

INNOVEMBER S.r.l.

DICHIARAZIONE DI APPLICABILITÀ

Statement of Applicability (SoA)

Documento	Dichiarazione di Applicabilità (SoA)
Standard di riferimento	ISO/IEC 27001:2022
Organizzazione	INNOVEMBER S.r.l.
Versione	1.4
Data di emissione	17 Marzo 2026
Classificazione	RISERVATO – Uso interno
Redatto da	INNOVEMBER S.r.l.
Approvato da	Direzione Generale – INNOVEMBER S.r.l.
Prossima revisione	Marzo 2027

Documento soggetto a revisione annuale. Ogni stampa o copia non aggiornata è da considerarsi non controllata.

INDICE

INFORMAZIONI SUL DOCUMENTO..... 3

INTRODUZIONE E SCOPO..... 3

CAMPO DI APPLICAZIONE DEL SGSI..... 3

METODOLOGIA DI SELEZIONE DEI CONTROLLI..... 5

LEGENDA 5

TABELLA DEI CONTROLLI – ALLEGATO A ISO/IEC 27001:2022 6

RIEPILOGO STATISTICO..... 30

DOCUMENTI CORRELATI E RIFERIMENTI 31

REGISTRO DELLE REVISIONI 32

FIRME DI APPROVAZIONE 33

informazioni sul Documento

Il presente documento costituisce la Dichiarazione di Applicabilità (SoA – Statement of Applicability) di INNOVEMBER S.r.l., redatta in conformità alla norma ISO/IEC 27001:2022, clausola 6.1.3 lett. d). È un documento obbligatorio del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e rappresenta il collegamento formale tra la valutazione del rischio e i controlli di sicurezza selezionati nell'Allegato A della norma.

Il documento è classificato RISERVATO – USO INTERNO e deve essere protetto da divulgazione non autorizzata. Le stampe non controllate devono essere distrutte in modo sicuro.

Introduzione e Scopo

La Dichiarazione di Applicabilità è il documento che certifica, per ciascuno dei 93 controlli dell'Allegato A della ISO/IEC 27001:2022, la decisione di INNOVEMBER S.r.l. in merito alla sua applicabilità, con la relativa giustificazione basata sui risultati della valutazione del rischio (Risk Assessment).

Il presente documento ha lo scopo di:

- Identificare tutti i controlli dell'Allegato A della ISO/IEC 27001:2022 applicabili al contesto di INNOVEMBER S.r.l.
- Indicare per ciascun controllo lo stato di implementazione attuale (Sì / Parziale / No).
- Giustificare l'inclusione o l'esclusione di ciascun controllo, con riferimento ai rischi identificati nel Risk Register.
- Fornire riferimento ai rischi del Risk Register che hanno originato la selezione del controllo.
- Fornire evidenza documentale all'organismo di certificazione e agli auditor del livello di maturità del SGSI.

Questo documento deve essere letto congiuntamente al Risk Register INNOVEMBER (documento correlato: INNOVEMBER_Risk_register_ISO27001_compliant.xlsx) e alla documentazione di policy e procedure del SGSI.

Campo di Applicazione del SGSI

Il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di INNOVEMBER S.r.l. si applica a:

- Tutti i processi di sviluppo, gestione ed erogazione di servizi informatici e di consulenza tecnologica.
- Le infrastrutture IT di proprietà aziendale e in cloud, incluso il tenant Microsoft 365, le piattaforme di web hosting (Hostinger), i sistemi SaaS e gli strumenti di intelligenza artificiale in uso.
- Tutto il personale dipendente, collaboratori, consulenti e fornitori con accesso ai sistemi informativi aziendali.
- Le sedi operative di INNOVEMBER S.r.l., incluse le postazioni di lavoro remoto (smart working).
- I servizi erogati ai clienti, incluso l'hosting e la gestione di siti web, applicazioni e infrastrutture digitali.

Sono esclusi dal campo di applicazione: i sistemi di terze parti non gestiti da INNOVEMBER S.r.l. e le attività di business non correlate ai servizi digitali e informatici. Le esclusioni sono motivate nella tabella dei controlli alla colonna 'Motivazione/Note'.

**INNOVEMBER s.r.l.**

Iscritta al registro delle PMI innovative

Sede legale in I-20123 Milano (MI) – Via Cicco Simonetta 7

Unità Locale in I-80143 Napoli (NA) – Via G. Porzio 4, Centro Direzionale, Isola G1

Codice fiscale e nr. iscrizione al Registro Imprese di Milano 10446260969

P.IVA IT10446260969 - Rea: MI -2532163 - Capitale sociale € 180.000,00 I.V.

Metodologia di Selezione dei Controlli

La selezione dei controlli applicabili è stata effettuata secondo il processo strutturato di seguito descritto, conforme ai requisiti della clausola 6.1.3 della ISO/IEC 27001:2022:

- Identificazione degli asset informativi critici e dei relativi proprietari (asset owner), inclusi ambienti cloud M365, piattaforme web, dispositivi endpoint, dati aziendali e di clienti.
- Analisi delle minacce e vulnerabilità per ciascun asset attraverso il processo di Risk Assessment con metodologia qualitativa (matrice 5x5 probabilità/impatto).
- Valutazione del rischio residuo: identificazione di 12 rischi principali classificati per ID, categoria, livello di rischio e stato (Risk Register).
- Confronto sistematico di ciascun rischio con tutti e 93 i controlli dell'Allegato A: per ogni abbinamento rischio-controllo pertinente sono state definite l'azione di controllo proposta e il risultato atteso.
- Selezione dei controlli Annex A proporzionali al livello di rischio e al contesto operativo di INNOVEMBER S.r.l.
- Revisione e approvazione del SoA da parte della Direzione e del CISO.

