CYBERSECURITY

Attestato di Cybersecurity

Esito della scansione di sicurezza dell'intero stack applicativo: vulnerabilità PHP di piattaforma del 21 ottobre 2026 e verifica di sicurezza applicativa di gestionale, console, sito e suo servizio.

Prodotto: BusItinera — Gestionale viaggi, noleggi e fatturazione per aziende di trasporto con autista
Documento: Attestato di Cybersecurity · **Data:** 22 ottobre 2026 · Versione del software: **1.28.3**
Autore del software: Ceol Andrea

Indice

1. Oggetto, ambito e metodo 2
2. Esito complessivo 3
3. Componenti in ambito 3
4. Vulnerabilità PHP di piattaforma (PHP2Shell) 4
5. Verifica di sicurezza applicativa 5
6. Separazione fra sito pubblico e console di gestione 7
7. Interventi applicati 7
8. Vigilanza e manutenzione 8
9. Dichiarazione conclusiva e avvertenze 8

Appendice — Avviso di Copyright 9

1. Oggetto, ambito e metodo

Il presente attestato riporta l'esito di una **scansione di sicurezza dell'intero stack applicativo BusItinera**, svolta il 22 ottobre 2026. L'attività è stata avviata in risposta al rilascio di sicurezza PHP del **21 ottobre 2026**, che ha corretto due vulnerabilità critiche dell'interprete, ed è stata poi estesa a una verifica completa di sicurezza applicativa su tutti i componenti.

Oggetto	Lo stack BusItinera nel suo complesso: il gestionale, la console di gestione della flotta, il sito pubblico e il servizio che lo serve
Versione	Gestionale 1.28.3; console e sito nello stato in linea alla data indicata
Ambito	Esposizione alle vulnerabilità PHP di piattaforma del 21 ottobre 2026; autenticazione e gestione delle sessioni; controllo degli accessi su tutti gli endpoint; iniezioni (base dati, comandi di sistema, XML, interfaccia); protezione CSRF; crittografia, gestione delle password e dei segreti; caricamento di file; attraversamento dei percorsi; richieste verso l'esterno; catena di fornitura delle librerie di terze parti; intestazioni di sicurezza HTTP; postura di contenimento dei container e della rete; superficie di esecuzione raggiungibile dal web
Metodo	Analisi statica del codice sorgente di tutti i componenti, condotta per classi di vulnerabilità e non a campione: enumerazione sistematica degli endpoint con verifica della guardia di autorizzazione su ciascuno; tracciamento dei dati non fidati dal punto d'ingresso fino a base dati, shell, interfaccia e filesystem; riscontro delle misure dichiarate contro la configurazione effettiva. Le correzioni sono state **verificate funzionalmente**: le configurazioni del server web sono state caricate in un'istanza reale e i controlli d'accesso provati con richieste HTTP, confrontando lo stato precedente con quello successivo; il controllo automatico di versione dell'interprete è stato provato su tutti i suoi casi; i file modificati sono stati sottoposti a controllo sintattico

© 2024–2026 Ceol Andrea — Tutti i diritti riservati

Data	22 ottobre 2026

Nota sul livello di dettaglio. Questo attestato è un documento pubblico e dichiara, per ogni classe di vulnerabilità esaminata, **l'esito** e, dove è stato individuato un rilievo, la sua **gravità** e la conferma che è stato **corretto e riverificato**. Non riporta invece nulla che possa agevolare un attacco: né percorsi, nomi di file, frammenti di codice o parametri di configurazione, né il componente, la funzione o le condizioni in cui un rilievo si manifestava. La ragione è concreta: il software è distribuito a più clienti, e un elenco circostanziato delle debolezze delle versioni precedenti sarebbe una lista di cose da provare su ogni copia non ancora aggiornata. Il dettaglio tecnico completo esiste, in un rapporto riservato non destinato alla diffusione.

