Università Ca' Foscari Venezia
Dorsoduro 3246, 30123 Venezia
P.IVA 00816350276 - CF 80007720271
www.unive.it

Linee guida sui requisiti di sicurezza informatica per l'acquisto di servizi in cloud e sistemi informatici

Questo documento fornisce indicazioni sui requisiti di sicurezza informatica da inserire nei capitolati per l'acquisto di forniture che prevedano apparati da connettere alla rete dati di Ateneo e/o servizi in cloud. Tali requisiti si rendono necessari al fine di preservare la sicurezza delle informazioni trattate da questi sistemi e sono in linea con quanto previsto dal regolamento sulla "Protezione dei dati personali" emanato con D.R. n. 190 del 22/02/2021.

Nelle sezioni che seguono sono indicati in dettaglio i requisiti da cercare nel caso di acquisto di servizi in cloud o di sistemi informatici, e/o nella definizione della loro manutenzione.

E' importante sottolineare come ad ogni acquisto di sistema informatico sia necessario prevedere una corrispondente manutenzione e, nel caso questa sia svolta da personale esterno all'Ateneo, fare attenzione ai requisiti riportati.

1. Requisiti per l'acquisto dei servizi in cloud

Per "servizi in cloud" si intendono quei servizi informatici che prevedono il trattamento (la trasmissione, elaborazione o conservazione) dei dati dell'Ateneo sui server messi a disposizione da un fornitore. L'accesso ai dati da parte dell'Ateneo può essere manuale (es. tramite sito web consultato dal personale dell'Ateneo) o automatico (es. che comunica direttamente con sistemi informatici di Ateneo). Questa tipologia di servizi viene spesso indicata dalle sigle SaaS (Software as a Service), PaaS (Platform as a Service), e IaaS (Infrastructure as a Service).

Al fine di tutelare i dati dell'Ateneo, è necessario che il fornitore dei servizi in cloud sia stato qualificato dall'Agenzia per la Cybersicurezza Nazionale (ACN) e, quindi, sia presente all'interno dell'elenco dei fornitori qualificati pubblicati in *Marketplace* (consultabile a: https://catalogocloud.acn.gov.it/).

Il livello di qualificazione **minimo** richiesto per i fornitori di servizi in cloud dell'Ateneo è **Q1.**

La deroga a questa prescrizione deve essere dettagliatamente motivata nell'atto di autorizzazione all'acquisto, dando evidenza alle motivazioni che precludono l'individuazione di fornitori o servizi differenti che assicurino il requisito, e le eventuali misure di mitigazione del rischio messe in atto.
Il servizio acquistato dovrà comunque soddisfare i requisiti riportati nella sezione 2 ("Requisiti per l'acquisto di sistemi informatici") del presente documento.

2. Requisiti per l'acquisto di sistemi informatici

Per "sistemi informatici" si intendono tutti quegli strumenti elettronici complessi in grado di interagire con l'ambiente e con gli utenti e/o di raccogliere e inviare dati in formato elettronico.
Sono da considerarsi "sistemi informatici" tutti gli apparati elettronici collegati ad una rete dati (sia essa ethernet, WiFi, GSM, ecc.) ed anche i computer e i sistemi interattivi anche se non collegati ad una rete nonché i sensori autonomi.

Nei capitolati redatti per l'acquisto di sistemi informatici è sempre necessario esplicitare i seguenti requisiti e verificarne il rispetto sia in fase di collaudo che in quella di esercizio.

2.1. Aggiornamento dei sistemi (*patch* di sicurezza informatica)

Il fornitore si impegna a garantire che il sistema, al momento della sua messa in produzione presso l'Ateneo, sia aggiornato al livello di patch sicurezza più recente disponibile sia per quel che riguarda il sistema operativo sia per quel che riguarda le applicazioni installate.

Qualora l'applicazione degli aggiornamenti risulti incompatibile con le funzionalità attive, il fornitore si impegna a documentare la problematica nel dettaglio in modo da permettere mitigazioni temporanee e a pianificare le modifiche necessarie a ripristinare la compatibilità del sistema con gli aggiornamenti di sicurezza.

2.2. Comunicazioni tra sistemi

Le comunicazioni tra i sistemi devono avvenire esclusivamente utilizzando crittografia forte e algoritmi non deprecati, possibilmente attraverso protocolli non proprietari (es.. HTTPS, TLS).

Tutti i servizi (intesi come i programmi) non necessari al buon funzionamento della fornitura devono essere disattivati.

Tutte le interfacce di comunicazione non necessarie al buon funzionamento della fornitura devono essere disattivate.

Il fornitore si impegna a fornire una documentazione completa che descriva puntualmente porte e protocolli necessari per le comunicazioni *inbound* e *outbound* dei vari elementi del sistema connessi alla rete dati. Tale documentazione dovrà anche riportare un elenco di indirizzi IP o nomi DNS per i quali vanno autorizzate le comunicazioni.

2.3. Account e credenziali

I sistemi acquistati devono permettere la modifica delle credenziali di *default*. Le credenziali utilizzabili dovranno soddisfare i requisiti di complessità richiesti per le credenziali di Ateneo al momento dell'installazione del sistema. Qualora limiti tecnici impediscano di raggiungere tale complessità le credenziali utilizzate dovranno essere scelte cercando di soddisfare quanti più requisiti possibile.

2.4. Vulnerabilità

Si chiede che venga indicato un punto di contatto del fornitore al quale possano essere segnalate eventuali criticità e/o presentate richieste in ambito sicurezza informatica. Qualora vengano individuate vulnerabilità sui sistemi informatici, il fornitore si impegna a dare riscontro entro 5 giorni lavorativi dalla segnalazione, applicando tempestivamente una correzione oppure concordando esplicitamente un piano di mitigazione ove la correzione non sia possibile per motivi tecnici o richieda più tempo (in questo caso si dovrà applicare una mitigazione temporanea).

