G L 0 D U W H G u G L F H P E U H

Sommario Rassegna Stampa

ItaliaOggi

Quotidiano Data 14-12-2021
Pagina 28
Foglio 1

Ingegneri certificatori per i periti industriali

Ingegneri certificatori delle competenze. Dopo aver stretto l'accordo con i veterinari, ieri è stata la volta dei periti industriali, che vedranno le loro competenze certificate dall'Agenzia Certing, organismo accreditato Accredia e costituito dall'interno della fondazione Cni. Il Consiglio nazionale periti industriali e Certing «collaboreranno alla redazione di uno schema di certificazione generale e trasversale a tutti i settori e le specializzazioni, tradizionali e recenti, degli iscritti all'albo dei periti industriali», si legge nella nota diffusa ieri dal Cni. «Il modello di certificazione sarà denominato perito industriale esperto».

«Dopo quello firmato per la certificazione delle competenze dei veterinari», ha commentato Armando Zambrano, presidente Cni, «questo accordo per la certificazione dei periti industriali segna un altro passaggio fondamentale nel processo di crescita di Certing, sempre più al servizio di tutto il mondo delle professioni, oltre che naturalmente degli ingegneri. Oltre tutto, la firma di questo documento conferma l'intenso rapporto di collaborazione che esiste tra il Cnpi e il nostro». «L'obiettivo di questo accordo», ha spiegato Giovanni Esposito, presidente del Cnpi, «è quello di mettere ogni professionista nelle condizioni di rispondere al meglio alle rinnovate esigenze del mercato».


28 GIUSTIZIA E SOCIETÀ ItaliaOggi

Avvocati, esame anche incinta

Ottenuto il rinvio della prova ma solo dopo il ricorso al Tar

Ingegneri certificatori per i periti industriali

Saranno otto mesi in più per diventare abogados

Commercialisti esclusi dalla negoziazione assistita

AGRICOLTURA

Unpain, su prestazioni e tariffe

Il Sole 24 ORE

Quotidiano Data 14-12-2021
Pagina 41
Foglio 1 / 2

I controlli antifrode sono limitati al profilo operativo del cedente

Anomalie. La responsabilità delle banche e degli intermediari finanziari nelle operazioni di acquisto dei crediti «edilizi» dopo il decreto 157/2021

Pagina a cura di
Davide De Girolamo

Nell'ultimo paragrafo della circolare delle Entrate 16/E del 29 novembre – già commentata sul Sole 24 Ore – l'agenzia delle Entrate fornisce alcuni preliminari chiarimenti anche in ordine alle possibili interrelazioni tra il nuovo obbligo di «non procedere all'acquisizione dei crediti» (edilizi) nelle ipotesi di "operazioni sospette" – introdotto dal decreto antifrodi (Dl 157/2021) per banche, poste, assicurazioni e gli altri soggetti indicati all'articolo 3 del Dlgs 231/2007 – e la ordinaria responsabilità del cessionario di questi crediti di cui all'articolo 121, commi 5 e 6, del Dl 34/2020.

L'Agenzia specifica, in particolare, che se questi soggetti procedono all'acquisto del credito benché ricorrano i presupposti per la segnalazione di operazioni sospette, tale condotta è valutata «anche ai fini del concorso nelle violazioni relative all'utilizzo dei crediti in argomento». E chiarisce ulteriormente, richiamando la relazione illustrativa al testo del decreto, che, ai fini dell'individuazione delle operazioni sospette oggetto dell'obbligo di comunicazione all'Uif, è necessario tener conto dei rischi connessi con:

i) l'eventuale natura fittizia dei crediti stessi;

ii) la presenza di cessionari dei crediti che pagano il prezzo della cessione con capitali di possibile origine illecita;

iii) lo svolgimento di abusiva attività finanziaria da parte di soggetti privi delle prescritte autorizzazioni che effettuano plurime operazioni di acquisto di crediti da un'amplia platea di cedenti" (si veda la comunicazione Uif – Covid 19 dell'11 febbraio 2021). Nessuna ulteriore specificazione viene fornita al riguardo.