2. Esito complessivo

Esito: stack protetto dalle vulnerabilità PHP del 21 ottobre 2026; tutti i rilievi corretti e riverificati

Lo stack è stato messo in sicurezza rispetto a entrambe le vulnerabilità di piattaforma, con la correzione dell'interprete resa **obbligatoria e verificata automaticamente** e con l'adozione integrale delle misure di mitigazione raccomandate. La verifica applicativa ha individuato **un rilievo di livello Alto** e **alcuni di livello Medio e Basso**, tutti sanati nel corso dell'attività e riverificati. Nessun rilievo è rimasto aperto alla data di chiusura.

Il rilievo di livello Alto **non riguardava il gestionale usato dalle aziende clienti**, ma uno strumento interno del fornitore, che per progetto non è esposto su Internet ed è raggiungibile solo da rete riservata: una misura perimetrale già in essere al momento della verifica, indipendente dalle protezioni applicative. Il rilievo è stato chiuso su **due livelli indipendenti** e la chiusura verificata con richieste reali, confrontando il comportamento prima e dopo l'intervento.

Gli esiti per classe di vulnerabilità esaminata sono riportati al capitolo 5.

3. Componenti in ambito

La scansione ha coperto **tutti** i componenti dello stack. Nessuno è stato escluso.

Componente	Natura	Esito
Gestionale	Applicazione web usata dalle aziende clienti: pianificazione, noleggi, contabilità, fatturazione elettronica, portale autista. È il componente esposto agli utenti finali.	Protetto dalle vulnerabilità di piattaforma; rilievi applicativi di livello Basso e Medio corretti
Console di gestione	Strumento interno del fornitore per creare e governare le istanze dei clienti. Non è accessibile ai clienti ed è raggiungibile solo da rete riservata.	Protetta dalle vulnerabilità di piattaforma; un rilievo di livello Alto e alcuni Medi corretti
Sito pubblico	Sito vetrina e pagine informative, composto da contenuti statici.	

© 2024–2026 Ceol Andrea — Tutti i diritti riservati

		Non interessato dalle vulnerabilità di piattaforma: non impiega l'interprete in questione
Servizio del sito	Servizio che gestisce le notifiche agli iscritti e raccoglie le richieste di prova dal sito.	Non interessato dalle vulnerabilità di piattaforma; verificato l'isolamento dalla console (capitolo 6)

4. Vulnerabilità PHP di piattaforma (PHP2Shell)

Il 21 ottobre 2026 il progetto PHP ha pubblicato un rilascio di sicurezza che corregge **due vulnerabilità di esecuzione di codice remoto** nell'interprete, identificate come **CVE-2026-109618** e **CVE-2026-109619** e divulgate con il nome collettivo **PHP2Shell**. Entrambe hanno gravità **9,2 su 10** secondo la metrica CVSS v4.0.

Le due vulnerabilità risiedono nella gestione della memoria e degli errori dell'interprete, cioè in meccanismi attraversati da qualunque richiesta: **un'applicazione può essere colpita anche se il proprio codice è corretto**. Sono raggiungibili da richieste **non autenticate** e il rischio è più elevato nella modalità di esecuzione impiegata dallo stack. Le vulnerabilità sono state individuate con il contributo di strumenti di intelligenza artificiale impiegati da gruppi di ricerca indipendenti, e alla data della scansione risultavano pubblicamente segnalati tentativi di sfruttamento.

Il rimedio definitivo indicato dal progetto PHP è **l'aggiornamento dell'interprete**: le misure di configurazione riducono l'esposizione ma non sostituiscono la correzione. Lo stack ha adottato entrambe le vie. Le misure qui elencate sono quelle raccomandate pubblicamente dal progetto PHP e dai ricercatori: riportarle non aggiunge nulla a quanto già noto.

