ALLEGATO SECURITY

CONTRATTO N. REP. _____

1. SCOPO E OGGETTO DEL DOCUMENTO 2
2. OBBLIGHI E ISTRUZIONI PER IL FORNITORE 2
I. OBBLIGHI GENERALI 4
I.1 Governance della sicurezza 4
I.2 Inventario dei dispositivi e dei software autorizzati e non autorizzati 4
I.3 Proteggere le configurazioni hardware e software sui dispositivi mobili, laptop, workstation e server- e-mail & Web Browser Protection 4
I.4 Valutazione e correzione continua delle vulnerabilità 5
I.5 Identity and Access Management 5
I.6 Gestione, monitoraggio e analisi dei Log di attività 6
I.7 Difese contro i Malware 6
I.8 Copie di sicurezza 7
I.9 Configurazione sicura dei dispositivi di rete come firewall, router e switch 7
I.10 Difese perimetrali 7
I.11 Sicurezza Fisica e Ambientale 7
I.12 Protezione dei dati 7
I.13 Application Software Security 8
I.14 Incident Response and Management 8
I.15 Business Continuity & Disaster Recovery 8

1. SCOPO E OGGETTO DEL DOCUMENTO

Il presente documento ("*Allegato Security*") intende disciplinare gli obblighi e le istruzioni che il Fornitore è tenuto ad osservare per garantire la sicurezza dei servizi, dei sistemi e delle informazioni nell'ambito dell'erogazione della fornitura per Sogei, nonché la compliance alla normativa vigente di riferimento in materia di cybersecurity.

Il presente Allegato Security ivi inclusi gli eventuali allegati, costituisce parte integrante e sostanziale del *Contratto* tra *Sogei* e il *Fornitore*.

2. OBBLIGHI E ISTRUZIONI PER IL FORNITORE

Il Fornitore si impegna ad erogare i servizi previsti nel Contratto alla Sogei esclusivamente in conformità alle istruzioni previste nel Contratto e nel presente *Allegato Security* e alle ulteriori istruzioni che potranno essere eventualmente impartite da Sogei, nel rispetto degli obblighi ivi previsti e delle Norme in materia di Cybersecurity.

Al fine di conformarsi alle disposizioni della Determinazione AgID 628/2021 con particolare riferimento ai requisiti dell'Allegato A2 alla Determinazione ACN 307/2022, il fornitore è tenuto laddove pertinente, in relazione alle misure di sicurezza di cui all'Allegato A alla Determinazione n. 628/2021 e all'Allegato A2 alla Determinazione ACN 307/2022, a supportare Sogei e le Amministrazioni clienti nella fase di adozione di tali misure, ponendo in essere le condizioni per il loro recepimento.

- **Perimetro di Sicurezza Nazionale Cibernetica**

Al fine di conformarsi alle disposizioni del Decreto-legge n. 105 del 2019 e ss.mm.ii. e successivi decreti attuativi, qualora i servizi previsti nel contratto rientrino nella tipologia di beni e servizi inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC) per Sogei e le Amministrazioni Clienti, il Fornitore è tenuto a:

- farsi carico degli oneri derivanti dal supporto necessario che dovrà garantire a Sogei e alle Amministrazioni identificate quali Soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica, durante l'effettuazione delle verifiche preliminari e condizioni e test hardware e software laddove previste dal CVCN o dai CV o dai LAP sui prodotti/servizi oggetto di convenzione e rientranti fra le categorie individuate dal DPCM del 15 giugno 2021 e successivi aggiornamenti intervenuti dopo la pubblicazione della gara. Nel caso di attivazione di suddette verifiche e/o condizioni, qualora il fornitore venisse coinvolto nello svolgimento delle attività, i relativi costi devono essere considerati a carico del fornitore stesso limitatamente agli ambiti di specifica competenza;
- laddove pertinente, in relazione alle misure di sicurezza di cui all'Appendice 1, Allegato B del DPCM n. 81/2021 di attuazione del Perimetro di Sicurezza Nazionale Cibernetica e al corrispondente ambito di cui all'articolo 1, comma 3, lettera b), n. 8) del Decreto-legge n. 105/2019, relative ai sopra indicati beni e i servizi connessi all'oggetto di affidamento, a supportare Sogei e le Amministrazioni clienti nella fase di adozione di tali misure, ponendo in essere le condizioni per il loro recepimento.