Responsabilità più ampie

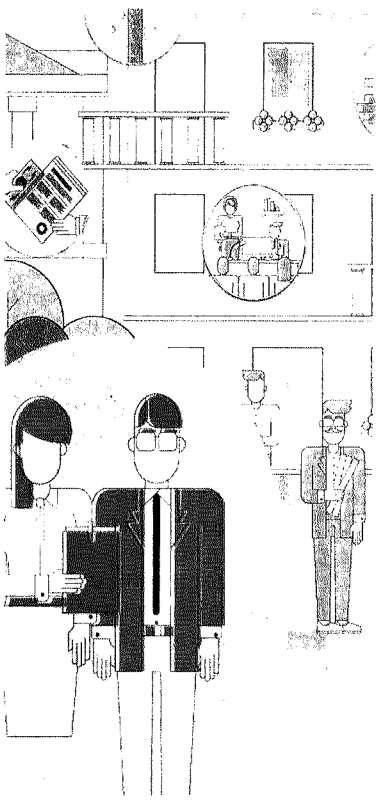
L'interpretazione dell'Agenzia sembra postulare un potenziale ampliamento della responsabilità dei cessionari "qualificati" individuati dalla nuova norma: ampliamento che la stessa Agenzia ha inteso ricollegare alla violazione del richiamato "divieto di acquisto". Tale possibilità, ad avviso di chi scrive, va decisamente respinta in via interpretativa.

Il concorso nell'illecito

I rigorosi presupposti giuridici che presiedono alla configurazione di una ipotesi di concorso nell'illecito – secondo le condizioni disposte dall'articolo 9 del Dlgs 472/1997 (richiamato dall'articolo 121 del decreto Rilancio, su cui la nuova norma non è in alcun modo intervenuta) – consentono di continuare ad assumere che il nuovo obbligo di verifica previsto dall'agenzia delle Entrate si debba comunque arrestare al profilo soggettivo e oggettivo dell'operatività del cedente e a indici di anomalia più macroscopici, senza poter tracimare anche in un controllo dei contenuti dell'operazione sottostante, che si tradurrebbe in una indebita riattribuzione dei compiti ordinariamente riservati ai soli organi pubblici deputati alle relative verifiche.

L'APPUNTAMENTO
Proseguono gli approfondimenti che due volte alla settimana (il martedì e il venerdì) saranno dedicati ad analizzare casi concreti legati al superbonus

NT+FISCO
Speciale 110%: tutti gli ultimi chiarimenti del fisco
Le novità in materia di superbonus
ntplusfisco.ilsole24ore.com



C'è il rischio di indebita attribuzione di compiti normalmente riservati agli organi pubblici

Il Sole 24 ORE

Quotidiano Data 14-12-2021
Pagina 41
Foglio 1

L'obbligo di verifica non può sfociare nell'esame dei documenti

Responsabilità

Diversi sono gli indici che consentono di concludere che l'assolvimento del nuovo obbligo di verifica a carico del cessionario non possa sfociare anche nella necessità di acquisire ed esaminare la documentazione a supporto dei crediti di imposta.

In primo luogo, la stessa comunicazione Uif dell'11 febbraio 2021, richiamata dall'Agenzia, rinvia agli schemi rappresentativi di comportamenti anomali concernenti operatività connesse con illeciti fiscali, pubblicati dalla stessa Uif il 10 novembre 2020. In particolare, nello schema D di questa comunicazione – proprio per l'ipotesi di eventuale «natura fittizia dei crediti» – le anomalie più ricorrenti sono individuate in quelle che riguardano il profilo soggettivo dei cedenti dei crediti e quello oggettivo dei soli comportamenti "estrinseci" rilevati.

A questo proposito viene specificato che assumono rilievo, sotto il profilo soggettivo, gli indici concernenti le caratteristiche dell'impresa cedente (costituita o divenuta operativa di recente, con forme giuridiche flessibili e semplici, prive di strutture organizzative reali, coinvolte in plurime cessioni, con frequenti variazioni nella compagine proprietaria e/o esponenti di dubbia reputazione o prestanome).