I controlli inclusi nel presente documento sono stati selezionati sulla base dei rischi identificati nel Risk Register. Tutti i 93 controlli dell'Allegato A sono stati presi in considerazione. I controlli per cui è stato applicato lo stato 'Parziale' sono in corso di implementazione con piano di completamento definito.

Legenda

Stato	Significato
✓ Sì	Controllo applicabile e pienamente implementato. Le misure sono operative e verificabili.
● Parziale	Controllo applicabile ma implementato solo parzialmente. Il completamento è in corso con piano e data prevista.
X No	Controllo applicabile ma non ancora implementato. È incluso nel piano di trattamento del rischio.
N/A	Controllo non applicabile al contesto operativo di INNOVEMBER S.r.l. La motivazione di esclusione è riportata nella colonna Note.

Nota: nella colonna 'Rischi collegati' è riportato il numero di rischi del Risk Register per cui il controllo è stato selezionato come misura di trattamento. Il dettaglio degli ID rischio è consultabile nel documento Risk_mapping_Annex_A del Risk Register.



Tabella dei Controlli – Allegato A ISO/IEC 27001:2022

La seguente tabella riporta tutti i 93 controlli dell'Allegato A della norma ISO/IEC 27001:2022. Per ciascun controllo sono indicati: applicabilità, stato di implementazione, motivazione/nota operativa e numero di rischi del Risk Register a cui il controllo è associato.

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
5 - CONTROLLI ORGANIZATIVI (A.5)				
A.5.1	Politiche per la sicurezza delle informazioni	Sì	Sì	Policy ISMS approvata dalla Direzione, comunicata a tutto il personale e revisionata annualmente. Include policy specifica per M365, AI Acceptable Use Policy, password policy, credential management policy, data governance policy e supplier security policy. Rischi collegati: RSK-CYB-PHI-45, RSK-REP-DAT-44, RSK-CYB-MIS-25, RSK-CYB-CRE-34, RSK-CYB-DAT-25, RSK-CYB-DEV-34, RSK-BUS-DAT-35, RSK-SUP-FOR-24, RSK-REP-BUS-15.
A.5.2	Ruoli e responsabilità per la sicurezza delle informazioni	Sì	Sì	RACI definito e documentato per CISO, DPO e owner di sicurezza. Responsabilità esplicite per gestione MFA/accessi M365, tenant M365 e identity security. Rischi collegati: RSK-CYB-PHI-45, RSK-CYB-MIS-25, RSK-COM-PRI-34.
A.5.3	Separazione dei compiti	Sì	Sì	Segregation of duties implementata: chi richiede



INNOVEMBER s.r.l.

Iscritta al registro delle PMI innovative

Sede legale in I-20123 Milano (MI) – Via Cicco Simonetta 7

Unità Locale in I-80143 Napoli (NA) – Via G. Porzio 4, Centro Direzionale, Isola G1

Codice fiscale e nr. iscrizione al Registro Imprese di Milano 10446260969

P.IVA IT10446260969 - Rea: MI -2532163 - Capitale sociale € 180.000,00 I.V.

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.5.4	Responsabilità della direzione	Sì	Sì	accesso è distinto da chi approva. Processo di approvazione accessi con doppio controllo attivo. Rischio collegato: RSK-COM-PRI-34. La Direzione ha formalmente approvato e supporta il SGSI. Revisione annuale del management inclusa nel programma ISMS. Rischio collegato: RSK-CYB-PHI-45 (livello governance).
A.5.5	Contatti con le autorità	Sì	Sì	Procedura documentata per contatti con autorità competenti (Garante Privacy, ACN/CNAIPIC) in caso di incidente. Rischio collegato: RSK-CYB-PHI-45 (obbligo notifica data breach).
A.5.6	Contatti con gruppi di interesse speciali	Sì	Parziale	Formalizzazione in corso dell'iscrizione a ISAC e gruppi di settore per la condivisione di threat intelligence. Feed threat intelligence attivo per CMS e campagne BEC. Rischi collegati: RSK-BUS-WEB-34, RSK-REP-BUS-15.
A.5.7	Threat intelligence	Sì	Parziale	Feed threat intelligence attivo per vulnerabilità CMS (WordPress/plugin) e campagne BEC. Monitoraggio threat landscape per i principali rischi identificati. Completamento previsto: processo strutturato di

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
				raccolta e analisi TI. Rischi collegati: RSK-BUS-WEB-34, RSK-REP-BUS-15.
A.5.8	Sicurezza delle informazioni nella gestione dei progetti	Sì	Sì	Requisiti di sicurezza integrati nel ciclo di vita dei progetti. Checklist AI risk integrata nel project management per progetti che prevedono uso di strumenti AI. Rischio collegato: RSK-REP-DAT-44.
A.5.9	Inventario delle informazioni e degli altri asset associati	Sì	Sì	Asset register centralizzato con classificazione dati e restrizioni AI. Inventario endpoint aggiornato mensilmente. Revisione semestrale. Rischi collegati: RSK-REP-DAT-44, RSK-CYB-DEV-34.
A.5.10	Utilizzo accettabile delle informazioni e degli altri asset associati	Sì	Sì	Acceptable Use Policy pubblicata e firmata da tutti gli utenti. Include sezione specifica sull'uso di strumenti AI, regole per gestione password, policy per dispositivi aziendali e BYOD. Rischi collegati: RSK-REP-DAT-44, RSK-CYB-CRE-34, RSK-CYB-DEV-34.
A.5.11	Restituzione degli asset	Sì	Sì	Checklist di restituzione dispositivi e revoca accessi integrata nel processo di offboarding. Applicabile al ciclo di vita endpoint aziendali. Rischio collegato: RSK-CYB-DEV-34.

