Qualità

2/22
MARZO / APRILE

DAL 1971 LA RIVISTA ITALIANA PER I PROFESSIONISTI DELLA QUALITÀ E DEI SISTEMI DI GESTIONE

ITALIAN JOURNAL OF QUALITY & MANAGEMENT SYSTEMS

aicq
Associazione Italiana Cultura Qualità

SPECIALE

Integrazione nelle costruzioni:

sostenibilità chiama digitalizzazione

MV EDIZIONI

sommario

Qualità 2/2022
MARZO-APRILE

Sulla sicurezza delle informazioni nel settore costruzioni

ANTONIO LORENZO RASSU
Vice Presidente Comitato Qualità del Software dell'AICQ
Imprenditore e Consulente di Direzione
antonio@rassu.eu

La gestione sicura delle informazioni sta diventando sempre più un tema centrale in tutti i settori e lo è, in modo rilevante, anche nel settore delle costruzioni vista la sua importanza.

I sistemi e le tecnologie per il trattamento e la conservazione delle informazioni stanno perciò assumendo un'importanza crescente perché spesso trattano dati sensibili. Per esempio si stanno sempre più affermando metodi di progettazione digitale quale il BIM (Building Information Model) e i relativi sistemi di supporto alla gestione/conservazione delle informazioni condivise nel Common Data Environment dove viene depositato quanto compete alle singole commesse in modo che siano accessibili, secondo differenti diritti, a tutti i soggetti interessati (committenti, progettisti, fornitori, ecc.). Il CDE diventa il contenitore delle informazioni accumulate nel corso del progetto BIM e dunque il target di malintenzionati.

Sull'Information Security

Le imprese sono responsabili, per legge, della conservazione e archiviazione del patrimonio informativo: ne consegue l'esigenza di strumenti efficaci, efficienti ed integrati che consentano una gestione e consultazione dei dati senza correre rischi derivanti da accessi o attacchi esterni o interni non autorizzati.

Un moderno Sistema di Gestione deve garantire (fig. 1):

- **Riservatezza** - proprietà delle informazioni di essere note solo a chi ne ha diritto, necessaria al fine di assicurare un accesso selettivo da parte dei soli processi o utenti autorizzati a diverse tipologie di dati o informazioni o applicazioni;
- **Integrità** - proprietà delle informazioni di non essere alterabili da parte di processi o utenti non autorizzati, necessaria al fine di operare su informazioni complete, accurate ed in assenza di manomissioni;
- **Disponibilità** - proprietà delle informazioni di essere accessibili ed utilizzabili quando richiesto dai processi e dagli utenti autorizzati, finalizzata a garantire la costante funzionalità ed operatività del sistema nonostante il verificarsi di danni e/o guasti.

La normativa di riferimento si basa sul Regolamento Europeo sulla Protezione dati (679 del 2016) e sul Provvedimento del Garante della Privacy del marzo 2007 e, particolarmente importante, sul D.Lgs. 231/01 "Responsabilità amministrativa degli enti" il quale stabilisce che gli enti (imprese, società, associazioni) devono adottare adeguate modalità operative mirate alla prevenzione di reati.

Vale la pena ricordare come nacque il D.Lgs. 231/01. Nel 2001 negli Stati Uniti la società Enron improvvisamente fallì. Fino ad allora era stata considerata un modello perché nei dieci anni precedenti aveva decuplicato il suo valore passando dal business tradizionale nel campo dell'energia al lancio di spericolate ma non trasparenti operazioni finanziarie, anche se tali non apparivano. Era classificata come una delle più importanti multinazionali USA ed era considerata solidissima. Ma improvvisamente, a inizio 2001, non fu più in grado rispettare gli impegni finanziari e il titolo perse in tempi brevissimi ben il 99,7% del suo valore, bruciando così circa

130 miliardi di dollari a cui vanno aggiunti i debiti finanziari di almeno 10 miliardi. L'Arthur Andersen, che ne certificava i bilanci, non si accorse che da diversi anni venivano falsificati facendoli apparire con significativi utili mentre erano forti le perdite. A seguito di ciò la stessa Arthur Andersen, che era la più importante società di certificazione a livello mondiale con circa 170.000 dipendenti, dovette chiudere i battenti. Peraltro la Enron non fu l'unica azienda che fallì perché si scoprì che anche altre importanti società alteravano strutturalmente i bilanci. Il Congresso americano si occupò subito della cosa affidando ai parlamentari Sarbanes e Oxley la redazione di una normativa, denominata appunto Sarbanes-Oxley Act, o semplicemente SOx, che ancora oggi è in vigore.

