DICHIARAZIONE DI APPLICABILITÀ (SoA)

ISO/IEC 27001:2022 - Allegato A

Organizzazione	COMIN COSTRUZIONI GENERALI S.R.L.
Sede principale	Via Callalta 43, 31037 Loria (TV), Italia
Settore	IAF 28 - Costruzioni
Perimetro SGSI	Processi direzionali, amministrativi, tecnici, gestione commesse, gestione documentale, sistemi informativi e informazioni aziendali a supporto delle attività di costruzione e cantiere.
Norma di riferimento	ISO/IEC 27001:2022 - punto 6.1.3 d) e Allegato A
Versione documento	Rev. 0 - Bozza per Stage 1
Data	24/04/2026

Nota: il presente documento costituisce una bozza operativa accettabile per il riesame Stage 1 e deve essere approvato dalla Direzione dopo verifica puntuale dell'analisi dei rischi, del piano di trattamento, degli asset e delle evidenze disponibili.

1. Scopo e riferimenti

La presente Dichiarazione di Applicabilità identifica i controlli dell'Allegato A della ISO/IEC 27001:2022 ritenuti applicabili o non applicabili al Sistema di Gestione per la Sicurezza delle Informazioni di COMIN COSTRUZIONI GENERALI S.R.L., fornendo per ciascun controllo una motivazione e una modalità di attuazione/evidenza attesa.

La SoA deve essere mantenuta coerente con la valutazione dei rischi, il piano di trattamento del rischio, gli obblighi di conformità, i requisiti contrattuali e l'effettivo perimetro del SGSI.

2. Perimetro considerato

Il perimetro considerato comprende la sede principale di Via Callalta 43, 31037 Loria (TV), i processi direzionali, amministrativi, tecnici e di gestione delle commesse, la gestione di informazioni e documentazione aziendale, contrattuale, tecnica, economica, personale e di cantiere, nonché i sistemi informativi, gli archivi digitali, la PEC, i dispositivi endpoint, i servizi cloud e i fornitori IT a supporto dei processi aziendali.

I cantieri temporanei e mobili sono considerati estensioni operative del sistema per quanto riguarda la gestione, il trasferimento e la protezione delle informazioni di commessa, dei documenti tecnici, dei dati personali e delle comunicazioni con clienti, fornitori, direzione lavori, coordinatori, subappaltatori e altri stakeholder.

3. Criteri di applicabilità

Un controllo è indicato come applicabile quando contribuisce al trattamento di rischi informativi, privacy, contrattuali, organizzativi, fisici o tecnologici rilevanti per il perimetro. Un controllo è indicato come non applicabile quando il processo o la tecnologia cui si riferisce non risulta presente nel perimetro attuale; tale esclusione deve essere confermata e riesaminata in caso di modifiche organizzative, tecnologiche o contrattuali.

4. Riepilogo controlli

Totale controlli Allegato A	93
Controlli applicabili	86
Controlli non applicabili	7
Nota	Le esclusioni riguardano principalmente controlli di sviluppo software/codice sorgente, da confermare formalmente con la Direzione e il responsabile IT.

5. Dichiarazione di Applicabilità - Allegato A ISO/IEC 27001:2022

ID	Controllo	Applicabile	Motivazione	Modalità attuativa / evidenze attese
A.5.1	Politiche per la sicurezza delle informazioni (Policies for information security)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.2	Ruoli e responsabilità per la sicurezza delle informazioni (Information security roles and responsibilities)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.3	Separazione dei compiti (Segregation of duties)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.4	Responsabilità della direzione (Management responsibilities)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.5	Contatti con le autorità (Contact with authorities)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.6	Contatti con gruppi specialistici (Contact with special interest groups)	**Sì**	Applicabile per mantenere contatti con consulenti, associazioni, organismi, fornitori IT e fonti specialistiche utili al monitoraggio di sicurezza e compliance.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.7	Informazioni sulle minacce (Threat intelligence)	**Sì**	Applicabile per ricevere e valutare informazioni su minacce informatiche, vulnerabilità, phishing, malware, compromissione account, sicurezza cloud e PEC.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.8	Sicurezza delle informazioni nella gestione dei progetti (Information security in project management)	**Sì**	Applicabile ai progetti/commesse e cantieri, nei quali sono trattati documenti tecnici, contrattuali, dati di fornitori/subappaltatori e informazioni riservate.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.9	Inventario delle informazioni e degli asset associati (Inventory of information and other associated assets)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.10	Uso accettabile delle informazioni e degli asset associati (Acceptable use of information and other associated assets)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.11	Restituzione degli asset (Return of assets)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.12	Classificazione delle informazioni (Classification of information)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.13	Etichettatura delle informazioni (Labelling of information)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.14	Trasferimento delle informazioni (Information transfer)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.15	Controllo degli accessi (Access control)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.16	Gestione delle identità (Identity management)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.17	Informazioni di autenticazione (Authentication information)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.18	Diritti di accesso (Access rights)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.

