzialità utilizzando il protocollo di comunicazione HTTPS (HTTP over TLS), impostando di default il *redirect* della comunicazione sulla porta 80 (http) verso la porta 443 (HTTPS).

2.4. Utilizzo di versione stabile e aggiornamenti di sicurezza

Il server su cui è ospitato il servizio/applicativo deve avere una versione stabile del sistema operativo, che sia supportata dal produttore, abbia superato i test di qualità e sia considerata affidabile per un utilizzo in produzione.
Installare gli aggiornamenti di sicurezza rilasciati regolarmente per correggere le vulnerabilità del sistema operativo e prevenire gli attacchi informatici.
Per il servizio/applicativo deve essere previsto l'aggiornamento periodico di moduli e librerie che dovrebbe essere programmato e automatizzato, per garantire che sia eseguito in modo regolare e senza interruzioni. Inoltre, è importante verificare che gli aggiornamenti non interferiscano con il funzionamento dell'applicativo e che siano adeguatamente testati prima di essere installati in produzione

2.5. Implementazione e conservazione dei log di sistema ed applicativi

Prevedere le registrazioni degli accessi e delle attività che avvengono all'interno del sistema e che possono essere utilizzate anche per identificare e risolvere eventuali problemi di sicurezza.
Richiedere al fornitore che il servizio/applicazione effettui la registrazione dei log applicativi, le attività che avvengono all'interno dell'applicazione, come le eccezioni e gli errori.

2.6. Conformità ai parametri OWASP e rispetto dei requisiti minimi di sicurezza

Richiedere al fornitore che il servizio/applicazione web sia conforme ai parametri OWASP a garanzia della corrispondenza dell'applicativo servizio ai requisiti minimi di sicurezza applicati da Sapienza. Alcune delle misure di sicurezza raccomandate da OWASP includono ad esempio: autenticazione sicura, autorizzazione limitate alle funzioni e dati nel rispetto dei ruoli attribuiti, input validation, protezione dei dati particolari, aggiornamento continuo, monitoraggio e registrazione degli eventi applicativi.

2.7. Regole per lo sviluppo di siti internet e servizi digitali erogati dalle PA, Accessibilità degli strumenti informatici, Usabilità del servizio digitale

Per servizi/applicativi erogati dalla Sapienza, tramite la rete internet, agli utenti è necessario richiedere al fornitore la corrispondenza del prodotto a quanto previsto nelle linee guida:

- "Linee guida di design per i siti internet e i servizi digitali della PA"
- "Le linee Guida sull'Accessibilità degli strumenti informatici"
- "Usabilità"

Tali linee guida hanno lo scopo di definire e orientare la progettazione e la realizzazione dei servizi digitali erogati dalle Pubbliche Amministrazioni secondo quanto definito dal CAD, nel perseguire gli obiettivi di:

- Accessibilità
  Rendere accessibili a tutti gli utenti il contenuto, la struttura e il comportamento degli strumenti informatici, secondo i requisiti di legge.

- Affidabilità, trasparenza e sicurezza
  Progettare e sviluppare servizi digitali che garantiscano la trasparenza delle informazioni e la sicurezza, nel rispetto della normativa europea e nazionale in materia di protezione dei dati personali.

- Semplicità di consultazione ed esperienza d'uso
  Progettare, realizzare e mantenere siti internet e servizi digitali utili e facili da usare, secondo una metodologia di progettazione centrata sull'utente.

2.8. Standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici

In presenza di servizio/applicativo che debba interagire con altri servizi/applicativi della Sapienza o che richieda transazioni digitali realizzate tra e verso le Pubbliche Amministrazioni è necessario richiedere al fornitore una dichiarazione di aderenza alle linee guida per la

sicurezza dell'interoperabilità tramite API (Application Programming Interface) dei sistemi informatici.
Le Linee Guida contribuiscono alla definizione del modello di interoperabilità delle Pubbliche Amministrazioni (ModI).

3. La sicurezza nel procurement ICT (acquisti ICT)

Utilizzare nelle fasi di scelta ed acquisto delle soluzioni, servizi/applicativi, le procedure indicate nelle linee guida della sicurezza nel procurement ICT per definire ed affrontare:

- la problematica della sicurezza nel procurement ICT;
- mettere a sistema e 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 per verificare il livello di sicurezza dei processi di acquisizione.

3.1. Azioni da svolgere durante la fase di procurement

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.

3.1.1. Analizzare la fornitura e classificarla in base a criteri di sicurezza

In generale, il livello di criticità del livello di sicurezza 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.

3.1.2. Scegliere lo strumento di acquisizione più adeguato, tenendo conto della sicurezza

Determinare lo strumento amministrativo più idoneo per l'acquisto ad esempio Accordo Quadro, Mepa, Bando o Gara.

