INFORMAZIONI SUL QUESTIONARIO	
Versione del Questionario	*1.2 (Gennaio 2025)*
Obiettivo del Questionario	*Obiettivo del questionario è valutare le caratteristiche di sicurezza informatica delle applicazioni erogate da terze parti al fine di identificare rischi e vulnerabilità da indirizzare tramite l'implementazione di specifiche contromisure.* *Gli ambiti di controllo sono correlati al Framework nazionale per la Cybersecurity e al Cybersecurity Framework del NIST.*

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*	
Nome Applicazione	*Inserire il nome dell'applicazione*	
Descrizione applicazione	*Descrivere brevemente le funzionalità dell'applicazione*	
Descrizione architettura tecnica	*Descrivere brevemente l'architettura e soluzione tecnica prevista*	
URL applicazione	*Specificare URL di accesso all'applicativo*	
Produttore Applicazione	*Specificare il produttore dell'applicazione*	

VALUTAZIONE LIVELLO DI SICUREZZA

Ambito Controllo	Controlli di Sicurezza	Linee Guida Compilazione	Risposta	Descrizione Risposta
Identity Management, Authentication and Access Control (PR.AC)	1. L'applicazione prevede l'autenticazione di utenti e la relativa profilazione?	*Specificare Tipi di utenti (Clienti/Partner/Interni/Pubblici) e Numero di utenti (<50, 50-100, ecc)*		
Identity Management, Authentication and Access Control (PR.AC)	2. Quali sono le modalità di autenticazione?	*Specificare le modalità di autenticazione (SSO con AD, standard, anonimo, strong authentication, ecc.)*		
Identity Management, Authentication and Access Control (PR.AC)	3. Esiste una Password Policy a protezione delle credenziali?	*Specificare le regole di complessità, scadenza e ogni altro meccanismo di sicurezza utile a proteggere la confidenzialità delle credenziali*		
Identity Management, Authentication and Access Control (PR.AC)	4. E' prevista la gestione di profili applicativi?	*Specificare le tipologie di profili / ruoli previsti (es. amministratore, utente base, utente avanzato, ecc.)*		
Protective Technology (PR.PT)	5. L'applicativo è esposto su internet?	*Specificare le modalità di esposizione (es.esposta su reti pubbliche, reti private, VPN site to site, ecc.)*		
Protective Technology (PR.PT)	6. I flussi di comunicazione sono protetti da misure di sicurezza?	*Specificare i protocolli utilizzati (es. https, ecc.)*		
Protective Technology (PR.PT)	7. Il servizio è erogato esclusivamente tramite macchine on premises (non viene quindi erogato tramite cloud computing pubblico o privato)?	*Specificare quale tipo di cloud computing è utlizzato (se pubblico o privato) ed il relativo cloud provider (es. Google, Amazon, ecc.)*		
Protective Technology (PR.PT)	8. E' richiesto lo scambio di dati con l'esterno (invio e/o ricezione), ivi incluse eventuali integrazioni con altre applicazioni?	*Indicare le modalità di scambio dati prevista (es. upload https, sftp, batch, ecc.) e/o le modalità di integrazione utilizzate (web services, connettori jdbc, batch, ecc.)*		
Information Protection Processes and Procedures (PR.IP)	9. L'applicativo è supportato dal produttore tramite il rilascio di patch di sicurezza che vadano a coprire le vulnerabilità del sistema?	*Indicare se l'applicativo è ancora supportato dal produttore e l'eventuale data di End of Life (EOL)*		
Information Protection Processes and Procedures (PR.IP)	10. Sono previste specifiche misure di sicurezza applicative?	*Specificare le misure di sicurezza (o controlli compensativi) implementate volte ad assicurare l'adeguata protezione dei dati*		
Information Protection Processes and Procedures (PR.IP)	11. Sono previste specifiche misure di sicurezza infrastrutturale?	*Specificare le misure di sicurezza (o controlli compensativi) implementate volte ad assicurare l'adeguata protezione dei dati*		
Information Protection Processes and Procedures (PR.IP)	12. Viene eseguita una attività di rilevazione periodica delle vulnerabilità (Vulnerability Assessment, Penetration Test e Source Code Review)?	*Specificare il perimetro di verifica, le attività eseguite e la periodicità*		
Information Protection Processes and Procedures (PR.IP)	13. L'applicazione si basa su un software di mercato (per cui non sono previsti sviluppi custom di web application o componenti della stessa)?	*Specificare le attività di sviluppo applicabili*		
Information Protection Processes and Procedures (PR.IP)	14. L'applicazione è sviluppata secondo le regole standard di sviluppo sicuro (es. OWASP)?	*Descrivere le regole di sviluppo sicuro utilizzate*		
Information Protection Processes and Procedures (PR.IP)	15. Sono previsti ambienti di sviluppo o test oltre all'ambiente di produzione?	*Specificare quanti e quali ambienti sono stati predisposti e le eventuali misure di sicurezza adottate sui dati degli ambienti inferiori alla produzione (es. data masking)*		
Information Protection Processes and Procedures (PR.IP)	16. L'applicativo è soggetto a normative o adempimenti di legge (es. antiriciclaggio, ecc.)?	*Specificare le normative cui è soggetto l'applicativo ed i relativi obblighi*		
Information Protection Processes and Procedures (PR.IP)	17. L'applicativo registra log delle attività svolte dagli utenti?	*Specificare quali tipologie di azioni sono loggate (es. login, logout, failed login) e l'eventuale integrazione con strumenti SIEM*		
Information Protection Processes and Procedures (PR.IP)	18. E' previsto un piano di continuità operativa e di disaster recovery, che prevede l'implementazione di soluzioni per tutelare l'erogazione del servizio in caso di eventi disastrosi?	*Descrivere il DRP e i valori previsti di RTO e RPO* *Condividere i documenti di BCP e DRP aziendali*		
Information Protection Processes and Procedures (PR.IP)	19. Sono previste delle procedure di backup dei dati?	*Indicare la tipologia di backup utilizzata (nastro, cloud, storage on-site) e frequenza (giornaliera, settimanale, mensile, ecc.)*		
Governance (ID.GV)	20. Il servizio offerto è certificato secondo uno schema di certificazione di sicurezza esistente (es. ISO27001,…)?	*Specificare lo schema di certificazione adottato*		
Data Management (DP-ID.DM)	21. L'applicativo prevede la gestione di dati personali esclusivamente all'interno dell'unione europea?	*Specificare se l'applicativo che gestisce dati personali è in hosting o trasferisce dati al di fuori dell'Unione Europea (ivi inclusa UK a seguito della brexit)*		
Data Management (DP-ID.DM)	22. L'applicativo gestisce esclusivamente dati personali e/o di business comuni (non è quindi previsto il trattamento di dati particolari / ex sensibili e/o dati commercialmente sensibili)?	*Dettagliare le tipologie di dati personali trattate dall'applicativo*		
Data Management (DP-ID.DM)	23. Viene adottato un sistema di cifratura dei dati archiviati?	*Specificare l'ambito e la modalità di applicazione*		
Data Management (DP-ID.DM)	24. Viene adottato un sistema di anonimizzazione dei dati archiviati?	*Specificare l'ambito e la modalità di applicazione*		
Data Management (DP-ID.DM)	25. E' prevista la segregazione dei dati dei clienti?	*Specifiche le misure di sicurezza implementate volte ad assicurare un'adeguata separazione degli storage e dei dati dei differenti clienti*		