ID	Controllo	Applicabile	Motivazione	Modalità attuativa / evidenze attese
A.5.19	Sicurezza delle informazioni nei rapporti con i fornitori (Information security in supplier relationships)	**Sì**	Applicabile in relazione a fornitori IT, cloud, consulenti, subappaltatori e soggetti che trattano o accedono a informazioni aziendali o di commessa.	Da verificare contratti, NDA, nomine privacy, requisiti di sicurezza, gestione credenziali, SLA, backup, accessi e riesame periodico dei servizi.
A.5.20	Sicurezza delle informazioni negli accordi con i fornitori (Addressing information security within supplier agreements)	**Sì**	Applicabile in relazione a fornitori IT, cloud, consulenti, subappaltatori e soggetti che trattano o accedono a informazioni aziendali o di commessa.	Da verificare contratti, NDA, nomine privacy, requisiti di sicurezza, gestione credenziali, SLA, backup, accessi e riesame periodico dei servizi.
A.5.21	Gestione della sicurezza nella catena di fornitura ICT (Managing information security in the ICT supply chain)	**Sì**	Applicabile in relazione a fornitori IT, cloud, consulenti, subappaltatori e soggetti che trattano o accedono a informazioni aziendali o di commessa.	Da verificare contratti, NDA, nomine privacy, requisiti di sicurezza, gestione credenziali, SLA, backup, accessi e riesame periodico dei servizi.
A.5.22	Monitoraggio, riesame e gestione modifiche dei servizi dei fornitori (Monitoring, review and change management of supplier services)	**Sì**	Applicabile in relazione a fornitori IT, cloud, consulenti, subappaltatori e soggetti che trattano o accedono a informazioni aziendali o di commessa.	Da verificare contratti, NDA, nomine privacy, requisiti di sicurezza, gestione credenziali, SLA, backup, accessi e riesame periodico dei servizi.
A.5.23	Sicurezza nell'utilizzo dei servizi cloud (Information security for use of cloud services)	**Sì**	Applicabile in relazione a fornitori IT, cloud, consulenti, subappaltatori e soggetti che trattano o accedono a informazioni aziendali o di commessa.	Da verificare contratti, NDA, nomine privacy, requisiti di sicurezza, gestione credenziali, SLA, backup, accessi e riesame periodico dei servizi.
A.5.24	Pianificazione e preparazione alla gestione degli incidenti (Information security incident management planning and preparation)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.25	Valutazione e decisione sugli eventi di sicurezza (Assessment and decision on information security events)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.26	Risposta agli incidenti di sicurezza (Response to information security incidents)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.27	Apprendimento dagli incidenti di sicurezza (Learning from information security incidents)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.28	Raccolta delle evidenze (Collection of evidence)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.29	Sicurezza delle informazioni durante le interruzioni (Information security during disruption)	**Sì**	Applicabile per assicurare disponibilità di informazioni e sistemi essenziali in caso di interruzioni, indisponibilità ICT, perdita dati, incidenti o eventi esterni.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.30	Preparazione ICT per la continuità operativa (ICT readiness for business continuity)	**Sì**	Applicabile per assicurare disponibilità di informazioni e sistemi essenziali in caso di interruzioni, indisponibilità ICT, perdita dati, incidenti o eventi esterni.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.31	Requisiti legali, statutari, regolamentari e contrattuali (Legal, statutory, regulatory and contractual requirements)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.32	Diritti di proprietà intellettuale (Intellectual property rights)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.33	Protezione delle registrazioni (Protection of records)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.34	Privacy e protezione dei dati personali (Privacy and protection of PII)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.35	Riesame indipendente della sicurezza delle informazioni (Independent review of information security)	**Sì**	Applicabile per assicurare riesame indipendente o audit interno/esterno del SGSI rispetto a requisiti ISO/IEC 27001 e controlli selezionati.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.