Questi fatti produssero un notevole clamore anche in Europa e le autorità europee chiesero a tutti gli Stati di studiare una normativa atta a prevenire tali reati. Nacque il D.Lgs. 231/01 il quale stabilisce che gli amministratori dell'ente sono direttamente responsabili se, prima della commissione del reato, l'ente non ha adottato ed efficacemente attuato un Modello di Organizzazione e Gestione (il MOG) idoneo a prevenire reati. Si evidenzia che la norma fa riferimento a tutte le informazioni riservate che possono danneggiare l'impresa se finiscono nelle mani sbagliate. Negli anni il D.Lgs. 231/01 si è evoluto, per esempio includendo i reati informatici, ma le modalità con cui gli enti sono tenute a metterlo in atto sono rimaste sostanzialmente le stesse.

Il trattamento dell'informazione e la gestione dei rischi

Il sistema informativo deve essere visto come insieme organico di risorse organizzato e gestito, costituito da applicazioni, servizi, infrastrutture IT, competenze ed altre risorse utili. Sono fondamentali le persone e i processi che utilizzano o gestiscono le tecnologie e i sistemi di Information/Communication. Le persone devono essere consapevoli dei rischi che devono essere messi in evidenza attraverso un processo di valutazione (identificazione-analisi-ponderazione) che ciascuna organizzazione è tenuta a fare basandolo su criteri definiti per la valutazione del rischio nel proprio ambito. Tali valutazioni devono ripetersi sistematicamente nel tempo -per esempio annualmente- o al verificarsi di fatti imprevisti che possono incidere sulle valutazioni precedentemente fatte e devono essere comparate con le valutazioni precedenti. Il processo di valutazione deve identificare i responsabili dei rischi, cioè persona o entità con responsabilità e autorità per gestire un rischio, che devono essere dotati di adeguati budget e devono essere noti a tutte le persone che operano a qualsiasi titolo per conto delle singole organizzazioni in modo da ottimizzare la gestione dei potenziali rischi.

La fase di "identificazione" deve mirare a evidenziare i rischi associati alla perdita di riservatezza, di integrità e di disponibilità delle informazioni individuando i relativi responsabili. Si devono identificare le possibili minacce cioè qualsiasi azione, accidentale o deliberata che può potenzialmente portare alla violazione di un obiettivo della sicurezza. Le possibili minacce, classificabili in tre diverse tipologie, possono essere ad esempio:

- deliberata: intercettazioni, infiltrazione nelle comunicazioni, accessi non autorizzati, furto, errore dell'utente, uso non corretto delle risorse o addirittura danno intenzionale;
- accidentale: indirizzamento o reindirizzamento non corretto dei messaggi/comunicazioni, guasto sui sistemi di comunicazione, mancanza del personale preposto, disfunzione del software;
- ambientale: terremoto, inondazione, fulmine.

Nella successiva fase di "analisi" si valuteranno le possibili conseguenze ove tali rischi si concretizzassero tenendo conto della probabilità che ciò possa effettivamente avvenire. I danni possono essere diretti con impatto sulle risorse di supporto del sistema, quali i costi e i tempi di contrasto e ripristino (es. ricostruzione di archivi), o di rimpiazzo (es. sostituzione di HW danneggiato) oppure indiretti con impatto sulle risorse primarie (immagine, interruzione del servizio, ecc.) che normalmente sono i più gravi.

Infine vi è la fase di "ponderazione" che stabilisce la priorità fra i rischi analizzati sulla base dei criteri definiti per la valutazione del rischio.

Non ultimi sono gli aspetti riguardanti la protezione della proprietà intellettuale nel contesto dei progetti collaborativi, la responsabilità civile di trattamento dei dati e i contenziosi legali connessi che possono nascere in merito a quanto citato.

Il Modello di Organizzazione e Gestione

Per predisporre il Modello dovranno preliminarmente essere analizzati i processi, i soggetti coinvolti e i loro ruoli nel contesto aziendale e quindi procedere alla individuazione dei rischi. Si dovrà altresì definire un'organizzazione che preveda le modalità di auditing e il conseguente riporto alla direzione.