Il fornitore deve rendersi disponibile a supportare il personale autorizzato dall'Ateneo per eseguire analisi di vulnerabilità manuali o automatizzate e *penetration test* sui sistemi forniti, al fine di valutare la reale esposizione ad attacchi informatici.

2.5. Copie di sicurezza (opzionale)

Nell'eventualità in cui i sistemi informatici trattino dati dei quali è richiesta la continua disponibilità è necessario assicurarsi che il fornitore preveda un adeguato sistema di *backup* e *recovery* in grado di ripristinare i dati a fronte di un'eventuale perdita in tempi compatibili con le esigenze dell'Ateneo.

3. Requisiti per i capitolati di manutenzione di sistemi informatici

Per "sistemi informatici" si intendono tutti quegli strumenti elettronici complessi in grado di interagire con l'ambiente e con gli utenti e/o di raccogliere e inviare dati in formato elettronico.
Sono da considerarsi "sistemi informatici" tutti gli apparati elettronici collegati ad una rete dati (sia essa ethernet, WiFi, GSM, ecc.) ed anche i computer e i sistemi interattivi anche se non collegati ad una rete nonché i sensori autonomi.

In tutti i capitolati nei quali viene richiesta la manutenzione di sistemi informatici da parte di personale esterno all'Ateneo, sia essa direttamente collegata all'acquisto dei sistemi, oppure venga acquistata in un secondo momento per sistemi esistenti è sempre necessario esplicitare i seguenti requisiti e verificarne il rispetto sia in fase di collaudo che in quella di esercizio.

3.1. Aggiornamento dei sistemi (*patch* di sicurezza informatica)

Il manutentore si impegna a garantire, per la durata del contratto di manutenzione, l'aggiornamento di tutti gli elementi del sistema con eventuali *patch* che riguardino aspetti di sicurezza informatica. L'applicazione di tali *patch* deve avvenire entro 10 giorni lavorativi dalla loro disponibilità salvo diverso accordo con il RUP dipendente da esigenze dell'Ateneo.

Qualora l'applicazione degli aggiornamenti risulti incompatibile con le funzionalità attive, il fornitore si impegna a documentare la problematica nel dettaglio in modo da permettere mitigazioni temporanee e a pianificare le modifiche necessarie a ripristinare la compatibilità del sistema con gli aggiornamenti di sicurezza.

3.2. Comunicazioni tra sistemi

Le comunicazioni tra i sistemi devono avvenire ove possibile utilizzando crittografia forte e algoritmi non deprecati, possibilmente attraverso protocolli non proprietari (es. HTTPS, TLS).

Tutti i servizi (intesi come i programmi) non necessari al buon funzionamento del sistema devono essere disattivati.

Tutte le interfacce di comunicazione non necessarie al buon funzionamento del sistema devono essere disattivate.

Il manutentore si impegna a tenere aggiornata una documentazione che descriva puntualmente porte e protocolli necessari per le comunicazioni *inbound* e *outbound* dei vari elementi del sistema connessi alla rete dati. Tale documentazione dovrà anche riportare un elenco di indirizzi IP o nomi DNS per i quali vanno autorizzate le comunicazioni.

3.3. Account e credenziali

Eventuali credenziali di *default* preimpostate sui sistemi informatici devono essere immediatamente cambiate con credenziali dedicate.
Le credenziali utilizzate dovranno soddisfare i requisiti di complessità richiesti per le credenziali di

Ateneo al momento dell'installazione del sistema. Qualora limiti tecnici impediscano di raggiungere tale complessità le credenziali utilizzate dovranno essere scelte cercando di soddisfare quanti più requisiti possibile.

Ove possibile gli account di *default* devono essere disabilitati e sostituiti con account dedicati.

Ove possibile vanno abilitati sistemi di limitazione dei tentativi di accesso (es. *fail2ban*) al fine di prevenire gli attacchi *brute force*.

3.4. Vulnerabilità

Si chiede che venga indicato un punto di contatto del manutentore al quale possano essere segnalate eventuali criticità e/o presentate richieste in ambito sicurezza informatica. Qualora vengano individuate vulnerabilità sui sistemi informatici, il manutentore si impegna a dare riscontro entro 2 giorni lavorativi dalla segnalazione, applicando tempestivamente una correzione oppure concordando esplicitamente un piano di mitigazione ove la correzione non sia possibile per motivi tecnici o richieda più tempo (in questo caso si dovrà applicare una mitigazione temporanea).

Il manutentore deve rendersi disponibile a supportare il personale autorizzato dall'Ateneo per eseguire analisi di vulnerabilità manuali o automatizzate e *penetration test* sui sistemi forniti, al fine di valutare la reale esposizione ad attacchi informatici.

3.5. Copie di sicurezza (opzionale)

Nell'eventualità in cui i sistemi informatici trattino dati dei quali è richiesta la continua disponibilità è necessario assicurarsi che il manutentore preveda un adeguato sistema di *backup* e *recovery* in grado di ripristinare i dati a fronte di un'eventuale perdita in tempi compatibili con le esigenze dell'Ateneo.

4. Requisiti in caso di trattamento di dati personali

Nel caso in cui vengano acquistati servizi in cloud ovvero servizi informatici che trattano dati personali, oltre ad assicurare il rispetto di tutti i requisiti indicati nei paragrafi che precedono nel presente documento, sarà necessario prendere contatto con il DPO o lo Staff di supporto al DPO scrivendo al dpo@unive.it per considerare gli aspetti contrattuali e organizzativi relativi al trattamento dei dati personali.