ID	Controllo	Applicabile	Motivazione	Modalità attuativa / evidenze attese
A.5.36	Conformità a politiche, regole e standard di sicurezza (Compliance with policies, rules and standards for information security)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.5.37	Procedure operative documentate (Documented operating procedures)	**Sì**	Applicabile al SGSI per il governo dei processi aziendali, tecnici, amministrativi e di commessa e per la protezione di dati clienti, fornitori, personale, documentazione tecnica, contratti, offerte, PEC e archivi digitali.	Prevista/da verificare evidenza di politica SGSI, ruoli, procedure, registri, accordi, controlli su accessi, fornitori, incidenti, continuità, conformità normativa e riesami.
A.6.1	Verifiche sul personale (Screening)	**Sì**	Applicabile al personale dipendente, amministratori, consulenti e soggetti che accedono a informazioni, sistemi, documenti aziendali o dati di commessa.	Da verificare: lettere/contratti, informative, istruzioni autorizzati, NDA, formazione, procedure di onboarding/offboarding, gestione dispositivi e segnalazione eventi.
A.6.2	Termini e condizioni di impiego (Terms and conditions of employment)	**Sì**	Applicabile al personale dipendente, amministratori, consulenti e soggetti che accedono a informazioni, sistemi, documenti aziendali o dati di commessa.	Da verificare: lettere/contratti, informative, istruzioni autorizzati, NDA, formazione, procedure di onboarding/offboarding, gestione dispositivi e segnalazione eventi.
A.6.3	Consapevolezza, formazione e addestramento (Information security awareness, education and training)	**Sì**	Applicabile al personale dipendente, amministratori, consulenti e soggetti che accedono a informazioni, sistemi, documenti aziendali o dati di commessa.	Da verificare: lettere/contratti, informative, istruzioni autorizzati, NDA, formazione, procedure di onboarding/offboarding, gestione dispositivi e segnalazione eventi.
A.6.4	Processo disciplinare (Disciplinary process)	**Sì**	Applicabile al personale dipendente, amministratori, consulenti e soggetti che accedono a informazioni, sistemi, documenti aziendali o dati di commessa.	Da verificare: lettere/contratti, informative, istruzioni autorizzati, NDA, formazione, procedure di onboarding/offboarding, gestione dispositivi e segnalazione eventi.
A.6.5	Responsabilità dopo cessazione o cambio mansione (Responsibilities after termination or change of employment)	**Sì**	Applicabile al personale dipendente, amministratori, consulenti e soggetti che accedono a informazioni, sistemi, documenti aziendali o dati di commessa.	Da verificare: lettere/contratti, informative, istruzioni autorizzati, NDA, formazione, procedure di onboarding/offboarding, gestione dispositivi e segnalazione eventi.
A.6.6	Accordi di riservatezza o non divulgazione (Confidentiality or non-disclosure agreements)	**Sì**	Applicabile al personale dipendente, amministratori, consulenti e soggetti che accedono a informazioni, sistemi, documenti aziendali o dati di commessa.	Da verificare: lettere/contratti, informative, istruzioni autorizzati, NDA, formazione, procedure di onboarding/offboarding, gestione dispositivi e segnalazione eventi.
A.6.7	Lavoro da remoto (Remote working)	**Sì**	Applicabile se sono presenti accessi remoti, consultazione di e-mail/PEC/cloud fuori sede, dispositivi mobili, smart working o attività da cantiere.	Da verificare regole per accesso remoto, VPN/MFA ove presenti, protezione dispositivi, divieto condivisione credenziali, cifratura, backup e supporto IT.
A.6.8	Segnalazione eventi di sicurezza (Information security event reporting)	**Sì**	Applicabile al personale dipendente, amministratori, consulenti e soggetti che accedono a informazioni, sistemi, documenti aziendali o dati di commessa.	Da verificare: lettere/contratti, informative, istruzioni autorizzati, NDA, formazione, procedure di onboarding/offboarding, gestione dispositivi e segnalazione eventi.
A.7.1	Perimetri di sicurezza fisica (Physical security perimeters)	**Sì**	Applicabile alla sede principale, agli uffici, archivi, dispositivi, apparati IT, supporti removibili e asset utilizzati anche presso cantieri o fuori sede.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.7.2	Accessi fisici (Physical entry)	**Sì**	Applicabile alla sede principale, agli uffici, archivi, dispositivi, apparati IT, supporti removibili e asset utilizzati anche presso cantieri o fuori sede.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.7.3	Protezione di uffici, locali e strutture (Securing offices, rooms and facilities)	**Sì**	Applicabile alla sede principale, agli uffici, archivi, dispositivi, apparati IT, supporti removibili e asset utilizzati anche presso cantieri o fuori sede.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.7.4	Monitoraggio della sicurezza fisica (Physical security monitoring)	**Sì**	Applicabile alla sede principale, agli uffici, archivi, dispositivi, apparati IT, supporti removibili e asset utilizzati anche presso cantieri o fuori sede.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.7.5	Protezione da minacce fisiche e ambientali (Protecting against physical and environmental threats)	**Sì**	Applicabile alla sede principale, agli uffici, archivi, dispositivi, apparati IT, supporti removibili e asset utilizzati anche presso cantieri o fuori sede.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.7.6	Lavoro in aree sicure (Working in secure areas)	**Sì**	Applicabile se sono presenti aree ad accesso controllato, archivi, locali server, uffici amministrativi o aree con documentazione riservata.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.7.7	Scrivania e schermo puliti (Clear desk and clear screen)	**Sì**	Applicabile alla sede principale, agli uffici, archivi, dispositivi, apparati IT, supporti removibili e asset utilizzati anche presso cantieri o fuori sede.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.7.8	Posizionamento e protezione delle apparecchiature (Equipment siting and protection)	**Sì**	Applicabile alla sede principale, agli uffici, archivi, dispositivi, apparati IT, supporti removibili e asset utilizzati anche presso cantieri o fuori sede.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.7.9	Sicurezza degli asset fuori sede (Security of assets off-premises)	**Sì**	Applicabile alla sede principale, agli uffici, archivi, dispositivi, apparati IT, supporti removibili e asset utilizzati anche presso cantieri o fuori sede.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.7.10	Supporti di memorizzazione (Storage media)	**Sì**	Applicabile alla sede principale, agli uffici, archivi, dispositivi, apparati IT, supporti removibili e asset utilizzati anche presso cantieri o fuori sede.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.7.11	Servizi di supporto (Supporting utilities)	**Sì**	Applicabile alla sede principale, agli uffici, archivi, dispositivi, apparati IT, supporti removibili e asset utilizzati anche presso cantieri o fuori sede.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.7.12	Sicurezza dei cablaggi (Cabling security)	**Sì**	Applicabile per cablaggi di rete, collegamenti internet, apparati e infrastrutture ICT presso la sede principale.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.7.13	Manutenzione delle apparecchiature (Equipment maintenance)	**Sì**	Applicabile alla sede principale, agli uffici, archivi, dispositivi, apparati IT, supporti removibili e asset utilizzati anche presso cantieri o fuori sede.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.