Misure adottate su gestionale e console:

- **Correzione dell'interprete resa obbligatoria e verificata automaticamente.** È stato introdotto un controllo che, alla costruzione di ogni immagine applicativa, accerta che l'interprete includa la correzione di sicurezza e **interrompe la procedura** in caso contrario. Il controllo copre tutti i rami di versione supportati e fallisce deliberatamente anche su un ramo non previsto, in modo che una versione non valutata non possa passare inosservata. È quindi impossibile mettere in esercizio un'immagine costruita su un interprete non corretto senza che la procedura segnali l'errore. Il controllo è stato provato su tutti i suoi casi, compresi quelli di rifiuto.
- **Adozione integrale delle mitigazioni raccomandate** per entrambe le vulnerabilità, mantenute come difesa in profondità anche a interprete corretto, e applicate **in modo non sovrascrivibile dal codice applicativo**, così che nessuna impostazione dell'applicazione possa reintrodurre la condizione vulnerabile.
- **Disattivazione delle funzionalità non necessarie** individuate dai ricercatori come inneschi dell'attacco, con particolare riguardo a quelle che entrano in azione prima del codice applicativo e che quindi non potrebbero essere intercettate a livello di applicazione.
- **Limiti sulle richieste in ingresso** fatti rispettare dal server web, cioè prima che l'interprete elabori la richiesta: non solo sulla dimensione complessiva, ma anche sulla struttura del contenuto, poiché le tecniche di attacco pubblicate agiscono durante l'analisi della richiesta. I limiti si applicano anche alle richieste che non dichiarano correttamente la propria lunghezza.

© 2024–2026 Ceol Andrea — Tutti i diritti riservati

- **Contenimento della memoria spostato al livello corretto.** Il tetto di memoria è ora imposto dal contenitore e non dall'interprete: così un eccesso abbatte il singolo processo interessato, invece di innescare all'interno dell'interprete la condizione da cui nasce la vulnerabilità. È stata evitata la tecnica di limitazione che i ricercatori segnalano come controproducente.
- **Riduzione della superficie di errore raggiungibile dall'esterno.** Una delle due vulnerabilità si innesca a partire da errori fatali provocabili dall'esterno: la superficie da cui tali errori potevano originare è stata ridotta.

Il sito pubblico e il suo servizio **non impiegano l'interprete interessato** e non sono quindi esposti a queste due vulnerabilità. Anche per essi è stata comunque svolta la verifica applicativa descritta ai capitoli 5 e 6.

5. Verifica di sicurezza applicativa

Oltre alle vulnerabilità di piattaforma è stata svolta, su richiesta, una verifica estesa a tutti i componenti. Di seguito le classi esaminate e il relativo esito. Dove la verifica ha prodotto un rilievo, è indicata la gravità e la conferma della correzione; la natura tecnica del rilievo resta nel rapporto riservato, per le ragioni spiegate al capitolo 1.

Classe esaminata	Esito
Controllo degli accessi — guardia di autorizzazione su ogni endpoint	**Conforme.** Enumerazione completa degli endpoint di entrambe le applicazioni: ciascuna operazione risulta protetta lato server dalla guardia appropriata al proprio livello di privilegio. Le sole operazioni prive di guardia sono quelle che per natura precedono l'autenticazione. Nessuna scalata di privilegi né accesso a dati di altri soggetti individuati.
Iniezione su base dati	**Conforme.** Uso pervasivo di interrogazioni parametrizzate. Le interrogazioni costruite per composizione sono state esaminate una per una: gli elementi variabili provengono esclusivamente da elenchi fissi nel codice o da valori convertiti a numero intero, mai da dati forniti dall'utente. Nessuna iniezione sfruttabile individuata.
Iniezione di comandi di sistema	**Conforme.** Dove l'applicazione invoca strumenti esterni, ogni argomento è sottoposto a protezione e gli identificativi che concorrono a comporre i comandi sono normalizzati a un insieme ristretto di caratteri prima dell'uso. Nessuna iniezione individuata.
Iniezione in interfaccia	**Conforme.** Tutti i dati di provenienza esterna mostrati nelle interfacce risultano codificati prima dell'inserimento nella pagina, compresi quelli che possono essere immessi da visitatori anonimi.
Iniezione e XXE su XML	**Conforme.** L'XML della fatturazione elettronica viene costruito con codifica automatica del testo; non viene effettuata alcuna analisi di XML di provenienza non fidata, quindi la classe XXE non è applicabile.
Deserializzazione non sicura	**Non applicabile.** Nessun impiego di deserializzazione di dati su tutto lo stack.
Autenticazione e sessioni	**Conforme.** Password protette con algoritmo dedicato e parametro di costo adeguato; confronto a tempo costante anche per utenze inesistenti, così da non rivelarne l'esistenza; rigenerazione dell'identificativo di sessione all'accesso; secondo fattore e accesso con passkey; limitazione dei tentativi ripetuti; cookie con attributi di sicurezza.

