fowhe.com

Videosorveglianza: conformità e sicurezza

Guida operativa alla sicurezza e verifica normativa dei sistemi di videosorveglianza

Ottobre 2025

www.fowhe.com/it/sicurezza

Contenuti

Prefazione

Negli ultimi anni la videosorveglianza si è evoluta rapidamente: telecamere IP, registratori digitali e servizi cloud e di video analisi sono diventati strumenti potenti per il controllo e la sicurezza degli ambienti di lavoro e del patrimonio. Questa evoluzione porta con sé anche nuove sfide. I sistemi moderni non sono più isolati: sono costantemente connessi in rete, spesso raggiungibili anche da remoto. Questa connettività, se da un lato offre comodità e funzionalità avanzate, dall'altro apre la porta a **potenziali vulnerabilità informatiche**.

L'adozione di sistemi di videosorveglianza deve sempre avvenire nel pieno **rispetto della normativa sulla protezione dei dati personali (GDPR)** e delle disposizioni previste dallo Statuto dei Lavoratori (Legge 300/1970, art. 4). Queste regole garantiscono un equilibrio tra l'esigenza di sicurezza e la tutela dei diritti e della dignità dei lavoratori, promuovendo un uso responsabile e trasparente della tecnologia.

Questo documento rappresenta una breve guida all'implementazione dei livelli essenziali di sicurezza e contemporaneamente fornisce delle checklist per verificare la conformità normativa al GDPR e la necessità di **autorizzazione da parte dell'Ispettorato Nazionale del Lavoro**.

La videosorveglianza aumenta la sicurezza aziendale solo se gestita con responsabilità, nel rispetto del GDPR e dello Statuto dei Lavoratori, garantendo trasparenza, tutela e fiducia reciproca.

Cybersecurity

La crescente integrazione dei sistemi di videosorveglianza con reti IP e infrastrutture IT espone questi dispositivi a potenziali vulnerabilità informatiche. Telecamere, NVR, server e piattaforme cloud possono essere soggetti a accessi non autorizzati, malware, attacchi DDoS o intercettazioni dei flussi video.

Una corretta strategia di cybersecurity deve prevedere l'adozione di protocolli sicuri (HTTPS, VPN), la segmentazione delle reti, l'autenticazione a più fattori, la gestione centralizzata degli accessi e l'aggiornamento costante del firmware e dei sistemi.

Ecco un elenco delle principali vulnerabilità dovute ad errori umani.

Password predefinite

L'uso delle credenziali di fabbrica ("admin/admin", "1234", ecc.) è ancora una delle vulnerabilità più diffuse. Queste password sono facilmente reperibili online e consentono a chiunque di accedere al dispositivo. In ambito tecnico, si tratta di un problema di autenticazione debole che può essere evitato con policy di password robuste e un controllo periodico degli accessi.
Molti dispositivi vengono installati senza modificare le credenziali di fabbrica. Queste informazioni, spesso pubbliche, consentono a chiunque di accedere al sistema da remoto.

Accessi cloud non protetti

Molti dispositivi consentono la visualizzazione da remoto tramite servizi cloud. Tuttavia, se la connessione non utilizza protocolli sicuri (HTTPS o VPN) o manca l'autenticazione a due fattori, un attaccante può intercettare le comunicazioni o violare l'account. È fondamentale che la trasmissione dei dati avvenga in forma cifrata.

Firmware non aggiornati

Ogni dispositivo elettronico contiene un firmware, ovvero il software interno che ne gestisce il funzionamento. Se non viene aggiornato, può contenere vulnerabilità note. Gli aggiornamenti servono proprio a correggere questi problemi di sicurezza, riducendo la superficie d'attacco.

Reti non protette

Le telecamere spesso condividono la rete aziendale con altri dispositivi. Se la rete non è segmentata o non è protetta da firewall, un attacco su un singolo dispositivo può compromettere l'intera infrastruttura. In termini tecnici, parliamo di un rischio di propagazione laterale o lateral movement.

Esempio pratico "Il DVR compromesso"

In un'azienda di medie dimensioni, un DVR connesso alla rete Internet era stato configurato con la password predefinita.