- **Soluzioni di tipo Cloud**

In caso di forniture di servizi cloud, il Fornitore è tenuto a conformarsi alle disposizioni riportate in:

  - Circolari dell'Agenzia per l'Italia Digitale (AgID) n. 2 e 3 del 9 aprile 2018 (GU n. 92 del 20/4/2018), come disciplinato dalla nuova procedura di qualificazione dettata dal Decreto direttoriale dell'ACN, protocollo n. 29 del 02/01/2023;
  - Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione" adottato da AGID con Determinazione 628/2021, con particolare riferimento agli articoli 8,11,12 e 13 nonché al suo Allegato B;
  - Determinazione ACN 307/2022, nonché agli Allegati B2 e C, con particolare riferimento alla necessità di possedere il livello di qualificazione del servizio cloud oggetto di fornitura coerente con il livello di classificazione del servizio (ordinario, critico, strategico);
  - Disposizioni delle Determinazioni dell'ACN riferibili alla qualificazione dei servizi cloud per la Pubblica Amministrazione emanate all'interno del Decreto direttoriale dell'ACN, protocollo n. 29 del 02/01/2023.

In ogni caso, il Fornitore si rende disponibile a sottoporsi a valutazioni (audit, assessment, self-assessment) da parte di Sogei e/o a fornire eventuali report emessi da Auditor di terza parte nell'ambito di Certificazioni e Attestazioni in materia di Cybersecurity, IT Security o IT Governance. Sogei informerà il fornitore delle suddette attività con un congruo preavviso.

Nell'ambito delle valutazioni di cui sopra, il Fornitore si impegna a fornire tutta la documentazione necessaria senza indebito ritardo per consentire a Sogei di formulare una valutazione completa nell'ambito delle sue attività di Audit in materia di Cybersecurity. Sogei informerà il fornitore della necessità di trasmettere tale documentazione con un congruo preavviso.

Le prescrizioni del presente *Allegato Security* possono essere integrate e derogate solo sulla base di ulteriori e specifici atti di istruzione di Sogei.

Ove il fornitore rilevi la sua impossibilità nel rispettare le condizioni disciplinate nel presente allegato, deve avvertire immediatamente la Sogei ed attuare tutte le possibili misure al fine di garantire la sicurezza nell'erogazione dei servizi concordando con la Sogei stessa le azioni da intraprendere e/o l'adozione di ulteriori misure di sicurezza.

Nel caso in cui si dovesse manifestare un incidente di sicurezza quale conseguenza del venire meno delle condizioni ivi prescritte, ovvero a seguito di non conformità riscontrate durante gli audit, ferma restando l'applicazione delle penali contrattualmente previste, Sogei, senza bisogno di assegnare alcun termine per l'adempimento, potrà risolvere il contratto, previa dichiarazione da comunicarsi all'Impresa tramite pec.

Qualora la non conformità fosse imputabile a cause di forza maggiore, trovano applicazione le previsioni dell'art. "Forza maggiore"

Si specifica che, nei casi in cui il Fornitore:

- corrisponda ad un Raggruppamento temporaneo di imprese (RTI), il presente Allegato Security si applica nei confronti di tutti i componenti del RTI;

- ricorra a un Sub Fornitori, è sua responsabilità garantire che questi ultimi adottino tutte le istruzioni previste nel Contratto e nel presente Allegato Security, nonché eventuali ulteriori e specifici atti di istruzione di Sogei.