Sotto il profilo oggettivo, rilevano: la sussistenza di rapporti alimentati in via esclusiva o prevalente dal corrispettivo di contratti di cessione di crediti fiscali; la stipula di ripetuti contratti di cessione di crediti fiscali o di rami d'azienda costituiti in via pressoché esclusiva da questi crediti; anomalie concernenti il coinvolgimento di professionisti, le condizioni economiche pattuite per la cessione o l'impiego del corrispettivo da essa derivante.

Questa ricostruzione è l'unica coerente anche con il più generale impianto normativo del concorso di persone nell'illecito tributario che prevede nel dettaglio per la sua configurabilità, tra gli altri, il contributo causale di ciascun concorrente alla realizzazione dell'illecito e l'elemento soggettivo. L'intervento del cessionario "terzo" avviene, invece, ordinariamente in una fase successiva e distinta rispetto alla maturazione del diritto alla detrazione; i controlli preventivi riguardanti la regolarità di tale diritto devono essere effettuati dai soggetti che prendono parte al processo di genesi del credito.

Conferma ulteriore dell'inesigibilità di un controllo di tipo contenutistico a carico delle banche e degli altri intermediari finanziari può essere, infine, rinvenuta nell'avvenuta "espunzione" dalla versione finale del decreto antifrodi di un comma originariamente destinato a "estendere" la responsabilità del cessionario al caso in cui egli non acquisisca preliminarmente la documentazione che comprova, in capo all'originario beneficiario, l'effettiva realizzazione degli interventi: addossare al cessionario un tale onere probatorio avrebbe ostacolato la circolazione del credito.


I controlli antifrode sono limitati al profilo operativo del cedente

L'obbligo di verifica non può sfociare

Videozone: la rivoluzione dell'immagine è iniziata

CORRIERE DELLA SERA

Quotidiano Data 14-12-2021
Pagina 37
Foglio 1

Piano di ripresa

«Pnrr, le gare stanno partendo»

di Giuliana Ferraino

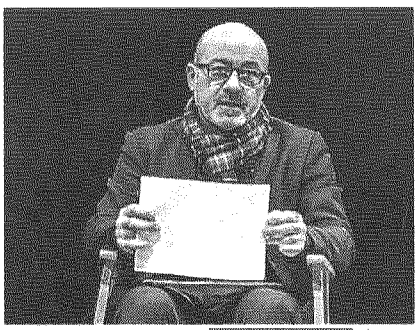
Road show di Cingolani e Colao: acceleriamo. «Prima di Natale il gestore del cloud»

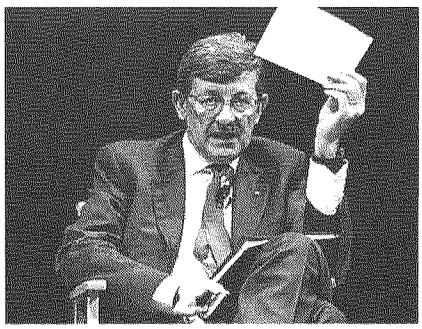
Sul Pnrr la parola d'ordine adesso è «accelerare». Il premier Mario Draghi manda a Milano due ministri chiave del suo governo, responsabili di digitale e transizione verde, per la messa a terra dei progetti che serviranno a modernizzare, a rilanciare e anche a rendere più sostenibile l'Italia. Finanziato dall'Unione europea attraverso i fondi del Next Generation Eu, il Piano nazionale di ripresa e resilienza (Pnrr) è un passaggio cruciale per il nostro Paese e tutte le istituzioni sono chiamate a partecipare, come ha rimarcato ancora una volta il presidente della Repubblica Sergio Mattarella.