Un bot automatico ha individuato il dispositivo in poche ore tramite una scansione globale e ha ottenuto l'accesso completo al sistema. L'attaccante ha potuto visualizzare le telecamere interne, scaricare registrazioni e sfruttare il DVR per lanciare ulteriori attacchi informatici verso l'esterno.

L'incidente è stato scoperto solo dopo che il traffico di rete è aumentato improvvisamente. Oltre alla violazione dei dati personali, l'azienda ha dovuto affrontare la temporanea sospensione dell'impianto e la segnalazione al Garante per la protezione dei dati personali. Una semplice modifica delle credenziali e l'uso di una VPN avrebbero impedito l'intera catena di eventi.

Compliance GDPR

La protezione dei dati video rientra negli obblighi previsti dal GDPR (Regolamento UE 2016/679), imponendo la cifratura dei contenuti, la limitazione dei diritti di accesso ed il monitoraggio degli eventi di sicurezza. L'obiettivo è garantire la resilienza, l'integrità e la disponibilità delle informazioni, assicurando che i sistemi di videosorveglianza contribuiscano alla sicurezza aziendale senza introdurre nuovi rischi. Poiché le immagini costituiscono dati personali, il loro trattamento deve rispettare il regolamento e tenere conto delle disposizioni previste dallo Statuto dei Lavoratori, che tratteremo nel prossimo paragrafo.

Principi e basi giuridiche

Ogni trattamento di dati deve basarsi su una base giuridica e rispettare principi come liceità, trasparenza, proporzionalità e limitazione della finalità.
Nel caso della videosorveglianza, la base più comune è il legittimo interesse del titolare del trattamento, come la tutela del patrimonio aziendale o la sicurezza dei locali, che deve tuttavia essere bilanciato con i diritti e le libertà delle persone riprese.

Informazione e trasparenza

Le persone devono essere informate chiaramente della presenza delle telecamere tramite cartelli ben visibili, collocati prima dell'area videosorvegliata. Devono indicare il titolare del trattamento, le finalità e le modalità per accedere all'informativa completa. La trasparenza è fondamentale per garantire consapevolezza e correttezza nel trattamento delle immagini.

Conservazione e sicurezza dei dati

Le registrazioni devono essere conservate solo per il tempo necessario al raggiungimento delle finalità dichiarate, di norma non oltre 72 ore, salvo esigenze specifiche (ad esempio in caso di indagini o eventi particolari).
L'azienda deve adottare misure di sicurezza adeguate per evitare accessi non autorizzati, come limitazioni all'accesso, password sicure e sistemi di cifratura.

Ruoli e responsabilità

Il titolare del trattamento (l'azienda) è responsabile della conformità al GDPR e deve poter dimostrare di rispettarlo (principio di accountability). È consigliabile designare un Responsabile della Protezione dei Dati (DPO) e fornire ai lavoratori una formazione adeguata sulla privacy e la sicurezza dei dati.

Autorizzazione Art.4 legge 300/1970

L'articolo 4 dello Statuto dei Lavoratori (Legge 300/1970) regolamenta l'uso dei sistemi di videosorveglianza e di altri strumenti che possono comportare un controllo a distanza dell'attività dei dipendenti. La norma non vieta tali sistemi, ma impone condizioni rigorose per garantire il rispetto della dignità e della riservatezza dei lavoratori.

Finalità ammesse

I sistemi di videosorveglianza possono essere installati solo per determinate finalità, ritenute legittime dalla legge quali: esigenze organizzative e produttive, esigenze di sicurezza del lavoro, tutela del patrimonio aziendale.
Al di fuori di questi casi, l'installazione di impianti di videosorveglianza è considerata illecita. In particolare, non è mai ammesso l'uso di telecamere per monitorare direttamente la produttività o il comportamento dei dipendenti durante l'attività lavorativa.