I. OBBLIGHI GENERALI

I.1 Governance della sicurezza

I.1.1 Il Fornitore adotta al proprio interno politiche e procedure di sicurezza applicabili ai processi e alle attività svolte dallo stesso, ivi comprese le attività riguardanti la gestione dei dati e dei servizi erogati per Sogei.

I.1.2 Il personale del Fornitore deve essere formato sulle politiche di sicurezza e deve essere informato in presenza di sostanziali modifiche.

I.1.3 Il Fornitore si impegna a fornire, a cadenza annuale, report sulla propria postura di sicurezza e/o sui risultati delle analisi circa il proprio rischio cyber.

I.2 Inventario dei dispositivi e dei software autorizzati e non autorizzati

I.2.1 Il Fornitore:

- adotta al proprio interno politiche e procedure per il governo delle attività di installazione del software dagli utenti sui dispositivi utilizzati per l'erogazione dei servizi previsti nel Contratto;
- monitora la compliance alle suddette politiche e procedure.

I.2.2 Il Fornitore sviluppa, implementa e gestisce un Asset Inventory dei software e dei sistemi utilizzati per l'erogazione dei servizi previsti nel Contratto.

I.2.3 Tutti i software e i sistemi applicativi utilizzati dal Fornitore per l'erogazione dei servizi previsti nel Contratto sono eseguiti utilizzando ambienti operativi installati su hardware protetti che utilizzano supporti di memoria di tipologia read-only.

I.3 Proteggere le configurazioni hardware e software sui dispositivi mobili, laptop, workstation e server-e-mail & Web Browser Protection

I.3.1 Il Fornitore adotta al proprio interno politiche e procedure per le attività di change management da effettuare sui sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto.

I.3.2 Il Fornitore:

- documenta ogni change applicato ai sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto;
- mantiene traccia (ad esempio mediante attività di raccolta dei log) delle suddette operazioni di change.

I.3.3 Il Fornitore:

- definisce, documenta e implementa le configurazioni per ogni tipologia di hardware e software a supporto dell'erogazione dei servizi previsti nel Contratto, con l'obiettivo di aumentare la sicurezza delle informazioni gestite mediante il loro uso;
- identifica, documenta ed approva ogni change da applicare alle configurazioni dei sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto, valutandone gli impatti di sicurezza.

I.3.4 Il Fornitore procede all'inibizione dell'utilizzo di tutte le funzionalità sia software sia hardware non necessarie all'operatività.

I.3.5 Il Fornitore per garantire la sicurezza dei sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto (sia nelle componenti hardware sia nelle componenti software):

- identifica e corregge le vulnerabilità riscontrate sui suddetti sistemi;
- effettua test agli aggiornamenti software e firmware necessari alla risoluzione delle vulnerabilità analizzandone eventuali side effects causati dall'installazione.

I.3.6 Il Fornitore inibisce l'utilizzo e l'installazione di software non customizzati o modificati da eventuali provider sui sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto.

I.3.7 Qualora il Fornitore utilizzi sistemi informativi o dispositivi (ad esempio PC) di proprietà di Sogei, questo garantisce il rispetto delle policy, delle linee guida e delle istruzioni in materia definite da Sogei, nonché l'utilizzo di questi esclusivamente per l'erogazione dei servizi previsti nel Contratto.

I.4 Valutazione e correzione continua delle vulnerabilità

I.4.1 Il Fornitore:

- effettua attività periodiche di vulnerability assessment sui sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto e nel caso in cui siano identificate nuove vulnerabilità provvede a censirle;
- pianifica gli interventi di rimedio da attuare per la risoluzione delle vulnerabilità individuate.

Sogei ha la facoltà di richiedere al Fornitore, con un congruo preavviso, la condivisione dei piani di vulnerability assessment e dei risultati ottenuti dopo la loro esecuzione. Sogei ha la facoltà di analizzare i suddetti piani e risultati e di richiedere, con congruo preavviso, eventuali approfondimenti.

I.4.2 Il Fornitore effettua il monitoraggio continuo dei sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto al fine di identificare eventi di sicurezza, accesso e connessioni locali o remote alla rete non autorizzati.

