Studio Violi S.r.l.
Organizzazione con sistema di gestione certificato secondo la norma ISO 9001: 2015

2003-2025
anni di consulenza per le imprese

ISO 9001
BUREAU VERITAS
Certification
IT334467

I Partners dello Studio

Giorgio Violi	tel: 3386132605	givioli@gmail.com
Alberto Sant'Unione	tel: 3409125853	santunionea@gmail.com

Qualità Sicurezza Privacy Ambiente Risk Management
Responsabilità Amministrativa 231 Etica Consulenza e Audit per la Direzione

Organizzazione con sistema di gestione certificato secondo la norma ISO 9001: 2015 per Progettazione ed erogazione di servizi di consulenza relativa ai Sistemi di Gestione Aziendale Qualità, Ambiente, Sicurezza, Etica; servizi di consulenza in ambito Privacy, Modelli Organizzativi, Sicurezza sul lavoro, Consulenza di Direzione e sostenibilità ESG

2025 Novembre **Il nostro punto di vista su…** *Anno 18 – 2° sem*

Periodico di informazione per i CLIENTI dello STUDIO VIOLI

Indice delle NOTIZIE (N)

SENTENZE DI CASSAZIONE SUL LAVORO

1. Sul sito http://www.dottrinalavoro.it/argomento/giurisprudenza-c/corte-di-cassazione-c sono presenti le ultime sentenze di Cassazione relative al lavoro

AFORISMA DEL MESE

"L'unico vantaggio competitivo sostenibile consiste nella capacità di apprendere e di cambiare più rapidamente degli altri"

Philip Kotler (economista statunitense)

Foto ing. Sant'Unione

"Caccia all'estintore"

Notizie

- N1) Privacy: In arrivo le semplificazioni su privacy e digitale, ma beneficiarne sarà complicato

Le semplificazioni su privacy e digitale sono finalmente state proposte dalla Commissione Europea, che lo scorso 19 novembre ha ufficialmente presentato il "Digital Omnibus",

ovvero la proposta legislativa che ha come obiettivo dichiarato quello di ridurre il carico burocratico di almeno il 25% per tutte le imprese e del 35% per le PMI, cercando così di fornire una risposta alle preoccupazioni espresse nel rapporto Draghi sulla competitività europea, anche se leggendo il testo sorge più che il semplice dubbio che a beneficiarne maggiormente saranno le grandi aziende tecnologiche e non quelle paneuropee.

Quello messo in cantiere dall'UE non è, infatti, un semplice snellimento della burocrazia, ma un **massiccio intervento che è destinato a produrre un vero e proprio cambio di paradigma nella protezione dei dati** come l'abbiamo vista in Europa negli ultimi trent'anni, che anziché concentrarsi su divieti e diritti, spiana adesso la strada all'intelligenza artificiale e al business del digitale.

Basti pensare che, una volta approvata definitivamente la riforma, le aziende tecnologiche potranno legittimamente allenare gli algoritmi delle loro intelligenze artificiali prendendo i dati personali presenti su social network, piattaforme online e siti web senza necessità di ottenere alcun consenso dagli utenti. E ci saranno meno vincoli anche per gli sviluppatori di sistemi di AI, che potranno processare legalmente categorie sensibili di dati come informazioni dalle quali è possibile dedurre convinzioni politiche o religiose, etnia o salute, per finalità di training e operatività.

Con le semplificazioni, gli utenti smetteranno, inoltre, di visualizzare continuamente i fastidiosi banner dei cookie, perché basterà indicare il proprio consenso con un solo click e salvare le proprie preferenze permanenti nel proprio browser e nel sistema operativo del dispositivo elettronico. E anche il perimetro dei dati soggetti agli **adempimenti del GDPR sarà ridotto, perché saranno considerati "dati personali" solo quelle informazioni che permettono di identificare direttamente una persona fisica (come il nome e cognome), e non più quelle che permettono di risalire alla sua identità anche indirettamente. In pratica, basterà ricorrere a pseudonimi come "user_123456" per essere esentati dagli adempimenti sulla privacy.**

Tra le varie novità, sono in arrivo anche semplificazioni per imprese e pubbliche amministrazioni che a seguito **di un data breach potranno effettuare le notifiche richieste con un'unica operazione valida sia ai fini del GDPR che di tutte le altre normative in materia.** Per le aziende tecnologiche sarà invece più semplice intrufolarsi nei nostri smartphone e computer, in quanto potrebbero essere autorizzate a estrarre dati direttamente dai dispositivi degli utenti per scopi di sicurezza, con tutte le conseguenti criticità in materia di cybersecurity, nonché le legittime perplessità che possa comportare il fatto di sapere che qualcuno potrà potenzialmente accedere a una miriade di informazioni che custodiamo gelosamente nei nostri apparecchi.

