INFORMAZIONI SUL QUESTIONARIO	
Versione del Questionario	*1.1 (Gennaio 2025)*
Obiettivo del Questionario	*Obiettivo del questionario è valutare il livello di sicurezza informatica del fornitore sulla base dei controlli essenziali di CyberSecurity, correlati al Framework nazionale per la Cybersecurity e al Cybersecurity Framework del NIST, predisposti dal CIS Sapienza. Per ogni informazione utile sui controlli riportati nel questionario è possibile visitare la documentazione informativa al seguente Link: https://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf*

ANAGRAFICA

Campo	Linee guida di Compilazione	Risposta
Fornitore	*Inserire la ragione sociale del fornitore cui si riferisce il questionario*	
Partita IVA Fornitore	*Inserire la Partita IVA del fornitore cui si riferisce il questionario*	
Responsabile Compilazione	*Inserire il nominativo della persona incaricata della compilazione del questionario*	
Data Compilazione	*Inserire la data di compilazione del questionario*	
Descrizione servizio erogato	*Inserire una breve descrizione del servizio erogato (es. consulenza, sviluppo software, application maintenance, ecc.)*	
Gestione e/o trattamento di dati personali	*Specificare se il fornitore gestisce o tratta dati personali in ambito GDPR per conto del Gruppo*	

VALUTAZIONE LIVELLO DI SICUREZZA

Ambito Controllo	Controlli di Sicurezza	Linee Guida Compilazione	Risposta	Descrizione Risposta
Asset Management (ID.AM)	1. Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Asset Management (ID.AM)	2. I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc. . .) offerti da terze parti a cui si è registrati sono quelli strettamente necessari?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Asset Management (ID.AM)	3. Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Asset Management (ID.AM)	4. È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Governance (ID.GV)	5. Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di cybersecurity che risultino applicabili per l'azienda?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Security Continuous Monitoring (DE.CM)	6. Tutti i dispositivi che lo consentono sono dotati di software di protezione (antivirus, antimalware, ecc...) regolarmente aggiornato?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Identity Management, Authentication and Access Control (PR.AC)	7. Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal provider del servizio (es. autenticazione a due fattori)?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Identity Management, Authentication and Access Control (PR.AC)	8. Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Identity Management, Authentication and Access Control (PR.AC)	9. Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Awareness and Training (PR.AT)	10. Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali (es. riconoscere allegati e-mail, utilizzare solo software autorizzato, . . .). I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Protezione dei Dati (PR.IP)	11. La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Information Protection Processes and Procedures (PR.IP)	12. Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda (identificati al controllo 3). I backup sono conservati in modo sicuro e verificati periodicamente?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Protective Technology (PR.PT)	13. Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (es: Firewall e altri dispositivi/software anti-intrusione)?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Mitigation (RS.MI)	14. In caso di incidente (es. venga rilevato un attacco o un malware) vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		
Mitigation (RS.MI)	15. Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi?	*Specificare le modalità di copertura del controllo ed allegare eventuali evidenze a supporto (es.procedure o policy aziendali, ecc.)*		