ID	Controllo	Applicabile	Motivazione	Modalità attuativa / evidenze attese
A.7.14	Smaltimento o riutilizzo sicuro delle apparecchiature (Secure disposal or re-use of equipment)	**Sì**	Applicabile alla sede principale, agli uffici, archivi, dispositivi, apparati IT, supporti removibili e asset utilizzati anche presso cantieri o fuori sede.	Da verificare accessi fisici, chiusura locali/armadi, protezione dispositivi, gestione visitatori, manutenzione, smaltimento sicuro, backup e controllo supporti.
A.8.1	Dispositivi endpoint utente (User endpoint devices)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.2	Diritti di accesso privilegiato (Privileged access rights)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.3	Restrizione dell'accesso alle informazioni (Information access restriction)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.4	Accesso al codice sorgente (Access to source code)	**No**	Non applicabile al perimetro attuale se l'organizzazione non sviluppa software, non gestisce codice sorgente e non mantiene ambienti di sviluppo/test/produzione. Applicabilità da rivalutare se emergono attività di sviluppo interno o esternalizzato.	Esclusione da giustificare nel SGSI; mantenere evidenza dell'assenza di processi di sviluppo software e rivalutare in caso di modifica del perimetro o introduzione di applicazioni sviluppate ad hoc.
A.8.5	Autenticazione sicura (Secure authentication)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.6	Gestione della capacità (Capacity management)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.7	Protezione contro malware (Protection against malware)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.8	Gestione delle vulnerabilità tecniche (Management of technical vulnerabilities)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.9	Gestione delle configurazioni (Configuration management)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.10	Cancellazione delle informazioni (Information deletion)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.11	Mascheramento dei dati (Data masking)	**Sì**	Applicabile quando dati personali o riservati vengono condivisi, esportati o usati in report, formazione, audit, test o comunicazioni esterne.	Prevedere minimizzazione, anonimizzazione/pseudonimizzazione o oscuramento dati quando necessario.
A.8.12	Prevenzione della perdita di dati (Data leakage prevention)	**Sì**	Applicabile alla prevenzione di invii impropri, perdita di documenti tecnici/contrattuali, dati personali e informazioni di commessa tramite e-mail, cloud, supporti o dispositivi.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.13	Backup delle informazioni (Information backup)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.14	Ridondanza delle strutture di elaborazione (Redundancy of information processing facilities)	**Sì**	Applicabile in misura proporzionata ai requisiti di disponibilità dei sistemi e dei dati; può essere realizzato tramite backup, servizi cloud ridondati o accordi con fornitori.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.15	Registrazione eventi/logging (Logging)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.16	Monitoraggio delle attività (Monitoring activities)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.17	Sincronizzazione degli orologi (Clock synchronization)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.18	Uso di programmi di utilità privilegiati (Use of privileged utility programs)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.