I.4.3 Il Fornitore:

- adotta al proprio interno politiche e procedura per la gestione delle attività di patching;
- documenta le azioni intraprese a fronte dell'individuazione di vulnerabilità, esplicitando i casi in cui non si è ritenuto opportuno, a fronte di un'analisi del rischio, applicare le dovute correzioni sui sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto.

I.4.4 Il Fornitore monitora la pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi e nelle infrastrutture utilizzate per erogare i servizi previsti nel Contratto.

I.4.5 Il Fornitore utilizza sistemi di identificazione di change non autorizzati che potrebbero introdurre vulnerabilità all'interno dei sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto.

I.5 Identity and Access Management

I.5.1 Il Fornitore adotta al proprio interno politiche e procedure di Access Management che descrivano le attività di gestione delle utenze che accedono ai sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto, nonché per l'utilizzo e la gestione di password efficaci.

I.5.2 Il Fornitore per ogni sistema utilizzato per l'erogazione dei servizi previsti nel Contratto:

- identifica le figure, i ruoli e le responsabilità di tipo amministrativo;
- assegna alle solo utenze identificate i privilegi amministrativi.

I.5.3 Il Fornitore gestisce i sistemi di autenticazione per l'accesso ai sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto in maniera tale da:

- assegnare i ruoli e le responsabilità in modo puntuale ad ogni utenza, nel rispetto dei principi del need to know e del least privilege;
- inibire il riutilizzo di utenze già assegnate in precedenza;
- disabilitare le utenze inutilizzate o inattive.

I.5.4 Il Fornitore adotta al proprio interno politiche e procedure che definiscano i principi e le modalità per accedere da remoto ai sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto.

I.6 Gestione, monitoraggio e analisi dei Log di attività

I.6.1 Il Fornitore, in accordo con le policy di Sogei, definisce per ogni tipologia di sistema informativo utilizzato per l'erogazione dei servizi previsti nel Contratto le informazioni da raccogliere mediante attività di log, nonché le misure di sicurezza per proteggere questi ultimi da accessi non autorizzati, modifica e cancellazione accidentali.

I.6.2 Il Fornitore adotta al proprio interno sistemi che consentono di inviare alert e generare report relativi all'accadimento di specifici eventi di sicurezza.

I.6.3 Il Fornitore implementa audit trail per collegare l'accesso ai componenti di sistema utilizzati per l'erogazione dei servizi previsti nel Contratto, a ogni singolo utente e conservarne la cronologia per almeno un anno, con un minimo di tre mesi di disponibilità immediata per l'analisi (ad esempio, online, archiviazione o recuperabile da backup).

I.6.4 Il Fornitore dispone di un sistema in grado di consentire lo storage sicuro di tutte le informazioni di log.

I.6.5 Il Fornitore dispone di un sistema in grado di consentire l'analisi sistematica di tutti i log raccolti sui sistemi utilizzati per l'erogazione dei servizi previsti nel Contratto al fine di identificare eventuali irregolarità.

I.7 Difese contro i Malware

I.7.1 I sistemi utilizzati per l'erogazione dei servizi previsti nel Contratto sono implementati su domini separati del Fornitore per evitare, nel caso di attacco malware, la diffusione del codice malevolo.

I.7.2 Con riferimento ai sistemi utilizzati per l'erogazione dei servizi previsti nel Contratto, il Fornitore:

- dispone di meccanismi di protezione anti-malware;
- effettua continue attività di aggiornamento dei software anti-malware installati al rilascio di nuove versioni software e di nuove firme antivirus;
- effettua scan periodici e scansioni real-time dei file critici;
- individua e blocca codice malevolo, inserendolo in appositi ambienti di quarantena e detonazione, e fornendo, laddove richiesto, alert a Sogei.