© 2024–2026 Ceol Andrea — Tutti i diritti riservati

Protezione CSRF	**Rilievo di livello Basso, corretto e riverificato.** Un gruppo ristretto di operazioni di scrittura non applicava questa specifica verifica, pur restando protetto da un secondo meccanismo che già impediva l'attacco nei browser aggiornati. La verifica è ora applicata a tutte le operazioni di scrittura, per non dipendere da quel solo presupposto.
Crittografia e gestione dei segreti	**Conforme.** Cifratura autenticata con algoritmo e parametri corretti, valore di inizializzazione casuale per ogni operazione e validazione della lunghezza della chiave. Generazione di valori casuali affidata esclusivamente a sorgenti crittograficamente sicure: nessun impiego di generatori deboli nei percorsi di sicurezza. Nessun segreto presente nel codice sorgente o nella cronologia dei repository.
Credenziali iniziali	**Rilievo di livello Medio, corretto e riverificato.** Una procedura interna generava credenziali iniziali non sufficientemente distinte fra loro. Il cambio obbligatorio al primo accesso era già previsto. Ogni credenziale iniziale è ora casuale e univoca.
Caricamento di file	**Conforme.** L'unico caricamento previsto verifica esito, dimensione, provenienza effettiva del file e tipo reale del contenuto, non la sola estensione dichiarata. La destinazione non è una posizione eseguibile.
Attraversamento dei percorsi	**Conforme.** I riferimenti ai file gestiti dall'applicazione sono validati sia contro la presenza di separatori di percorso sia contro un formato atteso, con doppio controllo indipendente.
Richieste verso l'esterno (SSRF)	**Conforme.** Tutte le destinazioni delle richieste uscenti derivano da parametri di configurazione dell'amministratore o da dati interni, e nessuna è influenzabile da un utente non autenticato.
Catena di fornitura (librerie di terze parti)	**Rilievo di livello Medio, corretto e riverificato.** Una libreria di terze parti non era servita con garanzie di integrità adeguate. **Nessun componente dello stack dipende più da codice eseguibile fornito da terzi attraverso la rete**: tutte le librerie sono ora servite dall'applicazione stessa.
Intestazioni di sicurezza HTTP	**Rilievo di livello Medio, corretto e riverificato.** Un componente non inviava l'insieme completo di intestazioni di sicurezza. Tutti i componenti applicativi dispongono ora di un insieme completo, politica restrittiva dei contenuti inclusa, verificato nelle risposte effettive.
Superficie di esecuzione raggiungibile dal web	**Rilievo di livello Alto, corretto e riverificato.** In entrambe le applicazioni risultavano raggiungibili dal web porzioni di codice destinate al solo uso interno. Nel gestionale si trattava di codice inerte, senza esposizione di dati; il rilievo di livello Alto riguardava lo strumento interno del fornitore, non esposto su Internet. La chiusura è stata realizzata su **due livelli indipendenti** — uno nel codice, che lo accompagna ovunque sia installato, e uno nella configurazione del server — ed è stata verificata con richieste reali, confrontando il comportamento prima e dopo l'intervento.
Contenimento di container e rete	**Conforme, con tetto di memoria introdotto.** La base dati non è esposta all'host; i segreti non sono presenti nei repository; le comunicazioni fra componenti restano su rete interna. È stato introdotto un tetto di memoria per contenitore, necessario a completare le mitigazioni descritte al capitolo 4.