Ciliegina sulla torta, se dopo il GDPR erano fioccati tutta una serie di altri regolamenti dall'UE per disciplinare ulteriormente la gestione dei dati, con il Digital Omnibus è prevista una riorganizzazione normativa che comporta un "taglia e cuci" di vari atti normativi per abrogarne alcuni e accorparne altri che neanche avevano fatto in tempo ad entrare pienamente in vigore o ad essere metabolizzati dagli addetti ai lavori della compliance aziendale.

Nel complesso, è quindi un pacchetto di misure che potrà fare felici quelli che affermano di non avere niente da nascondere e le aziende che considerano la privacy una burocrazia inutile, ma neanche per loro è tutto

oro quello che luccica, perché la sburocratizzazione e le semplificazioni tecnologiche potrebbero essere più complicate di quanto si possa pensare.

Infatti, se con le semplificazioni proposte dalla Commissione Europea il quadro normativo si orienta verso maggiore flessibilità nell'utilizzo dei dati personali per finalità di AI, la responsabilità dei professionisti della privacy e della cybersecurity diventa paradossalmente ancora più gravosa per districarsi nei nuovi scenari che si affacciano all'orizzonte delineandosi profondamente diversi da quelli attuali, e le aziende non potranno più fare affidamento su espliciti divieti normativi tediosi ma comunque certi, e dovranno esercitare un continuo bilanciamento tra opportunità di business e protezione dei diritti.

Inoltre, migliaia di imprese che avevano investito soldi e risorse per adeguarsi alle prescrizioni attuali dovranno adesso rimettere le mani sui loro modelli organizzativi per aggiornarli alle semplificazioni, senza pensare a modulistica e montagne di documentazione formalistica che presto potrebbe non servire più, e che necessiterà perciò di una revisione generale per non risultare erronea o fuorviante. Perfino chi aveva virtuosamente inserito un Data Protection Officer dovrà rifare le opportune valutazioni per verificare se sarà sempre necessario mantenerlo o organizzarsi per farne a meno. **Tirando le somme, per beneficiare delle semplificazioni occorrerà rimboccarsi le maniche e avviare un'accurata due diligence per accertare cosa sarà possibile smantellare di ciò che era stato precedentemente fatto, e cosa invece deve essere mantenuto e/o aggiornato.**

Pertanto, almeno in una prima fase di transizione, le semplificazioni rischieranno di penalizzare chi aveva investito risorse e denaro per adeguarsi, e daranno invece sollievo a chi finora non aveva fatto niente per adeguarsi, o peggio ancora, chi delle regole europee se ne era infischiato, e a questo riguardo forse lo sguardo andrebbe rivolto oltreoceano.

-N2) Privacy: Controllo dipendenti: nuova funzione di localizzazione WiFi di Microsoft Teams

Microsoft Teams attiva la rilevazione visibile della presenza in ufficio per le connessioni alla rete aziendale: le implicazioni sul fronte privacy.

È una specie di cartellino digitale automatico il nuovo tool sulla presenza in sede inserito in Microsoft Teams.

La nuova funzionalità **sarà attiva nel 2026 e svelerà da dove si sta collegando un dipendente in base alla rete a cui è connesso**.

Nel momento in cui accende il pc e ci si collega al WiFi, infatti, apparirà o meno la dicitura "in ufficio" se si è all'interno del perimetro della rete aziendale.

L'obiettivo è quello di rendere più facile l'organizzazione di riunioni o altre forme di collaborazione interna dando un'immediata visibilità sul modo in cui sono posizionate le persone, segnalando ad esempio chi è in smart working e chi invece in sede.

Il sistema Microsoft è in grado di riconoscere tutte le reti di connessione aziendale, mentre non registrerà l'utente come presente nel momento in cui si troverà per esempio a casa o comunque in un luogo con coperto dalla rete aziendale. Non ci sono altre forme di localizzazione se non l'indicazione relativa sulla presenza fisica in un luogo di lavoro registrato come tale sulla rete aziendale. Secondo la roadmap ufficiale di M365, l'aggiornamento sarà rilasciato a gennaio 2026.