«Nel 2026 vogliamo essere fra i migliori in Europa, dobbiamo partire subito e fare molto in fretta. Il 2022 è l'anno in cui tutto parte», afferma Vittorio Colao, ministro per l'Innovazione tecnologica e la Transizione digitale, a Italiadomani - Dialoghi sul Piano nazionale di ripresa e resilienza, il roadshow promosso dalla presidenza del consiglio per comunicare con cittadini, imprese e amministrazioni locali i contenuti e le opportunità del Pnrr. «Sulla fibra stiamo preparando i bandi: a gennaio ci saranno le gare, che verranno assegnate a giugno. E a luglio si vedranno le persone che scavano nelle città», aggiunge il ministro. Che ammette: «Sul 5G siamo leggermente più indietro, le gare saranno a marzo, perché siamo il primo Paese europeo a intervenire con i sussidi». Però sul digitale «per il Cloud, prima di Natale annunceremo quale sarà la proposta prescelta», anticipa Colao. E per le scuole «entro la metà dell'anno potremo partire».

Ai blocchi di partenza anche la rivoluzione green. Nel 2022 sono previsti 34,69 miliardi di investimenti per la transizione ecologia, dice Roberto Cingolani, il ministro che ne è responsabile. Quanto al fronte della sanità digitale, in particolare il fascicolo sanitario e la telemedicina, il governo sta approvando il disegno di una piattaforma nazionale. E «la Lombardia è una delle Regioni bandiera», sostiene Colao. L'idea è di «partire con gare a febbraio per una piattaforma nazionale e ad aprile per quelle verticali». Milano è pronta. Secondo il sindaco Giuseppe Sala, la città «ha capacità di investire un miliardo all'anno». Letizia Moratti, assessore al Welfare e vice presidente della Regione chiede però che il governo di riorganizzi in fretta la medicina generale, entro il 2022 come vuole la Ue, o i 7 miliardi di finanziamento saranno a rischio.

Rispettare i tempi per ogni progetto del Pnrr sarà cruciale, perché questa volta il tempo è davvero denaro.





Sopra, Roberto Cingolani, 59 anni, ministro della transizione ecologica con Vittorio Colao, 60 anni, della transizione digitale

L'evento

- E' arrivato a Milano l'evento «Italiadomani-Dialoghi sul Piano nazionale di ripresa e resilienza»
- Si tratta di un'iniziativa della Presidenza del Consiglio dei ministri per illustrare i contenuti e le opportunità del Pnrr. Ieri era la sesta tappa


«Banche decisive per crescita e sostenibilità. Ora il contratto»
«Pnrr, le gare stanno partendo»
La purificazione SMART dell'aria
Tecnologia al servizio della salute