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.5.12	Classificazione delle informazioni	Sì	Sì	Schema di classificazione a 4 livelli (Pubblico, Interno, Riservato, Segreto) applicato. Classificazione dati attiva su SharePoint/OneDrive con Microsoft Purview. Definite restrizioni su dati che possono essere inseriti in tool AI. Rischi collegati: RSK-REP-DAT-44, RSK-CYB-DAT-25.
A.5.13	Etichettatura delle informazioni	Sì	Parziale	Labelling automatico in rollout su suite M365 tramite Microsoft Purview Information Protection. Classificazione applicata su documenti critici. Completamento previsto: coverage 100% documenti classificati. Rischi collegati: RSK-REP-DAT-44, RSK-CYB-DAT-25.
A.5.14	Trasferimento delle informazioni	Sì	Sì	Policy di trasferimento dati definita: regole per condivisione file interni/esterni, link pubblici anonimi disabilitati per file sensibili. Dati confidenziali non trasferibili verso AI pubblici non autorizzati. DPA verificato per provider AI. Rischi collegati: RSK-REP-DAT-44, RSK-CYB-DAT-25.
A.5.15	Controllo degli accessi	Sì	Sì	Access control policy RBAC formale implementata. Conditional Access policies su M365 basate su ruolo e



Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
				posizione. Rischi collegati: RSK-CYB-PHI-45, RSK-COM-PRI-34.
A.5.16	Gestione delle identità	Sì	Sì	Identità centralizzate su Azure Active Directory. Processo formalizzato di onboarding/offboarding con checklist accessi. Registro account admin aggiornato con verifica trimestrale. Nessun account orfano tollerato. Rischi collegati: RSK-CYB-PHI-45, RSK-CYB-MIS-25, RSK-COM-PRI-34.
A.5.17	Informazioni di autenticazione	Sì	Sì	MFA obbligatoria abilitata per tutti gli utenti inclusi gli amministratori. Password manager aziendale adottato. Break-glass account documentato e testato. Credenziali non conservate in chiaro; conformità GDPR verificata. Rischi collegati: RSK-CYB-PHI-45, RSK-CYB-MIS-25, RSK-CYB-CRE-34.
A.5.18	Diritti di accesso	Sì	Sì	Access review semestrale documentata per tutti i sistemi. Diritti non necessari revocati entro 30gg dalla verifica. Permessi SharePoint/OneDrive rivisti e conformi al principio least privilege. Rischi collegati: RSK-CYB-PHI-45, RSK-COM-PRI-34, RSK-CYB-DAT-25.



Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.5.19	Sicurezza delle informazioni nelle relazioni con i fornitori	Sì	Sì	Vendor assessment formale completato per tutti i fornitori critici prima dell'onboarding. Valutazione sicurezza Hostinger, Microsoft e altri provider SaaS. Rischi collegati: RSK-BUS-WEB-34, RSK-REP-SER-24, RSK-SUP-FOR-24.
A.5.20	Sicurezza delle informazioni negli accordi con i fornitori	Sì	Sì	Requisiti di sicurezza ISO 27001/GDPR inclusi in tutti i contratti SaaS. Clausole di sicurezza, notifica incidenti, SLA e backup verificati nei contratti con Hostinger e Microsoft. NDA firmati da tutti i fornitori con accesso a dati aziendali. Rischi collegati: RSK-BUS-WEB-34, RSK-REP-SER-24, RSK-SUP-FOR-24.
A.5.21	Gestione della sicurezza delle informazioni nella catena di approvvigionamento ICT	Sì	Sì	ICT supply chain mapping completato. Valutazione sub-fornitori dei provider principali (Microsoft, Hostinger). Rischi identificati e gestiti. Rischio collegato: RSK-SUP-FOR-24.
A.5.22	Monitoraggio, revisione e gestione dei cambiamenti dei servizi dei fornitori	Sì	Sì	Review trimestrale dei provider documentata. KPI di uptime e sicurezza monitorati per M365 e Hostinger. Review annuale fornitore con revisione SLA. Rischi collegati: RSK-BUS-WEB-34, RSK-REP-SER-24, RSK-SUP-FOR-24.
A.5.23	Sicurezza delle informazioni per	Sì	Sì	Cloud risk assessment completato per M365,

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
	l'uso dei servizi cloud			Hostinger e altri SaaS critici. Rischi residui documentati e accettati o mitigati. Valutazione sicurezza cloud secondo criteri ISO/CSA. Rischi collegati: RSK-BUS-WEB-34, RSK-REP-SER-24, RSK-SUP-FOR-24.
A.5.24	Pianificazione e preparazione alla gestione degli incidenti di sicurezza	Sì	Sì	Piano di incident management con playbook specifici: phishing/BEC, perdita accesso tenant, interruzione SaaS, defacement web. Team di risposta agli incidenti definito. Rischi collegati: RSK-CYB-PHI-45, RSK-CYB-MIS-25, RSK-REP-SER-24, RSK-REP-BUS-15.
A.5.25	Valutazione e decisione sugli eventi di sicurezza delle informazioni	Sì	Sì	Processo di triage eventi di sicurezza documentato. Soglie di alert definite; eventi valutati entro SLA. Criteri per valutazione eventi email sospetti. Rischi collegati: RSK-CYB-PHI-45, RSK-REP-BUS-15.
A.5.26	Risposta agli incidenti di sicurezza delle informazioni	Sì	Sì	Procedura di risposta documentata: blocco account, reset credenziali, isolamento sistemi, notifica clienti/autorità. Tempo medio di risposta obiettivo < 4 ore. Test annuale dei playbook. Rischi collegati: RSK-CYB-PHI-45, RSK-BUS-WEB-34, RSK-REP-BUS-15.