ID	Controllo	Applicabile	Motivazione	Modalità attuativa / evidenze attese
A.8.19	Installazione software su sistemi operativi (Installation of software on operational systems)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.20	Sicurezza delle reti (Network security)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.21	Sicurezza dei servizi di rete (Security of network services)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.22	Segregazione delle reti (Segregation of networks)	**Sì**	Applicabile se sono presenti reti distinte per uffici, ospiti, dispositivi, apparati o servizi; da valutare in base all'architettura reale.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.23	Filtraggio web (Web filtering)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.24	Uso della crittografia (Use of cryptography)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.25	Ciclo di vita di sviluppo sicuro (Secure development life cycle)	**No**	Non applicabile al perimetro attuale se l'organizzazione non sviluppa software, non gestisce codice sorgente e non mantiene ambienti di sviluppo/test/produzione. Applicabilità da rivalutare se emergono attività di sviluppo interno o esternalizzato.	Esclusione da giustificare nel SGSI; mantenere evidenza dell'assenza di processi di sviluppo software e rivalutare in caso di modifica del perimetro o introduzione di applicazioni sviluppate ad hoc.
A.8.26	Requisiti di sicurezza delle applicazioni (Application security requirements)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.27	Principi di architettura e ingegneria sicura dei sistemi (Secure system architecture and engineering principles)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.28	Codifica sicura (Secure coding)	**No**	Non applicabile al perimetro attuale se l'organizzazione non sviluppa software, non gestisce codice sorgente e non mantiene ambienti di sviluppo/test/produzione. Applicabilità da rivalutare se emergono attività di sviluppo interno o esternalizzato.	Esclusione da giustificare nel SGSI; mantenere evidenza dell'assenza di processi di sviluppo software e rivalutare in caso di modifica del perimetro o introduzione di applicazioni sviluppate ad hoc.
A.8.29	Test di sicurezza in sviluppo e accettazione (Security testing in development and acceptance)	**No**	Non applicabile al perimetro attuale se l'organizzazione non sviluppa software, non gestisce codice sorgente e non mantiene ambienti di sviluppo/test/produzione. Applicabilità da rivalutare se emergono attività di sviluppo interno o esternalizzato.	Esclusione da giustificare nel SGSI; mantenere evidenza dell'assenza di processi di sviluppo software e rivalutare in caso di modifica del perimetro o introduzione di applicazioni sviluppate ad hoc.
A.8.30	Sviluppo esternalizzato (Outsourced development)	**No**	Non applicabile al perimetro attuale se l'organizzazione non sviluppa software, non gestisce codice sorgente e non mantiene ambienti di sviluppo/test/produzione. Applicabilità da rivalutare se emergono attività di sviluppo interno o esternalizzato.	Esclusione da giustificare nel SGSI; mantenere evidenza dell'assenza di processi di sviluppo software e rivalutare in caso di modifica del perimetro o introduzione di applicazioni sviluppate ad hoc.
A.8.31	Separazione ambienti sviluppo, test e produzione (Separation of development, test and production environments)	**No**	Non applicabile al perimetro attuale se l'organizzazione non sviluppa software, non gestisce codice sorgente e non mantiene ambienti di sviluppo/test/produzione. Applicabilità da rivalutare se emergono attività di sviluppo interno o esternalizzato.	Esclusione da giustificare nel SGSI; mantenere evidenza dell'assenza di processi di sviluppo software e rivalutare in caso di modifica del perimetro o introduzione di applicazioni sviluppate ad hoc.
A.8.32	Gestione delle modifiche (Change management)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.
A.8.33	Informazioni di test (Test information)	**No**	Non applicabile al perimetro attuale se l'organizzazione non sviluppa software, non gestisce codice sorgente e non mantiene ambienti di sviluppo/test/produzione. Applicabilità da rivalutare se emergono attività di sviluppo interno o esternalizzato.	Esclusione da giustificare nel SGSI; mantenere evidenza dell'assenza di processi di sviluppo software e rivalutare in caso di modifica del perimetro o introduzione di applicazioni sviluppate ad hoc.
A.8.34	Protezione dei sistemi durante audit e test (Protection of information systems during audit testing)	**Sì**	Applicabile ai sistemi informativi, dispositivi endpoint, account, rete, servizi cloud/PEC, archivi digitali, backup e applicativi a supporto dei processi aziendali e di commessa.	Da verificare: inventario asset, antivirus/EDR, aggiornamenti, password/MFA ove presenti, backup, logging, amministratori, firewall/rete, configurazioni, cancellazione dati, change management e controlli sui fornitori IT.