ItaliaOggi

Quotidiano Data 14-12-2021
Pagina 30
Foglio 1

RISPOSTA DELLA DRE CAMPANIA

Bonus facciate se tutto è finito al 31 dicembre

Sulla base delle nuove disposizioni del dl antifrodi (n. 157/2021), Il contribuente può usufruire della detrazione fiscale del 90% (bonus facciate) solo per le spese effettivamente sostenute entro il 31 dicembre 2021, per le quali a tale data sia intervenuta anche l'ultimazione dei lavori, oltre che l'asseverazione di congruità. Sono le indicazioni che arrivano dalla direzione regionale delle entrate della Campania nella risposta a interpello 914-1430/2021, che *ItaliaOggi* ha potuto visionare. L'istanza è stata promossa dall'amministratore di un condominio che ha deliberato l'appalto dei lavori di riqualificazione delle facciate esterne del fabbricato, convenendo l'applicazione dello sconto in fattura da parte dell'impesa appaltatrice. Il dubbio interpretativo investe la questione se, nell'assunto che l'asseverazione sulla congruità delle spese segua l'iter del superbonus, ovvero a stati di avanzamento o a fine lavori, il condominio possa comunque usufruire della detrazione al 90% sull'importo totale dei lavori saldati entro il 31 dicembre 2021, ovvero "soltanto per le spese effettivamente sostenute e vistate per congruità" entro la medesima data. La Dre richiama precedenti interpretazioni che hanno chiarito la portata, in casi quale quello in esame, del "principio di cassa" (circ. n. 2/2020, par. 3), nonché la possibilità, anche per i bonus "ordinari", di esercitare l'opzione per la cessione del credito/sconto in fattura in relazione a stati di avanzamento, ferma restando la necessità che gli interventi agevolabili risultino effettivamente realizzati (circ. n. 30/2020, risp. 5.1.6; risposte a interrogazioni parlamentari 5-06307 e 5-06751 del 7/7 e 20/10/2021). Passando ai risvolti applicativi (sui bonus ordinari) derivanti dalle modifiche che il dl antifrodi ha apportato al dl rilancio (34/2020) , rispetto a quest'ultimo l'ufficio si sofferma sul combinato disposto degli art. 121, c. 1 ter (visto di conformità; asseverazione di congruità) e 119, c. 13 bis (contenuto asseverazioni), facendone discendere la necessità che gli oneri procedimentali siano espletati in relazione a lavori eseguiti. In tale chiave sono evocate faq (aggiornamento 22/11/2021) e circolare 16/2021 (par. 1.2.2). La portata di questa interpretazione risulta piuttosto innovativa nel panorama della prassi e sarà interessante riscontrare un suo eventuale consolidamento in documenti di portata generale.

Giovanni Galli e Gianluca Stancati


30 IMPOSTE E TASSE ItaliaOggi

Affrancamento, calcolo al netto

Base imponibile considerando il costo della rivalutazione

Cartella post sgravio valida

Bonus facciate se tutto è finito al 31 dicembre

Il Sole 24 ORE

Quotidiano Data 14-12-2021
Pagina 21
Foglio 1

Attacco degli hacker ai dati della Sogin

Attacco contro il sistema informatico della Sogin, la Spa pubblica che gestisce l'eredità delle centrali nucleari. Per l'azienda, l'attacco non ha avuto effetto sulle funzionalità del sistema informatico, sulla sicurezza né sulle normali attività aziendali.

Su una pagina del "dark web" un criminale informatico ha annunciato la vendita di 800 giga di dati interni alla società italiana — contratti, progetti, schemi d'impianto — ceduti per 250mila dollari nella criptovaluta Monero. Come esempio dei dati rubati, il criminale ha esibito proposte di qualifica del 2016 per la fornitura di attrezzature all'impianto Eurex di Saluggia (Vercelli). Lo stesso ricattatore il 15 luglio aveva rubato 1 tera di dati alla Saudi Aramco chiedendo 5mila dollari (o 50mila per renderli alla compagnia petrolifera).

Il truffatore potrebbe essere penetrato attraverso i computer di alcuni dirigenti in lavoro da casa.

La Sogin ieri ha risposto: «che la sicurezza sia nucleare che convenzionale degli impianti e la loro operatività è sempre stata garantita».


Imprese & Territori

Ex Ilva punta tutto sull'idrogeno
Piano di transizione in 10 anni

Software per un business sostenibile

ZUCCHETTI

Il Sole 24 ORE

Quotidiano Data 14-12-2021
Pagina 29
Foglio 1 / 2

Cyber attacchi, la Sanità è la più colpita: a rischio il 90% delle strutture

L'allarme. Due studi confermano la vulnerabilità dei sistemi informativi sanitari: solo l'11% impiega software aggiornati e il 50% ha sperimentato una fuga di dati

Marzio Bartoloni

«Un attacco criminale e terrorista senza precedenti, potente e invasivo»: così il governatore del Lazio Nicola Zingaretti lo scorso agosto definì il clamoroso cyber attack inflitto dagli hacker alla rete informatica che si occupa delle prenotazioni dei vaccini, il portale «Salute» della Regione. Quello è stato forse il caso recente più eclatante, ma solo uno dei tantissimi cyber attacchi alla Sanità, il settore in assoluto più colpito in Italia. Anche perché si scopre che le organizzazioni sanitarie sono tra le più vulnerabili visto che quasi il 90% non impiega software obsoleti o usa dispositivi vecchi e non aggiornati. A sottolinearlo sono due studi appena pubblicati che lanciano l'allarme