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.5.27	Apprendimento dagli incidenti di sicurezza delle informazioni	Sì	Sì	Post-incident review documentata per ogni incidente significativo. Lessons learned integrate nei cicli formativi e nei controlli tecnici. Rischio collegato: RSK-REP-BUS-15.
A.5.28	Raccolta di prove	Sì	Sì	Unified Audit Log M365 attivo con conservazione minima 90 giorni. Procedure di conservazione delle prove forensi documentate per supporto eventuali procedimenti. Rischio collegato: RSK-CYB-PHI-45 (raccolta evidence post-incidente).
A.5.29	Sicurezza delle informazioni durante le interruzioni	Sì	Sì	Procedure operative documentate per continuità in caso di: perdita accesso tenant M365, perdita dati critici, outage SaaS. BCP aggiornato con RTO/RPO definiti. Rischi collegati: RSK-CYB-MIS-25, RSK-BUS-DAT-35, RSK-REP-SER-24.
A.5.30	Prontezza ICT per la continuità operativa	Sì	Sì	Piano BCP con scenari: M365 indisponibile, perdita dati, hosting down. Test annuale documentato. RTO < 4 ore per servizi critici. Rischi collegati: RSK-CYB-MIS-25, RSK-BUS-DAT-35, RSK-REP-SER-24.

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.5.31	Requisiti legali, statutari, normativi e contrattuali	Sì	Sì	Conformità GDPR verificata: registro dei trattamenti aggiornato, DPA con fornitori, audit contrattuale annuale. Conformità normativa nella catena di fornitura. Rischi collegati: RSK-COM-PRI-34, RSK-SUP-FOR-24.
A.5.32	Diritti di proprietà intellettuale	Sì	Sì	Policy uso software e IP definita. Licenze software monitorate. Applicabile al contesto di erogazione servizi informatici. Rischio collegato: RSK-REP-DAT-44 (uso non autorizzato di contenuti tramite AI).
A.5.33	Protezione delle registrazioni	Sì	Sì	Politica di data retention e cancellazione sicura conforme al GDPR. Log conservati con integrità garantita. Rischi collegati: RSK-CYB-DAT-25, RSK-BUS-DAT-35.
A.5.34	Privacy e protezione dei dati personali	Sì	Sì	Conformità GDPR garantita: dati personali su SharePoint protetti, credenziali non in chiaro, DPA con provider AI verificato, nessuna PII inviata a tool non autorizzati. Audit permessi su siti con PII completato. Rischi collegati: RSK-REP-DAT-44, RSK-CYB-CRE-34, RSK-CYB-DAT-25.
A.5.35	Revisione indipendente della	Sì	Sì	Audit interno annuale del SGSI. Penetration test su applicazioni critiche.



INNOVEMBER s.r.l.

Iscritta al registro delle PMI innovative

Sede legale in I-20123 Milano (MI) – Via Cicco Simonetta 7

Unità Locale in I-80143 Napoli (NA) – Via G. Porzio 4, Centro Direzionale, Isola G1

Codice fiscale e nr. iscrizione al Registro Imprese di Milano 10446260969

P.IVA IT10446260969 - Rea: MI -2532163 - Capitale sociale € 180.000,00 I.V.

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.5.36	sicurezza delle informazioni			Programma di audit include gestione accessi, email security, conformità policy. Rischi trattati nell'ambito: RSK-CYB-PHI-45, RSK-COM-PRI-34.
	Conformità alle policy, regole e standard per la sicurezza delle informazioni	Sì	Sì	Verifiche periodiche di conformità a policy di autenticazione, AI policy, password policy, email security policy e accessi. Audit semestrali documentati con evidence. Non conformità chiuse entro 30gg. Rischi collegati: RSK-CYB-PHI-45, RSK-REP-DAT-44, RSK-COM-PRI-34, RSK-CYB-CRE-34, RSK-REP-BUS-15.
	Procedure operative documentate	Sì	Sì	Procedure operative documentate per: provisioning/deprovisioning accessi, incident response, backup/restore, change management, dismissione dispositivi. Rischio collegato: RSK-COM-PRI-34.
6 - CONTROLLI SULLE PERSONE (A.6)				
A.6.1	Screening	Sì	Sì	Background check pre-assunzione definito per ruoli con accesso privilegiato. Verifica referenze completata per nuovi assunti. Requisiti di accesso verificati nel processo di screening. Rischio collegato: RSK-COM-PRI-34.



Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.6.2	Termini e condizioni di impiego	Sì	Sì	Clausole di sicurezza inserite in tutti i contratti di lavoro: obblighi su accessi, riservatezza, conformità policy ISMS. Rischio collegato: RSK-COM-PRI-34.
A.6.3	Consapevolezza, istruzione e formazione sulla sicurezza delle informazioni	Sì	Sì	Piano annuale di formazione attivo: modulo anti-phishing, gestione credenziali, uso sicuro AI, sicurezza endpoint, data leakage, sicurezza email. Simulazioni phishing trimestrali con target > 85% superamento. Formazione CMS/hardening per gestori siti web. Rischi collegati: RSK-CYB-PHI-45, RSK-REP-DAT-44, RSK-BUS-WEB-34, RSK-CYB-CRE-34, RSK-CYB-DAT-25, RSK-CYB-DEV-34, RSK-REP-BUS-15.
A.6.4	Processo disciplinare	Sì	Sì	Procedura disciplinare formalizzata per violazioni delle politiche di sicurezza. Graduazione sanzioni proporzionale alla gravità. Rischio collegato: RSK-COM-PRI-34 (misuse privilege).
A.6.5	Responsabilità dopo la cessazione o il cambiamento di impiego	Sì	Sì	Procedura di offboarding con revoca accessi entro 24h dalla cessazione, restituzione dispositivi e reminder obblighi NDA post-cessazione. Rischio collegato: RSK-COM-PRI-34.



Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.6.6	Accordi di riservatezza o di non divulgazione	Sì	Sì	NDA standardizzati firmati da dipendenti, collaboratori e fornitori con accesso a dati aziendali. Clausole esplicite su credenziali e dati sensibili. Rischi collegati: RSK-CYB-CRE-34, RSK-SUP-FOR-24.
A.6.7	Lavoro a distanza	Sì	Sì	Remote working policy documentata: VPN obbligatoria, MFA, dispositivi gestiti tramite MDM, endpoint protection attivo. Rischio collegato: RSK-CYB-DEV-34.
A.6.8	Segnalazione degli eventi di sicurezza delle informazioni	Sì	Sì	Canale di segnalazione email sospette attivo (pulsante/processo report phishing). Procedura di incident reporting con canali dedicati. Statistiche di segnalazione monitorate. Rischi collegati: RSK-CYB-PHI-45, RSK-REP-BUS-15.
7 - CONTROLLI FISICI (A.7)				
A.7.1	Perimetri di sicurezza fisica	Sì	Sì	Controllo accessi fisici alle sedi operative. Aree server e networking segregate con accesso limitato al personale autorizzato. Applicabile alle postazioni di lavoro e ai locali tecnici. Rischio collegato: RSK-CYB-DEV-34 (protezione dispositivi in sede).
A.7.2	Accesso fisico	Sì	Sì	Procedure di controllo accesso fisico documentate.

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.7.3	Messa in sicurezza di uffici, locali e strutture	Sì	Sì	Badge/chiave per accesso aree riservate. Registro visitatori per aree sensibili. Rischio collegato: RSK-CYB-DEV-34. Uffici e locali tecnici protetti con serrature adeguate. Server e apparati di rete in armadi chiusi. Rischio collegato: RSK-CYB-DEV-34 (protezione fisica dispositivi).
A.7.4	Monitoraggio della sicurezza fisica	Sì	Sì	Sistemi di monitoraggio fisico attivi nelle aree critiche. Controllo accessi registrato. Rischio collegato: RSK-CYB-DEV-34.
A.7.5	Protezione dalle minacce fisiche e ambientali	Sì	Sì	Misure di protezione da incendi, allagamenti e interruzioni di corrente nelle aree IT. UPS e sistemi di backup energetico. Rischio collegato: RSK-REP-SER-24 (continuità operativa).
A.7.6	Lavoro in aree sicure	Sì	Sì	Procedure per il lavoro in aree sicure documentate. Accesso limitato alle aree con sistemi critici. Rischio collegato: RSK-CYB-DEV-34.
A.7.7	Scrivania libera e schermo pulito	Sì	Sì	Clear desk e clear screen policy implementata e comunicata. Compliance verificata periodicamente. Lock automatico schermo attivo su tutti i dispositivi dopo

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
				inattività. Rischio collegato: RSK-CYB-DEV-34.
A.7.8	Posizionamento e protezione delle apparecchiature	Sì	Sì	Dispositivi posizionati in modo da prevenire accessi non autorizzati e danni fisici. Rischio collegato: RSK-CYB-DEV-34.
A.7.9	Sicurezza degli asset fuori sede	Sì	Sì	Policy asset off-premises comunicata: cifratura disco obbligatoria su tutti i dispositivi portatili. Procedura per segnalazione di smarrimento/furto. Rischio collegato: RSK-CYB-DEV-34.
A.7.10	Supporti di memorizzazione	Sì	Sì	Procedura di gestione, cifratura e smaltimento sicuro dei supporti rimovibili. Inventario supporti mantenuto. Rischio collegato: RSK-CYB-DEV-34 (protezione dati su dispositivi).
A.7.11	Servizi di supporto	Sì	Sì	UPS e sistemi di condizionamento per ambienti IT. Contratti di manutenzione con SLA per servizi critici. Rischio collegato: RSK-REP-SER-24 (continuità infrastruttura).
A.7.12	Sicurezza del cablaggio	Sì	Sì	Cavi di rete e alimentazione protetti fisicamente. Canalizzazioni dedicate per infrastruttura di rete. Rischio collegato: RSK-REP-SER-24 (continuità connettività).



INNOVEMBER s.r.l.

Iscritta al registro delle PMI innovative

Sede legale in I-20123 Milano (MI) – Via Cicco Simonetta 7

Unità Locale in I-80143 Napoli (NA) – Via G. Porzio 4, Centro Direzionale, Isola G1

Codice fiscale e nr. iscrizione al Registro Imprese di Milano 10446260969

P.IVA IT10446260969 - Rea: MI -2532163 - Capitale sociale € 180.000,00 I.V.