Quando gli utenti si connettono al Wi-Fi della propria organizzazione, Teams sarà presto in grado di aggiornare automaticamente la propria posizione di lavoro per riflettere l'edificio da cui lavorano. Questa funzionalità sarà disattivata per impostazione predefinita. Gli amministratori del tenant decideranno se abilitarlo e richiederanno agli utenti finali di aderire.

Si tratta di un meccanismo assimilabile a quello del cartellino dematerializzato che registra l'orario di ingresso e di uscita dei dipendenti. Tuttavia, in questo caso il sistema è più invasivo perché monitora la situazione in modo costante. L'opzione non si attiva automaticamente in tutte le aziende che usano Teams, ma sono il reparto IT o i decisori aziendali a decidere su utilizzarla o meno. E ogni lavoratore deve poi renderla operativa.

Per la compatibilità con le normative sul controllo a distanza sul luogo di lavoro, come per tutti i dispositivi di questo genere, dovrebbe essere necessario anche il consenso informato del lavoratore e, nei casi più complessi, anche un accordo sindacale. Bisognerà infatti capire se la segnalazione rivelerà la sola presenza negli uffici o se potranno essere indicate anche le reti private, ad esempio dei dipendenti che si trovano in lavoro agile.

L'articolo 4 dello Statuto dei Lavoratori stabilisce infatti che «gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali». Per le aziende che non hanno rappresentanza sindacale interna, vanno stipulati accordi territoriali.

- N3) Privacy: Licenziato chi visiona e preleva dati personali altrui accedendo al database aziendale per finalità diverse da quelle lavorative; Poltronesofà sotto attacco hacker: compromessi i dati personali dei clienti

Licenziato chi visiona e preleva dati personali altrui accedendo al database aziendale per finalità diverse da quelle lavorative. Con la sentenza n. 28887 depositata il 1° novembre 2025, la Corte di Cassazione ha ribadito un principio ormai consolidato riguardante l'accesso abusivo a sistema informatico, aggiungendo, però, la rilevanza della violazione del codice di comportamento del pubblico dipendente, del codice di condotta interno all'azienda e dall'art. 64 ccnl di comparto con sanzione espulsiva prevista dall'articolo 18, comma 8.

Una dipendente di una Azienda Ospedaliera Universitaria è stata licenziata per aver eseguito 30 accessi illeciti alla banca dati dei fascicoli sanitari elettronici, consultandoli senza alcuna giustificazione o ragione di servizio. Anzi, in taluni casi l'accesso ha riguardato i fascicoli di persone, segnatamente i suoi vicini di casa, con le quali la donna aveva in corso controversie giudiziarie.

Il Tribunale ha ritenuto legittimo il massimo provvedimento disciplinare, confermato anche dalla Corte di Appello. Ciò nonostante, la donna ha inteso ricorrere anche dinanzi la Suprema Corte.

Secondo i giudici, però, "l'accesso al sistema informatico aziendale non può essere considerato lieve quando realizzato per finalità personali o comunque non riconducibili a esigenze di servizio" e, per tale ragione, il comportamento è da ritenersi di gravità tale da non consentire la prosecuzione neppure provvisoria del rapporto di lavoro, potendosi così ritenere proporzionata la massima sanzione disciplinare.

Infatti, la violazione di cui all'articolo 615ter c.p., hanno ribadito gli Ermellini, si configura tutte le volte che un soggetto acceda ad un sistema informatico per fini diversi da quelli per i quali gli è stato facoltizzato l'accesso.

Ciò significa che a nulla rileva la conoscenza della password da parte dell'agente per averla ricevuta dall'interessato – il quale gli avrebbe quindi fornito una implicita o esplicita autorizzazione – qualora la condotta incriminata porti ad un esito certamente in contrasto con la volontà del titolare della banca dati. Con tale comportamento si ottiene infatti un risultato che non coincide con la volontà del suddetto, e che è esorbitante rispetto a qualsiasi possibile ambito autorizzatorio, vale a dire la conoscenza di informazioni riservate e dati personali sensibili.