© 2024–2026 Ceol Andrea — Tutti i diritti riservati

6. Separazione fra sito pubblico e console di gestione

È stata svolta una verifica specifica, su richiesta, per accertare che **il servizio del sito pubblico non possa in alcun modo impartire comandi alla console di gestione**. L'esito è negativo per l'attaccante.

Esito: nessun canale dal sito verso la console

La direzione della comunicazione è unidirezionale e **opposta** a quella che renderebbe possibile un attacco di questo tipo.

- **È la console a interrogare il servizio, mai il contrario.** Tutte le interazioni sono avviate dalla console. Il servizio non avvia alcuna connessione verso la console, non ne conosce l'indirizzo e non possiede credenziali per raggiungerla. Un attaccante che ottenesse il pieno controllo del servizio non acquisirebbe con ciò alcun canale verso la console.
- **Non esiste alcun punto d'ingresso della console invocabile dal servizio.** Le credenziali impiegate dalla console per interrogare il servizio restano lato server e non vengono mai esposte al browser.
- **Il solo flusso di dati dal sito alla console è la coda delle richieste di prova**, alimentata dal modulo pubblico del sito. Questo flusso è stato tracciato dall'ingresso fino a destinazione: i dati sono trattati come **dati** e non diventano mai istruzioni, in nessuno dei punti in cui vengono conservati, mostrati o impiegati. **Nessun percorso conduce dai contenuti di una richiesta di prova all'esecuzione di un comando.**
- **Il modulo pubblico è protetto contro l'abuso** con validazione dei campi lato server, verifica anti-robot, limitazione per indirizzo di provenienza, trappola per automatismi, consenso al trattamento verificato lato server e conservazione a termine.

7. Interventi applicati

Tutti gli interventi sono stati applicati durante l'attività e verificati. In sintesi, e nei termini sanitizzati di questo documento:

Intervento	Componenti
Controllo automatico, bloccante alla costruzione dell'immagine, che l'interprete includa la correzione di sicurezza del 21 ottobre 2026	Gestionale, console
Adozione integrale delle mitigazioni raccomandate per entrambe le vulnerabilità, in forma non sovrascrivibile dal codice applicativo	Gestionale, console
Disattivazione delle funzionalità individuate come inneschi dell'attacco e non necessarie al servizio	Gestionale, console
Limiti su dimensione e struttura delle richieste, imposti dal server web prima dell'interprete	Gestionale, console
Tetto di memoria per contenitore, a contenere un eccesso senza coinvolgere l'interprete	Gestionale, console

© 2024–2026 Ceol Andrea — Tutti i diritti riservati

Riduzione, su due livelli indipendenti, della superficie di esecuzione interna raggiungibile dal web	Gestionale, console
Insieme completo di intestazioni di sicurezza, con politica dei contenuti restrittiva, su tutti i componenti applicativi	Console
Eliminazione di ogni dipendenza da codice eseguibile fornito da terzi attraverso la rete	Console
Impostazioni di produzione dell'interprete, con messaggi diagnostici esclusi dalle risposte	Console
Estensione della verifica CSRF a tutte le operazioni di scrittura	Gestionale
Credenziali iniziali casuali e univoche per ciascun account	Gestionale

8. Vigilanza e manutenzione

La messa in sicurezza rispetto a una vulnerabilità di piattaforma non è un atto concluso. Sono previste le seguenti attività.