I.7.3 Lo scambio di posta elettronica convenzionale con il Fornitore deve avvenire su un canale cifrato in TLS 1.2 o superiore, e per il dominio di posta elettronica del Fornitore devono essere implementati i protocolli SPF, DKIM e DMARC che certificano l'autenticità del dominio mittente. Inoltre, il sistema di posta elettronica convenzionale del Fornitore deve essere protetto dalle minacce che si diffondono tramite posta elettronica, in particolare devono essere implementati controlli anti-spoofing e anti-phishing, e controlli anti-virus sia sulle email in ingresso che in uscita dal sistema di posta elettronica del Fornitore.

I.8 Copie di sicurezza

I.8.1 Il Fornitore adotta al proprio interno politiche e procedure per l'esecuzione dei backup sui sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto, nonché per proteggere le relative copie.

I.8.2 A valle dell'occorrere di incidenti di sicurezza gravi, il Fornitore garantisce il ripristino dell'operatività dei sistemi utilizzati per l'erogazione dei servizi previsti nel Contratto e delle relative delle informazioni utilizzando i backup effettuati.

I.8.3 Il Fornitore:

- effettua lo storage dei backup, delle informazioni critiche, delle configurazioni (impiegate per l'erogazione dei servizi previsti nel Contratto) in ambienti dedicati e segregati fisicamente;
- protegge le informazioni fino alla loro distruzione mediante tecniche e procedure definite.

I.8.4 Le copie di backup delle informazioni effettuate dal Fornitore in virtù delle attività previste nel Contratto sono periodicamente sottoposte a test che ne verifichino la disponibilità, l'integrità e la riservatezza.

I.9 Configurazione sicura dei dispositivi di rete come firewall, router e switch

I.9.1 Il Fornitore adotta al proprio interno politiche e procedure per l'utilizzo e la configurazione dei dispositivi di sicurezza perimetrale (ad esempio firewall, router, switch) implementati per proteggere i sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto.

I.9.2 Il Fornitore, in accordo con Sogei, definisce le modalità di connessione e di trasmissione dei dati tra i sistemi utilizzati per l'erogazione dei servizi previsti nel Contratto.

I.10 Difese perimetrali

I.10.1 Il Fornitore, sulla base di policy in ambito adottate da Sogei, definisce e manutiene le modalità di connessione sicura ai sistemi informativi e alla rete adoperati per l'erogazione dei servizi previsti nel Contratto e autorizza le sole connessioni che rispettano le regole definite.

I**.10.2** Il Fornitore dispone di un sistema che effettua il monitoraggio e il controllo dei device perimetrali dell'infrastruttura, implementa sub-network in grado di rendere accessibili le informazioni dall'esterno in maniera sicura e permette di interfacciare i sistemi informativi interni verso l'esterno soltanto mediante l'utilizzo di interfacce correttamente configurate.

I.10.3 Il Fornitore definisce i termini e le condizioni che consentono l'accesso da e verso l'esterno ai sistemi informativi utilizzati per l'erogazione dei servizi previsti nel Contratto e che regolamentano la trasmissione sicura delle informazioni tra i sistemi stessi.

I.11 Sicurezza Fisica e Ambientale

1.11.1 Il Fornitore, qualora debba accedere alle sedi operative e/o tecnologiche di Sogei, si attiene alle politiche, linee guida e istruzioni adottate da Sogei in materia di sicurezza fisica e ambientale.

I.12 Protezione dei dati

I.12.1 Il Fornitore adotta politiche e procedure, conformi a quelle definite da Sogei, volte a garantire la riservatezza, l'integrità e la disponibilità delle informazioni e dati trattati nell'ambito dell'erogazione dei servizi previsti nel Contratto. Tra le suddette politiche e procedure rientrano, a titolo esemplificativo ma non esaustivo, classificazione delle informazioni e dei documenti, clean desk & clear screen, etc.

I.12.2 Il Fornitore adotta al proprio interno politiche e procedure relative all'utilizzo di controlli crittografici per la protezione delle informazioni che sono trattate nell'ambito dell'erogazione dei servizi

previsti nel Contratto, che comprendano tutte le fasi del ciclo di vita e le modalità di gestione delle chiavi crittografiche.