Quando è necessaria l'autorizzazione

L'installazione di un impianto di videosorveglianza è sempre soggetta a valutazione preventiva, ma l'autorizzazione vera e propria è obbligatoria nei seguenti casi:

- quando le telecamere possono riprendere aree in cui operano i lavoratori, anche solo potenzialmente, e quindi è possibile un controllo indiretto sull'attività lavorativa.
- quando l'impianto non è installato esclusivamente per fini personali o di sicurezza privata, ma riguarda l'ambiente di lavoro aziendale.
- quando non è possibile raggiungere un accordo sindacale (nelle aziende con rappresentanza sindacale interna o territoriale).

L'autorizzazione non è necessaria solo se le telecamere sono installate solo per scopi di sicurezza, in aree non accessibili ai dipendenti (es. magazzini chiusi, aree esterne, parcheggi), oppure se si tratta di strumenti utilizzati direttamente dal lavoratore per svolgere la propria attività (es. GPS su veicoli aziendali o smartphone aziendali), ma in questi casi valgono comunque i principi di informazione e trasparenza

Come si richiede l'autorizzazione

Se non si raggiunge un accordo con le rappresentanze sindacali, l'azienda deve chiedere autorizzazione all'Ispettorato Territoriale del Lavoro (ITL) competente per sede. La procedura è la seguente:

Predisporre un'istanza formale indirizzata all'ITL, indicando:

- le motivazioni dell'installazione (es. esigenze di sicurezza, tutela del patrimonio, organizzazione del lavoro);
- la descrizione tecnica dell'impianto (numero e posizionamento delle telecamere, modalità di registrazione, tempi di conservazione);
- le misure adottate per tutelare la privacy dei lavoratori (es. oscuramento di aree sensibili, limiti di accesso alle immagini);
- copia dell'informativa ai sensi del GDPR.

Devono essere allegate planimetrie e schemi dell'impianto, con l'indicazione delle aree riprese e l'orientamento delle telecamere.

Si deve quindi attendere il rilascio del provvedimento autorizzativo da parte dell'Ispettorato del Lavoro prima di procedere con l'attivazione del sistema.

Sanzioni in caso di mancata autorizzazione

L'installazione e l'utilizzo di impianti audiovisivi senza accordo sindacale o senza autorizzazione dell'Ispettorato costituisce **illecito penale (art. 38 dello Statuto dei Lavoratori)** e può comportare ammenda o arresto per il datore di lavoro e/o sanzioni amministrative per violazione del GDPR, se vengono trattati dati personali in modo illecito.

Uso delle immagini e tutele

Le registrazioni devono essere utilizzate solo per le finalità dichiarate e nel rispetto della normativa sulla privacy. Ogni forma di controllo occulto o sproporzionato è vietata. La legge prevede sanzioni per il datore di lavoro in caso di violazioni, incluse la nullità delle prove e sanzioni penali o amministrative.

Controlli indiretti e strumenti di lavoro

La giurisprudenza ha chiarito che anche gli strumenti di lavoro che consentono un controllo indiretto sull'attività del lavoratore — ad esempio dispositivi digitali, software o sistemi GPS — rientrano nell'ambito dell'art. 4. Anche in questi casi, l'azienda deve agire con trasparenza, informando i lavoratori e rispettando le procedure di autorizzazione previste.

Checklist operativa

A conclusione della guida vi proponiamo una checklist che comprende la verifica sia degli aspetti legati alla sicurezza che della compliance al GDPR ed alla legge sulla tutela dei lavoratori. Questa checklist può essere utilizzata come strumento di autovalutazione della rispondenza del vostro sistema.

Sicurezza e Finalità

- Le finalità dell'impianto sono chiaramente definite (es. sicurezza, tutela del patrimonio, controllo accessi)?
- Le telecamere non sono utilizzate per il controllo a distanza dell'attività dei lavoratori?
- Le aree sorvegliate sono adeguate e proporzionate rispetto alle finalità dichiarate?
- Le telecamere non riprendono spogliatoi, bagni o zone di pausa?

Conformità allo Statuto dei Lavoratori (Art. 4 L. 300/1970)

- È stato raggiunto un accordo sindacale o ottenuta l'autorizzazione dell'Ispettorato Territoriale del Lavoro (ITL)?
- È disponibile la documentazione autorizzativa in caso di controlli ispettivi?
- I lavoratori sono stati informati per iscritto dell'esistenza e delle finalità del sistema?