Pertanto dovranno essere messe a punto le procedure operative per condurre, ad intervalli pianificati, audit per fornire informazioni tali da permettere di verificare se il proprio sistema di gestione integrata è conforme ai requisiti propri dell'organizzazione per la Sicurezza delle Informazioni e a quelli delle norme applicabili. Nello specifico l'organizzazione deve pianificare, stabilire, attuare e mantenere uno o più programmi di audit -comprensivi di frequenze, metodi, responsabilità, requisiti di pianificazione e reporting- che devono prendere in considerazione l'importanza dei processi coinvolti e i risultati di audit precedenti. Gli auditor devono essere selezionati in modo da assicurare l'obiettività e l'imparzialità del processo di audit. La documentazione sugli

audit effettuati va conservata negli anni successivi, almeno cinque, a quello in cui è stato eseguito.

Le tre tipologie di audit sono:

- Audit interni o "di prima parte" effettuati per fini interni all'organizzazione stessa;
- Audit esterni "di seconda parte" sono effettuati da chi ha un interesse nell'organizzazione, quali i clienti o i prime contractor;
- Audit esterni "di terza parte" sono effettuati da organismi di audit esterni indipendenti, quali quelli che rilasciano certificazioni di conformità tipo ISO9001, ISO 27001.

La frequenza degli audit è suggeribile sia annuale per ciascuna tipologia o anche con frequenza maggiore qualora il livello di rischio sia considerato rilevante. Naturalmente ove emergessero rischi imprevisti che possono modificare i risultati dell'ultimo audit è opportuno programmarne tempestivamente uno nuovo. Questo vale anzitutto per gli auditor interni ma, nel caso di rischi elevati, è bene eseguire anche audit di seconda parte.

Per gli audit esterni di terza parte è opportuno prevedere sistematicamente il cambio dell'auditor (es.: ogni uno o due anni o al massimo ogni tre nel caso di strutture articolate e complesse per poter mettere a frutto in modo ottimale le conoscenze via via maturate per quelle organizzazioni).

A seguito del processo di audit si esegue il Riesame della Direzione che ne analizzerà i risultati prestando particolare attenzione ove emergessero non conformità che richiedono azioni correttive. Il riesame deve comprendere le opportunità per il miglioramento continuo e eventuali modifiche al Sistema di Gestione per assicurarne la continua idoneità, adeguatezza ed efficacia.

La sicurezza delle informazioni: dal DOCUMENTO al DATO

In un contesto organicamente strutturato come quello illustrato possono essere minimizzati i livelli di rischio nella gestione e utilizzo degli ambienti documentali e di gestione dei dati.

La gestione documentale deve prevedere la disponibilità delle documentazioni tecniche (manuali, document sharing con disegni, condizioni di utilizzo, ...) e amministrative (offerte, ordini, ...) e deve supportare la trasmissione/ricezione documenti verso fornitori/clienti (offerte, ordini, depliant, ...). La gestione degli accessi deve ovviamente rispettare tutte le norme vigenti a partire dal D.Lgs. 231/01 consentendo l'accesso solo a chi autorizzato e gestendo delle abilitazioni in modo granulare in base all'area di competenza dello specifico operatore (es.: ordini verso fornitori, listini verso clienti, ...). Deve essere prevista la tracciabilità degli accessi a ciascun documento che va conservata per almeno cinque anni.

In parallelo la Gestione delle informazioni deve essere supportata da un ambiente Common Data Environment dove vengono depositati i dati e i file relativi alla specifica commessa (di progetto, di costruzione, ecc.) perché siano accessibili, secondo differenti diritti, a tutti i soggetti interessati per il loro specifico interesse (committenti, progettisti, fornitori, imprese, ecc.).

E' previsto che l'ambiente Common Data Environment sia suddiviso in 4 differenti aree o fasi: lavorazione (produzione e variazione dei file di commessa), condivisione (comunione dei file per il loro controllo e coordinamento), pubblicazione (esposizione dei file completati e coordinati, eventualmente autorizzati dal committente), archivio (conservazione dei file nel tempo a commessa ultimata).

Considerazioni finali e conclusioni

Negli ultimi vent'anni l'Information Communication Technology ha avuto un ruolo pervasivo nella società a tutti i livelli con strumenti come internet e gli smartphone. Si sono diffusi nei vari settori tecnologici strumenti come il BIM, il sistema di Modellizzazione delle Informazioni di Costruzione, e quelli di supporto alla gestione/conservazione delle informazioni quale il Common Data Environment. Molte applicazioni hanno assunto un ruolo determinante sotto il profilo economico e sociale.

In parallelo sono cresciute le possibili disfunzioni di varia natura e le minacce intenzionali. L'insufficienza delle protezioni è terreno fertile per gli hacker che possono non solo produrre il blocco dei servizi, come per esempio avvenne alla Regione Lazio, e favorire la concorrenza sleale, a partire dagli appalti pilotati, ma anche la corruzione e perfino azioni criminose.

