ConduCodice · Mandato audit, Blindata e test

Allegato al Contratto quadro. Regola audit, Revisione, Blindata e test di sicurezza.

Oggetto e autorizzazione

Art. 1. Oggetto e natura

1.1 Questo documento regola le prestazioni di audit, Revisione e Blindata indicate nel Preventivo, anche su software realizzato da altri.

1.2 Sono prestazioni di consulenza e obbligazioni di mezzi, come previsto dall'art. 3-ter.2 del Contratto quadro. Il Fornitore lavora a regola d'arte e documenta quanto svolto, ma non garantisce l'assenza di vulnerabilità né l'inviolabilità del sistema.

1.3 I test comprendono prove di carico, di stress, di violazione e altre prove tecniche, automatiche e manuali, secondo quanto indicato nel Preventivo.

Art. 2. Autorizzazione

2.1 Il Fornitore svolge test solo dopo che il Cliente ha firmato il modulo di autorizzazione allegato, che indica sistemi, perimetro, tipi di prova e periodo.

2.2 Il Cliente autorizza il Fornitore ad accedere ai sistemi e a svolgere le prove indicate, anche simulando attacchi, consapevole che altrimenti potrebbero essere vietate dalla legge (art. 615-ter c.p.).

2.3 Il Cliente dichiara di avere i poteri per autorizzare i test e di aver ottenuto i permessi di proprietari, fornitori di hosting, sviluppatori e altri terzi coinvolti. Dichiara inoltre di avere il diritto di consegnare il codice al Fornitore.

2.4 Il Fornitore può rifiutare o interrompere un test se ha dubbi sull'autorizzazione. Tutto ciò che è fuori dal perimetro è escluso.

Esecuzione

Art. 3. Ambiente di prova e produzione

3.1 Di norma i test si svolgono su una copia di prova.

3.2 Il Fornitore svolge test sul sistema in produzione solo se il Cliente lo chiede per iscritto nel modulo di autorizzazione. Prima del test il Cliente esegue un backup completo e ne verifica il ripristino.

3.3 Il Cliente sa che i test possono rallentare, interrompere o danneggiare il sistema e accetta questo rischio.

Art. 4. Dati trovati durante il lavoro

4.1 Il Fornitore non copia i dati personali, le password e le chiavi trovate durante il lavoro, salvo quanto strettamente necessario a documentare il problema, e li segnala al Cliente. Cancella le prove al termine della consegna, salvo diversa istruzione.

4.2 Se il lavoro comporta il trattamento di dati personali del Cliente, il Fornitore agisce come responsabile del trattamento secondo la nomina allegata al Contratto quadro.

Art. 5. Problemi scoperti

Se durante il lavoro scopre una vulnerabilità, una violazione dei dati o un possibile illecito, il Fornitore avvisa il Cliente. Il Cliente decide cosa fare e fa da solo le comunicazioni ad autorità e interessati. Resta salvo ogni obbligo di legge del Fornitore.

Report e Bollino

Art. 6. Report

6.1 Il report descrive le prove svolte e i risultati alla data indicata, per la versione esaminata. Non copre versioni successive né minacce scoperte dopo.

6.2 Il report è riservato e serve solo al Cliente. Non può essere dato a terzi senza consenso scritto del Fornitore, salvo obbligo di legge. Il Fornitore non risponde verso terzi che ne fanno uso.

Art. 7. Bollino Revisione

7.1 Il Bollino descrive l'esito dell'esame alla data indicata. Non è una certificazione, un'omologazione o una garanzia di sicurezza.

7.2 Il Cliente può esibirlo in pubblico solo con data e versione del software, usando il testo stabilito dal Fornitore. Il Bollino vale 12 mesi e decade prima se il software viene modificato in modo rilevante.

7.3 Il Fornitore può revocarlo se il Cliente ne fa un uso scorretto, se scopre un problema grave o se il Cliente non rispetta il Contratto. Dopo la scadenza o la revoca, il Cliente smette subito di usarlo.

7.4 Il Bollino è incluso nei software sviluppati dal Fornitore. In questo caso è una dichiarazione del Fornitore sul proprio lavoro, non una verifica di terzi. Per i software realizzati da altri richiede l'audit a pagamento.

Responsabilità e approvazione

Art. 8. Responsabilità

8.1 Il Cliente risponde dei danni causati da test svolti entro il perimetro autorizzato, anche se interrompono o danneggiano il sistema, salvo dolo o colpa grave del Fornitore.

8.2 Il Cliente tiene indenne il Fornitore dalle pretese di terzi, comprese quelle di proprietari e fornitori dei sistemi, che derivano da dichiarazioni false o incomplete nel modulo di autorizzazione, o dalla mancanza dei permessi dell'art. 2.3.

8.3 Per il resto valgono il limite e le esclusioni dell'art. 21 del Contratto quadro.

Art. 9. Approvazione specifica (artt. 1341 e 1342 c.c.)

Con il secondo codice OTP previsto dall'art. 27 del Contratto quadro, il Cliente approva specificamente: art. 1.2 (obbligazione di mezzi), art. 2.4 (rifiuto e interruzione), art. 3.3 (rischio dei test), art. 6.2 (limiti d'uso del report), art. 7.3 (revoca del Bollino), art. 8 (responsabilità e manleva).

Allegato. Modulo di autorizzazione ai test

Da compilare e firmare con OTP prima di ogni test.

Voce	Da compilare
Cliente e firmatario, con qualifica	
Software e versione	
Domini, indirizzi IP e server compresi	
Sistemi esclusi	
Tipi di prova autorizzati (carico, stress, violazione, altre)	
Ambiente (copia di prova o produzione)	
Data e ora di inizio e fine	
Proprietario dei server e fornitore di hosting	
Permesso dei terzi coinvolti ottenuto il	
Backup completo verificato il (solo per la produzione)	
Contatto di emergenza durante il test	

Il firmatario dichiara di avere i poteri per autorizzare il test, che i dati sono esatti e che valgono gli artt. 2, 3 e 8 del mandato.