Allo stesso modo, del tutto ininfluente è la motivazione che giustificherebbe la conoscenza e l'utilizzo delle informazioni così acquisite. Il reato, insomma, si configura non soltanto quando il colpevole violi le misure di sicurezza poste a presidio del sistema informatico, ma anche quando, pur legittimato all'accesso per ragioni di servizio, vi si mantenga, ovvero consulti o utilizzi le informazioni, per ragioni diverse da quelle di servizio, uniche circostanze per le quali era stato inizialmente autorizzato all'ingresso.

Poltronesofà sotto attacco hacker: compromessi i dati personali dei clienti. Nel pieno di un anno segnato da un aumento significativo degli attacchi informatici, Poltronesofà ha comunicato ai propri clienti di essere stata vittima di un attacco ransomware avvenuto il 27 ottobre 2025.

L'azienda sta inviando in queste ore una mail che, ai sensi del Gdpr, rappresenta l'obbligo di notifica previsto quando una violazione dei dati personali può esporre gli interessati a un rischio elevato. La portata dell'incidente è potenzialmente ampia, considerando la dimensione della base clienti di una delle principali catene italiane dell'arredamento.

Cosa è accaduto e quali dati sono stati compromessi - Nella comunicazione ufficiale, Poltronesofà spiega che soggetti non autorizzati hanno compromesso i server del gruppo, cifrando i file e rendendo indisponibili le macchine virtuali ospitate. Le informazioni potenzialmente esposte includono nome, cognome, codice fiscale, indirizzo postale, indirizzo e-mail e numero di telefono cellulare. Un dato importante per i clienti è che non risultano coinvolti dati bancari né numeri di carte di credito.

L'azienda specifica che questi dati "potrebbero essere stati interessati", una formula che indica che le analisi forensi sono ancora in corso. Resta da chiarire se i file siano stati solo cifrati internamente o anche copiati all'esterno verso infrastrutture controllate dagli attaccanti, come avviene di frequente nelle più recenti campagne di ransomware basate sulla cosiddetta doppia estorsione.

La dinamica dell'attacco e le prime contromisure - La ricostruzione fornita da Poltronesofà ricalca il modello tipico di un attacco ransomware: un malware penetra nella rete aziendale, blocca sistemi e applicazioni dopo un possibile furto di dati e i criminali chiedono un riscatto per decriptare i file o evitare la pubblicazione delle informazioni sottratte.

Poltronesofà afferma di avere contenuto rapidamente l'incidente, con il supporto di specialisti di cybersicurezza, isolando le macchine compromesse, rafforzando le difese e avviando un'analisi tecnica approfondita. In base alle verifiche effettuate finora, l'azienda dichiara che non sono emerse criticità ulteriori rispetto al giorno dell'attacco e che non ci sono, al momento, evidenze di un utilizzo illecito dei dati.

Quali rischi corrono i clienti coinvolti di Poltronesofà - La compromissione di dati come nome, indirizzo, e-mail e numero di telefono non comporta un danno economico immediato, ma apre la strada a una serie di rischi concreti legati soprattutto a tecniche di phishing avanzato. Con queste informazioni, i criminali possono costruire comunicazioni estremamente credibili, simulando per esempio

messaggi di Poltronesofà relativi a ritardi nelle consegne, aggiornamenti d'ordine o richieste di conferma dati. È possibile anche che vengano sfruttati SMS o telefonate da finti operatori del servizio clienti o di società finanziarie collegate all'acquisto di arredamento.
Combinando queste informazioni con altri dati reperibili online o ottenuti da precedenti data breach, i truffatori possono costruire identità digitali sufficientemente solide da tentare frodi più sofisticate. Per questo motivo la stessa Poltronesofà invita i clienti a mantenere alta la soglia di attenzione, evitando di rispondere a comunicazioni inattese che richiedano dati personali o azioni urgenti, verificando l'attendibilità dei mittenti, aggiornando le password e attivando, dove possibile, sistemi di autenticazione a due fattori.
Perché l'azienda è tenuta a comunicare il data breach - La mail inviata da Poltronesofà rientra negli obblighi previsti dall'articolo 34 del Gdpr, che impone ai titolari del trattamento di informare gli interessati senza ingiustificato ritardo in caso di violazione dei dati personali potenzialmente rischiosa per diritti e libertà. Parallelamente, l'azienda deve notificare il data breach al Garante per la privacy entro 72 ore dalla scoperta. Il fatto che la società abbia scelto di comunicare direttamente con i clienti indica che l'episodio è stato classificato come incidente potenzialmente grave.
Ransomware in forte crescita in Italia - L'attacco a Poltronesofà si inserisce in un quadro in cui il ransomware continua a crescere in Italia con ritmi preoccupanti. Secondo i più recenti rapporti sulla cybersicurezza, come quello del Clusit, gli attacchi nel 2025 hanno registrato un aumento a doppia cifra rispetto all'anno precedente, con l'Italia tra i Paesi più colpiti in Europa. Cresce non solo il numero degli episodi, ma anche la loro sofisticazione, con modelli di doppia estorsione sempre più diffusi.
Negli ultimi anni sono state vittime di ransomware aziende industriali, utility, amministrazioni locali, marchi del fashion e operatori del food. L'incidente che coinvolge Poltronesofà conferma che nessun settore della grande distribuzione è immune e che anche il settore del retail dell'arredo è diventato un obiettivo sensibile per la criminalità informatica..