E' molto recente il documento *Water Security Plan* rilasciato dalla UE che illustra delle misure di sicurezza per contrastare possibili azioni ostili contro l'integrità fisica e informatica dei sistemi di approvvigionamento idrico con le misure specifiche per migliorare la protezione del sistema idrico da minacce pericolose. In Florida, nel 2021, è stato sventato un attacco informatico che avrebbe prodotto l'avvelenamento del sistema idrico di una città di 15.000 abitanti.

Questo ci deve portare a riflettere sulle potenzialità di azione di hacker particolarmente agguerriti. Prendiamo il caso di un progetto BIM di un edificio prossimo a una infrastruttura critica: è possibile che vengano di nascosto trafugate masse di informazioni contenute nel CDE e che poi vengano analizzate con finalità criminali che possono addirittura avere connotazioni terroristiche, attraverso la modifica delle informazioni presenti negli archivi senza che ci si accorga di ciò. Da un lato gli attaccanti possono trasformare l'edificio in un varco per invadere/danneggiare/sequestrare l'infrastruttura critica, dall'altro l'intera supply chain del progetto BIM può subire un danno d'immagine letale.

Peraltro pensare che la soluzione relativa a un problema

di sicurezza digitale, per quanto efficace, possa proteggere per sempre è un errore compiuto da molte organizzazioni: le tecnologie sono in continua evoluzione e di conseguenza gli strumenti di protezione ma anche le minacce.

L'organizzazione che intraprende un progetto BIM dovrebbe indirizzare la sicurezza digitale nell'ambito della gestione del progetto per assicurare che i rischi digitali siano identificati e indirizzati nel corso del progetto secondo quanto stabilito nella norma ISO 19650-5. La metodologia di gestione del progetto BIM dovrebbe richiedere che:

- gli obiettivi relativi alla sicurezza digitale facciano parte degli obiettivi del progetto BIM;
- una valutazione dei rischi digitali sia condotta in avvio del progetto BIM per identificare approccio, strategia e piano per la sicurezza digitale;
- il piano per la sicurezza digitale sia parte integrante del piano di gestione del progetto BIM.

I rischi digitali e i relativi controlli di sicurezza dovrebbero essere indirizzati e riesaminati periodicamente in ogni progetto BIM. Le responsabilità per la sicurezza digitale dovrebbero essere definite e assegnate a specifici ruoli definiti nel piano di gestione del progetto BIM.

E' perciò fondamentale un approccio metodologico organico e strutturato come quello illustrato, che nel tempo sostanzialmente non cambia, atto a prevenire e a minimizzare i malfunzionamenti che possono coinvolgere sistemi e infrastrutture molto importanti come quelli delle costruzioni. Indicare semplicemente le misure da adottare potrebbe risultare insufficiente per garantire una loro corretta e sistematica applicazione. Il crollo della Funivia del Mottarone verosimilmente non sarebbe avvenuto se si fossero applicati tali metodi di controllo.

Confidiamo che nelle organizzazioni, a partire dalla scuola, si diffondano sensibilità e competenze su una cultura della gestione integrata (qualità, ambiente, sicurezza, sostenibilità) così essenziale.

BIBLIOGRAFIA

1. UNI CEI EN ISO/IEC 27001:2017 - Tecnologie Informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione – Requisiti
2. ISO/IEC FDIS 27002 - Information security, cybersecurity and privacy protection — Information security controls
3. ISO/IEC 27005:2018 - Information technology — Security techniques — Information security riskmanagement.
4. UNI ISO 31000:2018 - Gestione del rischio - Linee guida
5. UNI EN ISO 19650 - Organizzazione e digitalizzazione delle informazioni relative all'edilizia e alle opere di ingegneria civile, incluso il Building Information Modelling (BIM) - Gestione informativa mediante il Building Information Modelling. La serie è composta dalle seguenti parti:
   - Parte 1 - stabilisce i concetti e i principi raccomandati per lo sviluppo e la gestione dei processi informativi durante l'intero ciclo di vita di qualsiasi bene edile;
   - Parte 2 - definisce i processi per la consegna e la gestione delle informazioni durante la fase di progetto e costruzione;
   - Parte 3 - definisce i processi per l'utilizzo e la gestione delle informazioni durante la fase operativa;
   - Parte 4 - dettaglierà il processo e i criteri per scambiare le informazioni in progetti e processi BIM come definiti dalle precedenti parti ISO 19650;
   - Parte 5 - definisce un approccio orientato alla sicurezza per la gestione informativa.