I.12.3 Il Fornitore adotta al proprio interno politiche e procedure per la gestione e il trasporto dei dispositivi fisici contenenti le informazioni e i dati che sono trattati nell'ambito dell'erogazione dei servizi previsti nel Contratto.

I.12.4 I sistemi informativi utilizzati dal Fornitore per l'erogazione dei servizi previsti dal Contratto garantiscono la riservatezza, l'integrità e la disponibilità di tutte le informazioni trasmesse nella rete interna del Fornitore e/o verso l'esterno.

I.12.5 Il Fornitore è in grado di respingere attacchi di information spillage (ad esempio isolando le informazioni o i sistemi o le componenti dei sistemi contaminate) che dovessero occorrere sui sistemi o sulle informazioni utilizzati per l'erogazione dei servizi previsti nel Contratto.

I.13 Application Software Security

Qualora i servizi previsti nel Contratto implichino lo sviluppo di software:

I.13.1 Il Fornitore adotta al proprio interno politiche e procedure relative al Software Development Life Cycle, conformi a quelle definite da Sogei.

I.13.2 Il Fornitore dispone di un sistema in grado di analizzare il software e di indicare eventuali errori di progettazione e implementazione mediante alert di messaggi di errore.

I.13.3 Il Fornitore dispone di un sistema in grado di validare tutti i flussi informativi in input al codice sviluppato.

I.13.4 Il Fornitore garantisce che l'accesso al codice software sia ristretto al solo personale autorizzato nel rispetto del principio del need-to-know.

I.13.5 Gli ambienti di sviluppo, test e produzione del Fornitore sono segregati al fine di ridurre i rischi di accesso non autorizzato o change agli ambienti operativi.

I.14 Incident Response and Management

I.14.1 Il Fornitore definisce internamente un processo per la gestione degli incidenti che consenta l'individuazione dei ruoli e l'assegnazione delle responsabilità a tutti gli attori coinvolti, nonché le modalità operative per la gestione dell'incidente.

I.14.2 Il Fornitore si impegna a:

- concordare con Sogei le modalità di gestione e coordinamento in caso di incidente;
- coordinarsi con Sogei nell'ambito delle attività di esercitazione di risposta agli incidenti svolte da Sogei;
- concordare con Sogei i flussi di comunicazione e reportistica in caso di incidente;
- supportare Sogei nelle attività di indagine e analisi post-incidente;
- indicare un soggetto che funga da referente per il coordinamento con Sogei nell'ambito della gestione delle attività di risposta all'incidente.

I.14.3 Il Fornitore si impegna alla disclosure di incidenti informatici subiti da sé stesso o dalla sua supply chain nel momento che si dovesse prospettare un possibile impatto per Sogei.

I.15 Business Continuity & Disaster Recovery

I.15.1 Con riferimento ai servizi previsti nel Contratto, il Fornitore:

- adotta al proprio interno politiche e procedure di gestione della continuità operativa che contengano almeno: processi organizzativi per la verifica, l'attivazione, il ripristino del servizio e le modalità di rientro; programma di manutenzione (test e aggiornamento) del Piano e delle procedure di emergenza; processo di escalation; risorse necessarie;
- adotta al proprio interno, manutiene e testa periodicamente un piano di continuità operativa;
- esegue periodicamente esercitazioni del piano di continuità operativa.

I.15.2 Laddove applicabile e necessario, Sogei ha la facoltà di richiedere al Fornitore, in relazione ai servizi previsti nel Contratto, con congruo preavviso, il BCP (Business Continuity Plan) e DRP (Disaster Recovery Plan) adottato per garantire la continuità e ripristino della fornitura.

I.15.3 Con riferimento ai servizi previsti nel Contratto, il Fornitore deve garantire i livelli di servizio stabiliti all'interno della documentazione di gara.