6. Evidenze minime richieste per approvazione della SoA

- Analisi dei rischi SGSI aggiornata, con criteri di probabilità/impatto, trattamento e accettazione del rischio.

- Piano di trattamento del rischio e collegamento fra rischi, controlli selezionati e responsabilità.

- Inventario degli asset informativi e tecnologici, inclusi dispositivi, account, servizi cloud, PEC, archivi, backup e fornitori IT.

- Politica per la sicurezza delle informazioni approvata dalla Direzione.

- Procedure o istruzioni operative per controllo accessi, gestione credenziali, backup, malware, aggiornamenti, incidenti, conservazione/cancellazione dati, dispositivi mobili e fornitori.

- Dichiarazione di Applicabilità approvata dalla Direzione, con motivazione delle esclusioni.

- Registro degli obblighi di conformità, con inclusione di GDPR, D.Lgs. 196/2003, obblighi contrattuali, riservatezza e proprietà intellettuale.

- Evidenze di formazione/consapevolezza del personale e istruzioni agli autorizzati al trattamento.

- Audit interno e riesame della direzione comprensivi di esiti SGSI, rischi, incidenti, prestazioni e miglioramenti.

7. Approvazione

Funzione	Nome	Data	Firma
Direzione / Rappresentante legale	Comin Davide		
Responsabile SGSI			
Responsabile IT / Fornitore IT			