- **Ricostruzione delle immagini con interprete aggiornato** per tutte le istanze in esercizio: la correzione è efficace solo dopo la ricostruzione e il riavvio dei processi. Il controllo automatico introdotto rende l'operazione verificabile, perché una ricostruzione su interprete non corretto non va a termine.
- **Sorveglianza degli indicatori di attacco** segnalati dai ricercatori per queste due vulnerabilità, sulla registrazione degli eventi delle istanze.
- **Programmazione del passaggio a un ramo dell'interprete con supporto esteso.** Il ramo attualmente impiegato cessa di ricevere correzioni di sicurezza il **31 dicembre 2026**: il passaggio va completato entro tale data, e il controllo automatico introdotto copre già i rami successivi.
- **Mantenimento degli strumenti interni su rete riservata**, non esposti su Internet, come misura perimetrale indipendente dalle protezioni applicative.

9. Dichiarazione conclusiva e avvertenze

Sulla base delle attività svolte, alla data del 22 ottobre 2026 lo stack applicativo **BusItinera** risulta **protetto rispetto alle vulnerabilità PHP CVE-2026-109618 e CVE-2026-109619**, con la correzione dell'interprete resa obbligatoria e verificata automaticamente e con le misure di mitigazione raccomandate integralmente adottate; i **rilievi di sicurezza applicativa individuati durante la scansione sono stati tutti corretti e riverificati**, e nessuno è rimasto aperto; è stata accertata l'**assenza di qualunque canale** che consenta al servizio del sito pubblico di impartire comandi alla console di gestione.

Si richiama l'attenzione sul fatto che l'efficacia della correzione di piattaforma sulle singole istanze in esercizio è subordinata alla ricostruzione delle immagini e al riavvio dei processi, secondo quanto indicato al capitolo 8.

Avvertenze. Il presente attestato è redatto a fini informativi e di verifica interna. L'attività è stata condotta con l'assistenza di un sistema di intelligenza artificiale (Claude di Anthropic) per conto del titolare del software; non costituisce una certificazione accreditata di terza parte, né un test di penetrazione su sistemi in esercizio, né una garanzia assoluta di assenza di difetti o vulnerabilità. La verifica è stata svolta mediante analisi del codice sorgente e delle configurazioni, con riscontro funzionale delle correzioni in ambiente di prova. La sicurezza informatica è un processo continuo: l'esito si riferisce all'ambito, ai componenti, alle

© 2024–2026 Ceol Andrea — Tutti i diritti riservati

versioni e alla data indicati, e non si estende a vulnerabilità divulgate successivamente. Le informazioni sulle vulnerabilità di piattaforma sono riprese dagli avvisi pubblici del progetto PHP e dei gruppi di ricerca che le hanno segnalate. Restano impregiudicati i termini di licenza e le limitazioni di responsabilità applicabili al software.

Appendice — Avviso di Copyright e Proprietà Intellettuale

© 2024–2026 Ceol Andrea — Tutti i diritti riservati

AVVISO LEGALE: Questo software, la sua architettura, il codice sorgente, l'interfaccia grafica, la documentazione e l'idea progettuale sottostante sono opera dell'ingegno di Ceol Andrea e sono protetti dalla normativa italiana, europea e internazionale in materia di diritto d'autore e proprietà intellettuale.

Art. 1 — Titolarità dei Diritti

1.1. Il software denominato "BusItinera" (di seguito "il Software"), comprensivo di codice sorgente, codice oggetto, interfaccia grafica (GUI), database schema, documentazione tecnica e di utente, materiali grafici, loghi e ogni altro elemento connesso — fatta eccezione per i componenti di terzi elencati all'Art. 11 — è opera originale dell'ingegno di Ceol Andrea (di seguito "l'Autore" o "il Titolare").