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.7.13	Manutenzione delle apparecchiature	Sì	Sì	Manutenzione preventiva documentata per apparecchiature critiche. Contratti di manutenzione attivi. Rischio collegato: RSK-REP-SER-24.
A.7.14	Smaltimento sicuro o riutilizzo delle apparecchiature	Sì	Sì	Procedura di dismissione sicura dispositivi: wipe certificato o distruzione fisica. Registro dismissioni mantenuto. Procedura di remote wipe testata. Rischio collegato: RSK-CYB-DEV-34.
8 - CONTROLLI TECNOLOGICI (A.8)				
A.8.1	Dispositivi endpoint degli utenti	Sì	Sì	MDM (Microsoft Intune) attivo su 100% dei dispositivi aziendali. Compliance verificata centralmente. Policy di configurazione sicura distribuita via MDM. Rischio collegato: RSK-CYB-DEV-34.
A.8.2	Diritti di accesso privilegiati	Sì	Sì	Privileged Identity Management (PIM) abilitato su M365. Admin roles assegnati just-in-time. Minimo 2 Global Admin account attivi. Nessun admin permanente non necessario. Revisione mensile. Rischi collegati: RSK-CYB-PHI-45, RSK-CYB-MIS-25, RSK-COM-PRI-34.
A.8.3	Restrizione dell'accesso alle informazioni	Sì	Sì	Restrizioni di accesso configurate per ruolo su M365 (SharePoint/Exchange/Teams).

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.8.4	Accesso al codice sorgente	Sì	Sì	Permessi verificati conformi al principio least privilege. Rischi collegati: RSK-CYB-PHI-45, RSK-COM-PRI-34, RSK-CYB-DAT-25. Accesso ai repository di codice limitato agli sviluppatori autorizzati. Code review obbligatoria. Branch protection attiva. Applicabile nell'ambito dei servizi di sviluppo software erogati. Rischio collegato: attività di sviluppo gestite internamente.
A.8.5	Autenticazione sicura	Sì	Sì	MFA obbligatoria + Conditional Access + SSPR su M365. Admin login solo da device gestiti e conformi. Autenticazione forte su tutti i dispositivi aziendali (PIN/biometria). Rischi collegati: RSK-CYB-PHI-45, RSK-CYB-MIS-25, RSK-COM-PRI-34, RSK-CYB-CRE-34, RSK-CYB-DEV-34.
A.8.6	Gestione della capacità	Sì	Sì	Monitoraggio utilizzo storage e capacità SaaS. Capacity planning documentato con alert su soglie di utilizzo. Dashboard utilizzo SaaS attiva. Rischi collegati: RSK-BUS-DAT-35, RSK-REP-SER-24.
A.8.7	Protezione contro i malware	Sì	Sì	EDR di nuova generazione su tutti gli endpoint con aggiornamenti automatici. WAF attivo e configurato su



Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
				server web. Microsoft Defender for Office 365 attivo con Safe Links e Safe Attachments. Scan settimanale vulnerabilità. Rischi collegati: RSK-BUS-WEB-34, RSK-CYB-DEV-34, RSK-REP-BUS-15.
A.8.8	Gestione delle vulnerabilità tecniche	Sì	Sì	Patch management formalizzato con SLA: vulnerabilità critiche risolte entro 7gg. Aggiornamenti automatici CMS e plugin abilitati. Vulnerability scanning settimanale. Nessuna vulnerabilità critica aperta oltre i termini. Rischio collegato: RSK-BUS-WEB-34.
A.8.9	Gestione della configurazione	Sì	Sì	Baseline di configurazione sicura (CIS Benchmark) applicata a dispositivi e sistemi. Hardening CMS documentato. Configurazioni CMS: rimozione plugin inutilizzati, header di sicurezza, hardening applicato. Rischi collegati: RSK-BUS-WEB-34, RSK-CYB-DEV-34.
A.8.10	Cancellazione delle informazioni	Sì	Sì	Procedura di cancellazione sicura dati da dispositivi dismessi o rubati. Remote wipe documentato e testato. Data retention policy conforme GDPR. Rischio collegato: RSK-CYB-DEV-34.

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.8.11	Mascheratura dei dati	Sì	Parziale	Data masking applicato prima di condividere dati con tool AI e in ambienti di test/sviluppo. Tokenizzazione e pseudonimizzazione in corso di implementazione sistematica. Procedura masking documentata. Rischi collegati: RSK-REP-DAT-44, RSK-CYB-DAT-25.
A.8.12	Prevenzione della fuga di dati	Sì	Parziale	Microsoft Purview DLP in fase di completamento rollout: policy attive su email e cloud storage. Alert su tentativi di invio dati sensibili verso AI esterni e domini non autorizzati. Report mensile violazioni DLP. Rischi collegati: RSK-REP-DAT-44, RSK-CYB-DAT-25.
A.8.13	Backup delle informazioni	Sì	Sì	Politica di backup 3-2-1 implementata. Backup automatico giornaliero indipendente da M365 con retention minima 30gg. Backup giornaliero siti web completo con restore test mensile documentato. Test di ripristino trimestrali documentati. Rischi collegati: RSK-BUS-WEB-34, RSK-BUS-DAT-35, RSK-REP-SER-24.
A.8.14	Ridondanza delle strutture di	Sì	Sì	Architettura HA con cluster attivo-passivo. Datacenter primario con DR su cloud.

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
	elaborazione delle informazioni			Backup offline/alternativo per dati critici indipendente da SaaS. Piano ridondanza definito con fallback operativo per servizi critici. Rischi collegati: RSK-BUS-DAT-35, RSK-REP-SER-24.
A.8.15	Registrazione degli eventi	Sì	Sì	Unified Audit Log M365 attivo su tutti i servizi con conservazione 90gg+. Log accessi e autenticazioni attivi con alert su anomalie. Log admin e azioni privilegiate conservati. Log backup/restore tracciati. Log SharePoint/OneDrive per accessi e condivisioni. Rischi collegati: RSK-CYB-PHI-45, RSK-CYB-MIS-25, RSK-CYB-CRE-34, RSK-CYB-DAT-25, RSK-BUS-DAT-35, RSK-REP-BUS-15.
A.8.16	Monitoraggio delle attività	Sì	Sì	Alert automatici su: login anomali/fuori orario, accessi da posizioni insolite, mass mailing, forward email non autorizzati, condivisioni anomale SharePoint. Monitoring uptime SaaS con SLA breach alert. Monitoraggio siti web ospitati. Revisione settimanale report sicurezza. Rischi collegati: RSK-CYB-PHI-45, RSK-BUS-WEB-34, RSK-CYB-DAT-25, RSK-REP-SER-24, RSK-REP-BUS-15.

