ISO 27001 - Sicurezza informazioni

COMIN COSTRUZIONI GENERALI S.R.L.

Per COMIN COSTRUZIONI GENERALI S.R.L., la sicurezza delle informazioni riguarda principalmente la protezione di dati aziendali, amministrativi, tecnici, contrattuali, documentali e di cantiere. L'azienda opera nel settore costruzioni, lavori pubblici, impiantistica, manutenzioni, commercio materiali e gestione cantieri; quindi tratta informazioni sia interne sia riferite a clienti, fornitori, dipendenti, subappaltatori, commesse e documentazione tecnica.

Aree da considerare

Area	Aspetti da considerare
Informazioni critiche	Contratti, offerte, preventivi, computi metrici, documenti di gara, documentazione SOA, documenti ISO, documenti di cantiere, POS, DVR, piani sicurezza, documenti ambientali, formulari rifiuti, fatture, dati contabili, dati clienti, dati fornitori, dati dipendenti e consulenti.
Dati personali trattati	Dati di dipendenti, clienti, fornitori, subappaltatori, professionisti, consulenti, referenti di cantiere e soggetti coinvolti nelle commesse. Devono essere gestiti in conformita al GDPR.
Sistemi informatici utilizzati	PC aziendali, notebook, smartphone, email, PEC, software gestionali, software contabili, software per computi e cantieri, cartelle condivise, eventuale server locale, NAS, cloud, backup, stampanti/scanner e dispositivi mobili usati in ufficio o in cantiere.
Posta elettronica e PEC	La PEC societaria risulta cominsrl@arubapec.it. Per ISO 27001 occorre proteggere email e PEC da accessi non autorizzati, phishing, malware, perdita credenziali, invii errati e conservazione non controllata dei documenti.
Accessi e autorizzazioni	Deve essere definita una matrice degli accessi: chi puo accedere a contabilita, documenti del personale, documenti tecnici, documenti di cantiere, PEC, email, gestionali, cloud, backup e archivi documentali.
Password e autenticazione	Devono essere previste regole minime per password robuste, divieto di credenziali condivise, cambio password in caso di rischio, autenticazione multifattore dove possibile e gestione sicura degli account amministrativi.
Backup e ripristino	E necessario definire frequenza dei backup, sistemi inclusi, responsabile, conservazione, protezione da ransomware, eventuale copia esterna/cloud e test periodico di ripristino.
Dispositivi mobili e lavoro fuori sede	I tecnici e il personale di cantiere potrebbero utilizzare smartphone, tablet o notebook per foto, documenti, email, ordini, report e comunicazioni. Occorre disciplinare blocco schermo, protezione dispositivi, aggiornamenti, smarrimento e cancellazione dati.
Documenti cartacei	In edilizia sono ancora rilevanti documenti fisici come contratti, POS, DDT, formulari, disegni, schede tecniche, documenti del personale e documenti amministrativi. Devono essere definite regole di archiviazione, accesso, conservazione e distruzione sicura.
Fornitori IT e consulenti esterni	Devono essere identificati e qualificati i soggetti che accedono ai sistemi o ai dati aziendali: consulente IT, provider email/PEC, gestore cloud, consulente paghe, commercialista, consulente privacy, consulente sicurezza e altri fornitori critici.
Incidenti di sicurezza	Devono essere gestiti eventi come perdita di dispositivi, email compromessa, virus, ransomware, cancellazione accidentale dati, accesso non autorizzato, indisponibilita dei sistemi, errore di invio documenti o perdita di documentazione.
Continuita operativa	L'azienda deve poter continuare a operare anche in caso di guasto informatico, indisponibilita email/PEC, perdita dati, blocco del gestionale o attacco informatico. Servono backup, procedure di emergenza e responsabilita definite.

Rischi principali per la sicurezza delle informazioni

Rischio	Descrizione
Accesso non autorizzato ai dati aziendali	Possibile accesso improprio a documenti contabili, tecnici, contrattuali, dati del personale o dati di commessa.
Perdita o cancellazione di dati	Rischio legato a guasti hardware, errori umani, mancanza di backup, cancellazioni accidentali o malfunzionamenti software.
Phishing e compromissione email	Rischio elevato per aziende che usano email e PEC per comunicazioni con clienti, fornitori, banche, enti pubblici e stazioni appaltanti.

Rischio	Descrizione
Ransomware / malware	Possibile blocco di PC, server, documenti aziendali, contabilita, file di commessa e backup non protetti.
Uso improprio di dispositivi mobili	Smarrimento o furto di smartphone, notebook o tablet contenenti email, foto di cantiere, documenti tecnici o dati personali.
Credenziali condivise o deboli	Rischio di mancata tracciabilita, accessi impropri e impossibilita di attribuire correttamente le operazioni.
Fornitori esterni non controllati	Accessi tecnici o amministrativi da parte di consulenti IT, gestionali, cloud, paghe o commercialista senza adeguate regole contrattuali e di sicurezza.
Gestione non controllata dei documenti cartacei	Rischio di perdita, consultazione non autorizzata o smaltimento non sicuro di documenti contenenti dati personali, tecnici o contrattuali.
Mancata classificazione delle informazioni	Assenza di regole per distinguere documenti pubblici, interni, riservati o critici.
Assenza di procedure per incidenti IT	Ritardi nella risposta a malware, perdita dati, violazioni, errori di invio o compromissioni email.