- N4) Sicurezza sul lavoro: Stress lavoro correlato, indicatori su lavoro da remoto e nuove tecnologie

Chi lavora da remoto lo sa: la tecnologia porta grandi vantaggi, ma può anche diventare una fonte di stress.

Essere sempre connessi, non riuscire a staccare, sentirsi isolati dai colleghi o dover gestire strumenti complessi sono situazioni comuni che finiscono per pesare sul benessere delle persone e sull'efficacia del lavoro.

Per questo la nuova metodologia Inail ha introdotto una valutazione preliminare dedicata al lavoro da remoto e all'uso delle tecnologie digitali.

Non è un passaggio complicato: si tratta di una lista di 7 indicatori chiave che riguardano la dotazione tecnologica, la formazione digitale, le modalità di coordinamento a distanza, il diritto alla disconnessione, l'individuazione delle attività compatibili con il lavoro remoto e l'informazione su salute e sicurezza.

La compilazione di questi indicatori porta a un risultato che si colloca in tre possibili fasce:

1. implementazione adeguata, in questo caso l'organizzazione ha già introdotto misure solide,
2. necessità di potenziamento, quindi alcuni aspetti richiedono attenzione mirata,
3. necessità di potenziamento sostanziale, quando il rischio di criticità è più elevato e servono azioni strutturate.

Questa analisi preliminare è preziosa perché fornisce subito un quadro chiaro della situazione senza appesantire gli adempimenti.

Tuttavia, è sempre consigliato proseguire con la valutazione approfondita, che attraverso un questionario integrato indaga in modo più dettagliato le percezioni dei lavoratori su carico tecnologico, invasione nella vita privata, conflitto casa-lavoro e qualità delle interazioni a distanza.

In questo modo l'azienda non solo fotografa il presente, ma si mette nelle condizioni di intervenire in maniera mirata, prevenendo i rischi emergenti e costruendo un ambiente di lavoro che, anche a distanza, rimanga sano, sostenibile e inclusivo.

- N5) Sicurezza sul lavoro: Manutentori antincendio qualificati: dal 26 settembre 2026 in vigore il regime ordinario

Dopo oltre quattro anni di rinvii e aggiustamenti, il percorso di qualificazione dei tecnici manutentori antincendio entra nella sua fase conclusiva.

La Circolare del Corpo Nazionale dei Vigili del Fuoco n. 14644 del 10 settembre 2025 segna la fine delle proroghe e l'avvio del regime ordinario per la qualificazione dei tecnici manutentori antincendio.
Il 25 settembre 2026 sarà quindi la data di riferimento non più prorogabile: dal giorno successivo, ogni attività di manutenzione potrà essere svolta soltanto da professionisti qualificati e iscritti nell'elenco ufficiale del Corpo Nazionale dei Vigili del Fuoco.

IL QUADRO NORMATIVO: DAL D.M. 1° SETTEMBRE 2021 ALLA PROROGA DEL 2025

Il percorso di qualificazione obbligatoria dei **tecnici manutentori antincendio** nasce con il **D.M. 1° settembre 2021** (*Decreto Controlli*), che ha introdotto i criteri generali per il controllo e la manutenzione di impianti, attrezzature e sistemi di sicurezza antincendio ai sensi dell'art. 46, comma 3, lettera a), punto 3 del **D.Lgs. 81/2008**. L'articolo 4 del Decreto Controlli stabilisce che l'attività di manutenzione dei presidi antincendio possa essere svolta solo da tecnici qualificati, previa verifica dei requisiti e superamento di un **esame presso il Corpo Nazionale dei Vigili del Fuoco**.