1.2. L'Autore è titolare esclusivo di tutti i diritti morali e patrimoniali d'autore sul Software ai sensi della Legge 22 aprile 1941, n. 633 e successive modifiche, con particolare riferimento agli artt. 1, 2 n. 8, 12-19, 20-24, 64-bis, 64-ter, 64-quater.

1.3. Il Software è altresì protetto dal D.Lgs. 10 febbraio 2005, n. 30 (Codice della Proprietà Industriale) per quanto attiene alla tutela dei segni distintivi, del know-how e dei segreti commerciali.

Art. 2 — Diritto d'Autore sul Software

2.1. Ai sensi dell'art. 2, n. 8 della L. 633/1941, i programmi per elaboratore sono tutelati come opere letterarie ai sensi della Convenzione di Berna.

2.2. La tutela si applica a qualsiasi forma di espressione del programma, inclusi il codice sorgente, il codice oggetto, il materiale preparatorio, la documentazione tecnica e l'interfaccia utente, purché originali.

2.3. La protezione del diritto d'autore decorre dalla creazione dell'opera e non è soggetta a registrazione, conformemente all'art. 5, comma 2, della Convenzione di Berna e all'art. 6 del WIPO Copyright Treaty (WCT).

Art. 3 — Tutela Europea

3.1. Il Software è protetto dalla Direttiva 2009/24/CE relativa alla tutela giuridica dei programmi per elaboratore, recepita in Italia con il D.Lgs. 518/1992.

3.3. Il Software è inoltre tutelato dalla Direttiva 2001/29/CE (InfoSoc) e dalla Direttiva (UE) 2019/790 sul diritto d'autore nel mercato unico digitale.

Art. 4 — Divieti Espressi

Senza il preventivo consenso scritto dell'Autore, è fatto espresso divieto di:

- **Riproduzione** — Copiare, duplicare, riprodurre in tutto o in parte il codice sorgente, il codice oggetto, l'interfaccia grafica, la struttura del database, la documentazione o qualsiasi altro componente del Software (art. 64-bis, lett. a, L. 633/1941).
- **Modifica e Opera Derivata** — Tradurre, adattare, trasformare, modificare il Software o crearne opere derivate, incluso reverse engineering, decompilazione e disassemblaggio, salvo nei limiti tassativi dell'art. 64-quater L. 633/1941.
- **Distribuzione e Pubblicazione** — Distribuire, pubblicare, mettere a disposizione del pubblico, trasmettere il Software o parti di esso, sotto qualsiasi denominazione, a titolo gratuito o oneroso (art. 64-bis, lett. c).
- **Vendita e Commercializzazione** — Vendere, concedere in licenza, sub-licenziare, noleggiare, cedere a terzi il Software o qualsiasi diritto ad esso relativo.
- **Appropriazione dell'Idea** — Utilizzare l'idea progettuale, l'architettura, il modello di dati, i flussi operativi e la logica applicativa per sviluppare prodotti concorrenti (art. 2598 C.C.; artt. 98-99 D.Lgs. 30/2005; Direttiva (UE) 2016/943).
- **Rimozione delle Informazioni** — Rimuovere o alterare le informazioni sul diritto d'autore, i credits, le avvertenze legali o le indicazioni di titolarità (art. 102-quinquies L. 633/1941).
- **Elusione delle Misure Tecnologiche** — Eludere o disattivare qualsiasi misura tecnologica di protezione applicata al Software (art. 102-quater L. 633/1941).

Art. 5 — Tutela dei Segreti Commerciali

Il codice sorgente, l'architettura, gli algoritmi, i modelli di dati e il know-how tecnico costituiscono segreti commerciali ai sensi degli artt. 98-99 del D.Lgs. 30/2005 e della Direttiva (UE) 2016/943. L'acquisizione, l'utilizzo o la divulgazione illeciti sono puniti ai sensi dell'art. 623 c.p. e comportano responsabilità civile.