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.8.17	Sincronizzazione degli orologi	Sì	Sì	NTP sincronizzato su tutti i sistemi. Configurazione monitorata via SIEM. Coerenza temporale garantita per correlazione log e forensics. Rischio collegato: prerequisito per corretta correlazione eventi su tutti i rischi gestiti.
A.8.18	Utilizzo di programmi di utilità con privilegi	Sì	Sì	PAM implementato. Utilizzo di utility privilegiate limitato e auditato. Accesso just-in-time tramite PIM. Rischio collegato: RSK-CYB-PHI-45 (gestione tool privilegiati M365).
A.8.19	Installazione di software su sistemi operativi	Sì	Sì	Policy software whitelisting attiva. Installazioni gestite tramite MDM aziendale (Intune). Utenti standard senza privilegi di installazione. Rischio collegato: RSK-CYB-DEV-34.
A.8.20	Sicurezza delle reti	Sì	Sì	Segmentazione di rete con VLAN. Firewall next-gen con IDS/IPS integrati. Connessioni sicure verso fornitori SaaS verificate. Rischio collegato: RSK-SUP-FOR-24 (sicurezza connessioni verso provider).
A.8.21	Sicurezza dei servizi di rete	Sì	Sì	Accordi SLA con provider di rete. Verifica periodica delle configurazioni di rete. Connessioni cifrate (TLS 1.2+) per tutti i servizi. Rischio collegato: RSK-REP-SER-24



Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
				(qualità e sicurezza connettività SaaS).
A.8.22	Separazione delle reti	Sì	Sì	DMZ, rete produzione, sviluppo e guest network separati logicamente e fisicamente. Rischio collegato: RSK-REP-SER-24 (isolamento sistemi critici).
A.8.23	Filtraggio web	Sì	Sì	Proxy web con filtraggio categorie e blocco domini malevoli tramite DNS filtering. Web filtering integrato con email security per blocco URL malevoli. Rischi collegati: RSK-BUS-WEB-34, RSK-REP-BUS-15.
A.8.24	Utilizzo della crittografia	Sì	Sì	Politica crittografica: TLS 1.2+ per dati in transito, AES-256 per dati a riposo, RSA-2048/ECC per chiavi. BitLocker/FileVault abilitato su 100% dispositivi aziendali. Verifica trimestrale cifratura endpoint. Rischio collegato: RSK-CYB-DEV-34.
A.8.25	Ciclo di vita dello sviluppo sicuro	Sì	Parziale	SDLC sicuro in fase di formalizzazione. SAST/DAST integrati nella pipeline CI/CD. Applicabile all'attività di sviluppo software per clienti. Completamento previsto: processo SDLC formalizzato entro fine anno. Rischio collegato: RSK-BUS-WEB-34 (ciclo vita applicazioni web clienti).

Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.8.26	Requisiti di sicurezza delle applicazioni	Sì	Parziale	Checklist requisiti di sicurezza applicativa in corso di standardizzazione (OWASP-based). Applicabile a sviluppo e gestione applicazioni web per clienti. Rischio collegato: RSK-BUS-WEB-34.
A.8.27	Principi di architettura e ingegneria sicura	Sì	Sì	Adozione dei principi: least privilege, defence in depth, zero trust architecture. Applicati nella progettazione di infrastrutture cloud e sistemi M365. Rischio collegato: RSK-CYB-PHI-45 (architettura identity security).
A.8.28	Codifica sicura	Sì	Parziale	Linee guida di secure coding in fase di pubblicazione interna (OWASP Top 10 come riferimento). Code review obbligatoria per sviluppo siti e applicazioni clienti. Rischio collegato: RSK-BUS-WEB-34.
A.8.29	Test di sicurezza in sviluppo e accettazione	Sì	Parziale	Penetration test annuali su applicazioni critiche. Vulnerability assessment in roadmap. DAST in pipeline CI/CD. Test di sicurezza pre-release per applicazioni clienti. Rischio collegato: RSK-BUS-WEB-34.
A.8.30	Sviluppo esternalizzato	Sì	Sì	Clausole contrattuali di sicurezza nei contratti con sviluppatori terzi. Code review



Codice	Controllo ISO/IEC 27001:2022	Applicabile	Implementato	Motivazione / Note operative e riferimenti Risk Register
A.8.31	Separazione degli ambienti di sviluppo, test e produzione	Sì	Sì	obbligatoria per codice esterno. NDA sottoscritti. Rischio collegato: RSK-SUP-FOR-24 (supply chain sviluppo). Ambienti dev/test/prod separati con accessi distinti. Nessun dato reale in ambiente di sviluppo (dati anonimizzati/sintetici). Rischio collegato: RSK-BUS-WEB-34 (separazione ambienti web clienti).
A.8.32	Gestione dei cambiamenti	Sì	Sì	Change management proceduralizzato. Checklist change management include verifica backup prima di ogni modifica rilevante. Rollback plan obbligatorio. Rischio collegato: RSK-BUS-DAT-35.
A.8.33	Informazioni sui test	Sì	Sì	Dati di test anonimizzati. Generazione sintetica per scenari critici. Nessun dato personale in ambienti di test non protetti. Rischio collegato: RSK-REP-DAT-44 (protezione dati in ambienti AI/test).
A.8.34	Protezione dei sistemi informativi durante i test di audit	Sì	Sì	Accesso di sola lettura ai sistemi durante audit. Attività di audit concordate preventivamente e documentate. Perimetro audit definito. Rischio collegato: prerequisito per audit SGSI e certificazione ISO 27001.