Dopo vari rinvii, il D.M. 15 luglio 2025 ha fissato al 25 settembre 2026 l'ultima scadenza del regime transitorio.

Come chiarito con la Circolare prot. DCPREV n.14644/2025 si tratta dell'ultima proroga concessa: dal 26 settembre 2026 potranno operare esclusivamente tecnici in possesso dell'attestato di qualificazione rilasciato ai sensi del D.M. 1/9/2021.

LA CIRCOLARE VVF DEL 10 SETTEMBRE 2025: NESSUNA NUOVA PROROGA

La circolare DCPREV prot. n. 14644 del 10 settembre 2025 del Corpo Nazionale dei Vigili del Fuoco – Direzione Centrale per la Prevenzione e la Sicurezza Tecnica conferma che **non ci saranno ulteriori proroghe**. Il documento sancisce la **conclusione delle attività di implementazione** necessarie all'operatività del sistema di qualificazione: la piattaforma informatica nazionale, la rete di sedi d'esame e la definizione del quadro formativo sono ora pienamente funzionanti.

Di conseguenza, il CNVVF dichiara **terminata la fase transitoria** e conferma che dal **26 settembre 2026** potranno svolgere attività di manutenzione antincendio **solo i tecnici manutentori antincendio qualificati**. Le precedenti modalità di gestione manuale o cartacea non saranno più ammesse, a favore di un sistema **digitale, tracciabile e uniforme** a livello nazionale.

NULLA OSTA TRANSITORI (NOT): VALIDITÀ E SCADENZA

La circolare fornisce importanti chiarimenti sui **Nulla Osta Transitori (NOT)**, ossia i provvedimenti che hanno consentito ai tecnici di operare in attesa della qualificazione definitiva:

- I NOT già rilasciati restano **validi per un anno dalla data di emissione**, ma **non oltre il 25 settembre 2026**.

- I NOT emessi **dopo il 25 settembre 2025** avranno **scadenza automatica il 25 settembre 2026**, indipendentemente dalla data di rilascio.

Dal giorno successivo, ogni attività di manutenzione dei presidi antincendio svolta senza attestato di qualificazione disciplinato dal D.M. 1° settembre 2021 costituirà violazione delle disposizioni del D.M. 1/9/2021.

IL PORTALE INFORMATICO NAZIONALE "CORPO DIGITALE-ABILITAZIONE TECNICI MANUTENTORI QUALIFICATI"

L'**Appendice A** alla circolare **14644/2025** illustra il funzionamento del **Portale Informatico "Corpo Digitale – Abilitazione Tecnici Manutentori Qualificati"**, piattaforma ufficiale del CNVVF per la gestione delle procedure di qualificazione del tecnico manutentore.

Il portale consente:

- l'invio telematico delle **istanze di qualificazione**;
- la gestione delle **sessioni d'esame** da parte dei soggetti formatori;
- l'emissione digitale degli **attestati di qualificazione** dotati di **QR-code** per la verifica immediata;
- la consultazione dello **stato delle pratiche** e dell'**elenco pubblico** dei manutentori abilitati.

Il sistema è integrato con **PagoPA** per i pagamenti e con il protocollo documentale del Dipartimento dei Vigili del Fuoco.

L'accesso avviene tramite **SPID** o **CIE**, e l'uso del portale è **obbligatorio** per tutte le fasi del processo.

COSA CAMBIA PER MANUTENTORI, IMPRESE E COMMITTENTI?

Dal punto di vista operativo, la piena attuazione del sistema comporta novità significative.

I **tecnici manutentori** che ancora operano con un Nulla Osta Transitorio devono completare il percorso di qualificazione entro la data limite del 25 settembre 2026.

Le **imprese** che offrono servizi di manutenzione devono verificare che il proprio personale sia iscritto negli elenchi ufficiali e in possesso di attestato rilasciato dal CNVVF.

I committenti pubblici e privati, invece, dovranno controllare che i tecnici incaricati dispongano di attestato di qualificazione con QR-code e siano effettivamente presenti nel registro pubblico dei manutentori qualificati per la specifica tipologia di dispositivo antincendio oggetto di manutenzione.

Voglia gradire i nostri più cordiali saluti *ing. Giorgio Violi* *ing. Alberto Sant'Unione*