Conformità al GDPR

- È stata redatta una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) se il trattamento comporta rischi elevati?
- È stata fornita un'informativa completa ai sensi dell'art. 13 GDPR (cartelli e documentazione interna)?
- È definito un tempo di conservazione limitato (in genere non oltre 72 ore, salvo esigenze particolari)?
- Sono state definite le figure autorizzate all'accesso alle registrazioni?
- È stato nominato un Responsabile del Trattamento (Data Processor) se il servizio è gestito da terzi?
- Le registrazioni sono crittografate e protette da credenziali sicure?

Cyber Security

- Il sistema è protetto da firewall, antivirus e connessioni sicure (HTTPS/VPN)?
- Le password dei dispositivi sono complesse e aggiornate periodicamente?
- Il software delle telecamere e del server è costantemente aggiornato?
- Sono presenti backup periodici e procedure di risposta a incidenti di sicurezza?
- Gli accessi ai dati video sono tracciati e registrati?

Documentazione e Trasparenza

- È disponibile un registro dei trattamenti aggiornato ai sensi dell'art. 30 GDPR?
- È stato designato un DPO (Data Protection Officer), se previsto?
- L'azienda ha predisposto procedure interne per la gestione di richieste di accesso o cancellazione dei dati?
- Sono affissi cartelli informativi visibili in tutte le aree videosorvegliate.?

Chi siamo

www.fowhe.com/it/index

Fowhe è dal 2007 fornitore di servizi ed operatore di TLC, focalizzato sul settore business che progetta ed implementa soluzioni IT, favorendo la transizione digitale delle piccole e medie imprese e delle PA del territorio. Il team di Fowhe è costituito da **Ingegneri informatici, Ingegneri delle telecomunicazioni**, **tecnici specializzati nel settore dei sistemi e delle reti**.
Fowhe dispone di risorse di rete e datacenter sul territorio Pugliese e, secondo l'analisi 2025 di Plimsoll Italia sulle 524 aziende del settore, Fowhe si posiziona 31a tra le imprese del settore con maggior margine di profitto (www.plimsoll.it).
E' classificato come soggetto importante dall'Agenzia per la Cybersicurezza Nazionale (ACN), ai sensi della direttiva NIS2 e il Decreto Legislativo 138/2024.

NAMEX ROMA INTERNET EXCHANGE POINT RIPE NCC RIPE NETWORK COORDINATION CENTRE ASSOProvider

1 E' operatore di TLC

Fowhe è autorizzata dal 2007 ai sensi dell'articolo 25 del Decreto Legislativo n. 259/2003 e ss.mm.ii. del Codice delle comunicazioni elettroniche, è titolare di autorizzazione generale per l'offerta al pubblico di servizi di comunicazione elettronica, è titolare di autorizzazione generale per l'installazione e la fornitura di reti pubbliche di comunicazioni.

2 E' Autonomous System

Fowhe è Autonomous System con numero AS60443, presente nei principali Internet Exchange Point nazionali e dispone di risorse IT/TLC sul territorio Pugliese. Questo gli consente di essere un operatore di rete indipendente che implementa ed eroga i migliori servizi disponibili.

3 E' parte dell'ecosistema di Internet

Fowhe è socia dei consorzi e delle associazioni che rappresentano l'ecosistema di Internet come il Roma Internet Excenge Point (NAMEX), il Regional Internet Registry for Europe (RIPE), l'Associazione di Provider Internet Indipendenti Italiani (Assoprovider).

4 E' costantemente aggiornata

Il Team di Fowhe partecipa ai principali eventi e conferenze che interessano il mondo dell'informatica e delle telecomunicazioni restando sempre al passo con le innovazioni e le tendenze del settore.

fowhe.com

Contatti

Website
www.fowhe.com/it/index

E-mail
business@fowhe.com

Telefono
+ (39) **06 90285189**

Social Media
www.linkedin.com/company/fowhe-s-r-l-

Head quarter
Via A. Salandra 18 - ROMA

Sedi operative
Via Assunta 19 - MARTANO (LE)

Viale Donato De Leonardis zona ASI - BARI