Il primo sottolinea come nel 2021 l'Italia continui a essere tra le nazioni finita di più nel mirino dei cybercriminali. Negli ultimi mesi si è infatti confermata tra le prime cinque nazioni al mondo più colpite dai «malware» (qualsiasi tipo di software dannoso sviluppato con l'obiettivo di infettare computer o dispositivi) e a ottobre aggiunge un altro primato, classificandosi terza come Paese maggiormente colpito dai «ransomware» (un malware che blocca l'accesso ai sistemi o ai file personali degli utenti e chiede il pagamento di un riscatto per renderli nuovamente accessibili). Un dato, questo, che emerge dall'ultimo report di Trend Micro Research, la divisione di Trend Micro specializzata in ricerca e sviluppo e lotta al cybercrime. Nel dettaglio, a ottobre il numero totale di ransomware intercettati in tutto il mondo è stato di 1.297.400. Gli Stati Uniti sono il Paese maggiormente colpito con il 23,4% di attacchi, a seguire Francia (7,5%), Italia (5%), Belgio (4,5%) e Brasile (3,8%). Per quanto riguarda i malware, gli Stati Uniti rimangono i più attaccati, con 34.816.097 assalti, seguiti da Giappone (31.711.116), Australia (6.132.704), Italia (6.097.979) e Regno Unito (5.610.942).

A guidare la classifica dei settori più colpiti dai malware in Italia c'è appunto la Sanità (1.072 attacchi), poi la Pa (842 attacchi), il manufacturing (746 attacchi), il tech (525) e il banking (260).

Il rischio di cyber attacchi nel nostro paese è dunque molto alto anche perché solo l'11% delle organizzazioni sanitarie utilizza dispositivi medici con software aggiornati, mentre l'89% usa invece per la maggior parte dispositivi medici con un sistema operativo obsoleto a causa di problemi di compatibilità, costi elevati degli aggiornamenti o per la mancanza di conoscenze tecnologiche interne. Numeri questi che emergono dal secondo studio e cioè l'ultimo report Healthcare 2021 di Kaspersky appena pubblicato che sottolinea come questo comportamento espone le organizzazioni sanitarie a maggiori vulnerabilità e rischi informatici. «L'utilizzo di dispositivi obsoleti - spiega la società di sicurezza - può provocare incidenti informatici. Quando gli sviluppatori di software smettono di supportare un sistema interrompono anche il rilascio di eventuali aggiornamenti, che spesso includono soluzioni di sicurezza per le nuove vulnerabilità. Se lasciate senza correzioni, queste vulnerabilità possono diventare un vettore di attacco per penetrare in una infrastruttura. Le organizzazioni sanitarie archiviano un volume notevole di dati sensibili e preziosi che le rendono uno degli obiettivi più redditizi».

Interrogati sulle capacità di reazione in materia di cybersecurity, solo il 20% degli operatori sanitari italiani crede che la loro organizzazione sia in grado di bloccare gli attacchi alla sicurezza o le violazioni del perimetro. La stessa percentuale è certa che la loro organizzazione disponga di una protezione di sicurezza tecnologica hardware e software aggiornata e adeguata.

In Italia, poi, il 50% degli intervistati ha ammesso che la loro organizzazione ha già sperimentato incidenti che hanno causato una fuga di dati, il 40% un attacco DDoS (cioè mettere ko un sito) mentre il 30% un attacco ransomware. «Il settore sanitario si sta evolvendo verso l'adozione di dispositivi connessi in grado di soddisfare la domanda di maggiore accessibilità alle cure. Questo comporta anche alcune sfide di cybersecurity. Ad oggi, esistono soluzioni e misure disponibili che possono aiutare a minimizzare i rischi. Queste misure insieme alla formazione del personale medico, possono aumentare significativamente il livello di sicurezza», spiega Cesare D'Angelo, General Manager Italy di Kaspersky.