3.1.3. Scegliere i requisiti di sicurezza da inserire nel capitolato

Ove si sia scelto di procedere tramite gara, si 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.

3.1.4. Garantire competenze di sicurezza nella commissione di valutazione

Nel caso di gara è opportuno tenere conto nella scelta delle commissioni giudicatrici, dell'esigenza che almeno uno dei commissari abbia competenze in tema di sicurezza.

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

3.2.1. 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.

3.2.2. Gestire l'utilizzo di dispositivi di proprietà del fornitore

Le caratteristiche di sicurezza (ad esempio la crittografia dei dati, compliance alle misure minime di sicurezza) che i dispositivi del fornitore (computer, portatili, tablet, ecc.) devono rispettare per accedere alla rete dell'amministrazione devono essere inserite nel capitolato e verificate successivamente all'aggiudicazione e svolgimento del lavoro.

3.2.3. 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 (utilizzo di connessioni VPN per accesso remoto, registrazione dei Log).

3.2.4. 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, nel rispetto di quanto previsto dal trattamento dei dati.

3.2.5. Stipulare accordi di autorizzazione e riservatezza.

L'amministrazione deve stipulare accordi di autorizzazione (clearance) e riservatezza con ogni singolo fornitore prima dell'avvio di ogni progetto. Definire dei Modelli-Standard da applicare per ogni fornitore.

3.2.6. 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)

3.2.7. Monitorare le utenze e gli accessi dei fornitori

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.

3.2.8. Verificare la documentazione finale di progetto

Alla fine di ogni singolo progetto 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).

3.2.9. 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.

3.2.10. 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.

3.2.11. 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"

3.2.12. Vulnerability Assessment

Il centro di spesa, su beni e servizi classificati critici ed esposti sul web, deve richiedere al fornitore una dichiarazione di esecuzione di un Vulnerability Assessment (VA). A seguito dell'acquisizione del servizio è raccomandato eseguire, o richiedere al fornitore, un VA periodico. Come indicazione orientativa, si suggerisce di svolgere assessment a cadenza almeno annuale, e ogni volta che si apportano modifiche alla configurazione software/hardware.

3.3. Trattamento dei dati ed informativa

Sapienza Università di Roma adotta le misure necessarie all'applicazione del Regolamento Europeo 2016/679 GDPR (General Data Protection Regulation) e alla vigente normativa nazionale, relativamente alla protezione delle persone fisiche con riguardo al trattamento dei dati personali per cui nel caso in cui il servizio acquistato faccia una raccolta di dati personali degli utenti e/o contenga dati riservati è necessario far firmare al fornitore i seguenti documenti:

- Atto di nomina del Responsabile del trattamento dei dati
- Accordo di riservatezza.

4. Gestione da remoto del servizio acquisito

Nel caso di gestione da remoto del servizio acquisito, come soluzione on-premises all'interno dell'infrastruttura di Sapienza, è raccomandato l'uso del collegamento in VPN di Ateneo.
Per l'accesso da parte di personale/fornitori non appartenenti all'Ateneo, per consentire l'accesso in sicurezza tramite connessioni VPN, è necessario effettuare preliminarmente la profilazione di questi utenti come indicato nel documento "Rilascio credenziali a consulenti/fornitori per accesso remoto in VPN" reperibile nella sezione "sicurezza informatica" della pagina web del Centro InfoSapienza https://web.uniroma1.it/infosapienza/.

Appendice A – Documentazione di riferimento

Si raccomanda, a tutti coloro che sviluppano codice per la PA, di seguire le raccomandazioni:

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 - GDPR
  - https://www.garanteprivacy.it/regolamentoue
- Modello Informativa Privacy
  - https://www.uniroma1.it/it/pagina/settore-privacy
- "Le linee guida per lo sviluppo del software sicuro nella pubblica amministrazione".
  - https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro
- "Misure minime di sicurezza ICT per le pubbliche amministrazioni".
  - https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict
- "La sicurezza nel procurement ICT".
  - https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/201391021420O__OLG_Sicurezza_Procurement_ICT_versione_finale_pub.pdf
- "Le linee Guida sull'Accessibilità degli strumenti informatici"
  - https://www.agid.gov.it/it/design-servizi/accessibilita
- "Linee guida di design per i siti internet e i servizi digitali della PA"
  - https://www.agid.gov.it/it/design-servizi/linee-guida-design-servizi-digitali-pa
- Usabilità
  - https://www.agid.gov.it/it/design-servizi/usabilita
- Linee Guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici
  - https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_tecnologie_e_standard_sicurezza_interoperabilit_api_sistemi_informatici.pdf
- CAD – Codice dell'Amministrazione Digitale
  - https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82