Art. 6 — Tutela della Concorrenza

Ai sensi dell'art. 2598 C.C. compie atti di concorrenza sleale chi usi segni distintivi confondibili, imiti servilmente i prodotti dell'Autore o si avvalga di mezzi non conformi alla correttezza professionale. L'Autore ha diritto a inibitoria, risarcimento e pubblicazione della sentenza (artt. 2599-2600 C.C.).

Art. 7 — Sanzioni e Responsabilità

La violazione dei diritti d'autore è punita ai sensi degli artt. 171, 171-bis, 171-ter L. 633/1941 (reclusione e multa). Ai sensi degli artt. 156-170 L. 633/1941 il Titolare può agire per inibitoria, sequestro e distruzione delle copie illecite, risarcimento integrale del danno, pubblicazione della sentenza e restituzione degli utili.

Art. 8 — Normativa Internazionale

Il Software è protetto da: Convenzione di Berna (1886, rev. 1979); Accordo TRIPS (1994); WIPO Copyright Treaty (WCT, 1996); Convenzione Universale del Diritto d'Autore (UCC).

Art. 9 — Limitazioni d'Uso

9.1. Il Software è concesso in licenza d'uso esclusivamente al cliente finale presso il quale viene installato, limitatamente all'uso operativo interno dell'azienda.

9.2. La licenza d'uso non comporta il trasferimento della titolarità dei diritti, che rimangono in capo esclusivo all'Autore.

9.3. È vietata qualsiasi forma di sub-licenza, cessione o concessione in uso a terzi senza autorizzazione scritta.

Art. 10 — Riservatezza del Codice Sorgente

Il codice sorgente è fornito in forma confidenziale e riservata. Il destinatario si impegna a non divulgarlo, con qualsiasi mezzo. L'obbligo di riservatezza sopravvive alla cessazione del rapporto e si protrae per tutta la durata della protezione legale.

Art. 11 — Componenti di Terzi

Il Software può incorporare componenti di terzi, ciascuno protetto dalla propria licenza: qrcodejs (QR del 2FA) — MIT; Google Places / Maps — Google LLC; font DM Sans / DM Mono — SIL Open Font License (OFL). Le rivendicazioni del presente avviso non si estendono a tali componenti; ciò non riduce i diritti dell'Autore sulle parti originali.

Art. 12 — Prova di Paternità e Data Certa

La paternità e l'anteriorità sono documentate mediante mezzi idonei a conferire data certa (cronologia di versionamento, marche temporali). L'Autore si riserva la registrazione presso il Registro pubblico speciale SIAE ex art. 6 D.Lgs. 518/1992.

Art. 13 — Legge Applicabile e Foro Competente

Il presente avviso è disciplinato dalla legge italiana. Foro competente esclusivo quello del luogo di residenza dell'Autore, fatte salve le sezioni specializzate in materia di impresa (D.Lgs. 168/2003). Per le controversie transnazionali si applica il Reg. (UE) 1215/2012.

Art. 14 — Rapporto con il Contratto di Licenza

Il presente avviso integra e non sostituisce l'eventuale contratto di licenza sottoscritto; in caso di contrasto prevale il contratto. L'installazione, l'accesso o l'utilizzo del Software comportano l'accettazione dei presenti termini e delle limitazioni d'uso (Art. 9).

Art. 15 — Clausola di Salvaguardia

L'eventuale nullità di una clausola non comporta la nullità delle restanti. La mancata azione dell'Autore non costituisce rinuncia. Nessuna disposizione può escludere i diritti inderogabili dell'utente legittimo (artt. 64-ter e 64-quater L. 633/1941).

© 2024–2026 Ceol Andrea

Tutti i diritti riservati. All rights reserved. Alle Rechte vorbehalten. Tous droits réservés.

Qualsiasi uso non autorizzato del presente Software, in tutto o in parte, sarà perseguito nelle sedi competenti ai sensi della normativa vigente.

© 2024–2026 Ceol Andrea — Tutti i diritti riservati