Controlli ISO 27001 consigliati

Controllo	Applicazione pratica
Inventario asset informativi	Elenco di PC, notebook, smartphone, server, NAS, cloud, software, email, PEC, archivi cartacei e documenti critici.
Classificazione delle informazioni	Suddivisione minima in: pubblico, interno, riservato, critico.
Gestione accessi	Account personali, autorizzazioni per ruolo, rimozione accessi quando una persona cambia mansione o termina il rapporto.
Policy password e MFA	Password robuste, MFA su email/cloud/gestionali quando disponibile, divieto di password condivise.
Backup e restore	Backup programmati, protetti, verificati e testati periodicamente.
Protezione endpoint	Antivirus/EDR, aggiornamenti sistemi, protezione da malware e controllo dispositivi.
Gestione email e PEC	Regole contro phishing, allegati sospetti, invio documenti riservati, conservazione e accessi alla PEC.
Sicurezza dispositivi mobili	Blocco schermo, PIN/password, aggiornamenti, cifratura dove possibile, procedura in caso di furto o smarrimento.
Gestione fornitori IT	Contratti, accordi di riservatezza, nomine privacy/GDPR se necessarie, controllo accessi amministrativi e responsabilita su backup/sistemi.
Gestione incidenti	Procedura per segnalare, registrare, valutare e risolvere incidenti informatici o violazioni dati.
Continuita operativa	Piano minimo per recuperare documenti, email, PEC, dati contabili e file di commessa in caso di indisponibilita.
Formazione del personale	Sensibilizzazione su phishing, password, uso email, trattamento dati personali, documenti riservati e dispositivi mobili.

Documenti/procedure ISO 27001 da predisporre

Documento / procedura	Finalita
Politica per la sicurezza delle informazioni	Definire impegni, obiettivi e responsabilita aziendali.
Inventario asset informativi	Identificare beni informativi, sistemi, dispositivi, software e archivi.
Valutazione rischi ISO 27001	Analizzare minacce, vulnerabilita, impatti e controlli necessari.

Documento / procedura	Finalita
Dichiarazione di applicabilita	Indicare i controlli ISO 27001 applicabili e le eventuali esclusioni motivate.
Procedura gestione accessi	Regolare creazione, modifica, sospensione e revoca degli account.
Procedura backup e ripristino	Definire modalita, frequenza, responsabilita e test di restore.
Procedura gestione incidenti informatici	Gestire malware, phishing, perdita dati, accessi non autorizzati e indisponibilita dei sistemi.
Procedura gestione fornitori IT	Qualificare e controllare provider, consulenti IT, cloud, PEC, software e manutentori.
Policy uso strumenti informatici	Definire regole per PC, email, internet, dispositivi mobili, cloud, password e documenti aziendali.
Procedura classificazione e gestione documenti	Proteggere documenti cartacei e digitali in base alla criticita.
Piano di continuita operativa IT	Assicurare ripresa minima delle attivita in caso di blocco sistemi o perdita dati.

KPI suggeriti per ISO 27001

KPI	Esempio di misurazione
Backup eseguiti correttamente	% backup completati / backup programmati
Test di ripristino effettuati	Numero test restore eseguiti nell'anno
Incidenti informatici registrati	Numero incidenti IT, phishing, malware, perdita dispositivi
Tempo di risoluzione incidenti	Ore/giorni medi per chiusura incidente
Account disattivati tempestivamente	% account revocati entro tempi definiti
Dispositivi protetti da antivirus	% PC/notebook con protezione attiva
Aggiornamenti sistemi	% dispositivi aggiornati
Personale formato su cybersecurity	% lavoratori formati su phishing, password, email e dati personali
Fornitori IT qualificati	% fornitori IT valutati e contrattualizzati
Non conformita privacy/IT	Numero non conformita rilevate durante audit o controlli interni

Testo sintetico da inserire nel questionario

Per ISO 27001, le principali informazioni da proteggere riguardano dati clienti, fornitori, dipendenti, subappaltatori, documenti amministrativi, contratti, offerte, documenti di gara, documentazione tecnica, documenti di cantiere, POS, DVR, documenti ambientali, fatture, email e PEC. Gli asset informativi comprendono PC, notebook, smartphone, software gestionali, sistemi email/PEC, cartelle condivise, eventuali server o cloud, backup e archivi cartacei. I principali rischi sono accessi non autorizzati, perdita o cancellazione dati, phishing, malware/ransomware, credenziali deboli o condivise, smarrimento dispositivi mobili, fornitori IT non controllati e mancata continuita operativa. Il sistema ISO 27001 dovra prevedere inventario asset, classificazione informazioni, gestione accessi, backup, protezione endpoint, gestione incidenti, controllo fornitori IT, formazione del personale e piano minimo di continuita operativa.