INNOVEMBER s.r.l.

Iscritta al registro delle PMI innovative

Sede legale in I-20123 Milano (MI) – Via Cicco Simonetta 7

Unità Locale in I-80143 Napoli (NA) – Via G. Porzio 4, Centro Direzionale, Isola G1

Codice fiscale e nr. iscrizione al Registro Imprese di Milano 10446260969

P.IVA IT10446260969 - Rea: MI -2532163 - Capitale sociale € 180.000,00 I.V.

Riepilogo Statistico

La tabella seguente fornisce una sintesi dello stato di applicazione dei 93 controlli dell'Allegato A, suddivisi per macro-categoria. Il dato conferma la copertura totale dello standard nel contesto del SGSI di INNOVEMBER S.r.l.

Categoria	Totale controlli	Applicabili	Implementati	Parziali	% Completamento
A.5 – Controlli Organizzativi	37	37	34	3	92%
A.6 – Controlli sulle Persone	8	8	8	0	100%
A.7 – Controlli Fisici	14	14	14	0	100%
A.8 – Controlli Tecnologici	34	34	28	6	82%
TOTALE	93	93	84	9	90%

Note interpretative:

- Tutti i 93 controlli dell'Allegato A sono stati valutati e inclusi nella presente SoA.
- I controlli con stato 'Parziale' sono in corso di implementazione. Il completamento è pianificato entro il ciclo di revisione corrente (Aprile 2026 – Aprile 2027).
- Non vi sono controlli esclusi senza motivazione. Il SGSI di INNOVEMBER copre l'intero perimetro normativo dell'Allegato A ISO/IEC 27001:2022.
- I rischi che hanno originato la selezione di ciascun controllo sono documentati nel Risk Register allegato (INNOVEMBER_Risk_register_ISO27001_compliant.xlsx, foglio Risk_mapping_Annex_A).

Documenti Correlati e Riferimenti

Documento	Tipo	Versione	Note
Risk Register INNOVEMBER	Excel (.xlsx)	Aggiornato 2026	Documento principale di Risk Assessment e mapping Annex A
ISMS Policy Aziendale	Policy	1.x	Politica SGSI approvata dalla Direzione
AI Acceptable Use Policy	Policy	1.x	Regole per uso di strumenti AI in azienda
Password & Credential Policy	Policy	1.x	Gestione sicura credenziali e autenticazione
Data Governance & Sharing Policy	Policy	1.x	Classificazione dati, labelling, condivisione
Access Control Policy (RBAC)	Policy	1.x	Controllo accessi basato su ruolo
Incident Response Plan	Procedura	1.x	Playbook per gestione incidenti (phishing, BEC, outage)
Business Continuity Plan (BCP)	Procedura	1.x	Continuità operativa e RTO/RPO
Supplier Security Policy	Policy	1.x	Vendor assessment e requisiti contrattuali
Endpoint & Device Management Policy	Policy	1.x	Gestione sicura dispositivi aziendali (MDM/Intune)
Backup & Recovery Policy	Policy	1.x	Politica 3-2-1 backup e test ripristino



INNOVEMBER s.r.l.

Iscritta al registro delle PMI innovative

Sede legale in I-20123 Milano (MI) – Via Cicco Simonetta 7

Unità Locale in I-80143 Napoli (NA) – Via G. Porzio 4, Centro Direzionale, Isola G1

Codice fiscale e nr. iscrizione al Registro Imprese di Milano 10446260969

P.IVA IT10446260969 - Rea: MI -2532163 - Capitale sociale € 180.000,00 I.V.

Registro delle Revisioni

Ver.	Data	Autore	Approvatore	Descrizione modifica
1.0	Aprile 2026	CISO INNOVEMBER S.r.l.	Direzione Generale	Prima emissione – copertura completa 93 controlli Annex A ISO/IEC 27001:2022 con mapping risk register

**INNOVEMBER s.r.l.**

Iscritta al registro delle PMI innovative

Sede legale in I-20123 Milano (MI) – Via Cicco Simonetta 7

Unità Locale in I-80143 Napoli (NA) – Via G. Porzio 4, Centro Direzionale, Isola G1

Codice fiscale e nr. iscrizione al Registro Imprese di Milano 10446260969

P.IVA IT10446260969 - Rea: MI -2532163 - Capitale sociale € 180.000,00 I.V.

Firme di Approvazione

Il presente documento è stato redatto, revisionato e approvato dai seguenti soggetti responsabili di INNOVEMBER S.r.l.:

Redatto da (CISO)	Verificato da (DPO / Responsabile SGSI)	Approvato da (Direzione Generale)
Nome e Cognome: _____	Nome e Cognome: _____	Nome e Cognome: _____
Firma: _____	Firma: _____	Firma: _____
Data: _____	Data: _____	Data: _____



INNOVEMBER s.r.l.

Iscritta al registro delle PMI innovative

Sede legale in I-20123 Milano (MI) – Via Cicco Simonetta 7

Unità Locale in I-80143 Napoli (NA) – Via G. Porzio 4, Centro Direzionale, Isola G1

Codice fiscale e nr. iscrizione al Registro Imprese di Milano 10446260969

P.IVA IT10446260969 - Rea: MI -2532163 - Capitale sociale € 180.000,00 I.V.