Rilasciata nel novembre 2025

Dichiarazione di conformità del software alle normative vigenti

Nome del software: Appalti & Contratti E-Procurement
Versione: consultabile al seguente link https://releases.maggioli.cloud

Nome del produttore: Maggioli S.p.A. (nel seguito "**Maggioli**" o la "**Società**")

Dati del produttore: sede legale in Via Del Carpino n.8 (47822) Santarcangelo di Romagna (RN) - Italia, P.IVA. 02066400405

La scrivente Società in qualità di software house che ha sviluppato il Software Appalti & Contratti E-Procurement, dichiara che nella versione rilasciata è conforme alle seguenti norme e standard:

- *"Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale"* (Agenzia per la Cybersicurezza Nazionale) D.P.C.M. 9 dicembre 2021, n. 223;
- Direttiva (UE) 2022/2555 (NIS2), recepita in Italia con il Decreto Legislativo 4 settembre 2024, n. 138;
- Regolamento Generale sulla protezione dei dati (Reg. EU. 2016/679);
- Software Assurance Maturity Model (SAMM) come metodologia di DevSecOps e standard metodologico per l'integrazione della sicurezza informatica sin dalla fase di sviluppo;
- Domain Driven Design come standard metodologico di progettazione;
- Certificazioni che attestano la creazione, l'applicazione ed il mantenimento dei Sistemi Gestionali ed Organizzativi di Maggioli S.p.A. conformi alle norme, consultabili al seguente link: https://www.maggioli.com/it-it/chi-siamo/certificazioni
- Certificazione delle componenti e della piattaforma "Appalti&Contratti e-Procurement" alle Regole Tecniche AgID "Requisiti tecnici e modalità di certificazione delle Piattaforme di approvvigionamento digitale" e iscrizione nel Registro Piattaforme Certificate ANAC

Il software è stato sviluppato e testato in conformità con le seguenti

procedure:

- Maggioli S.p.A. ha adottato la metodologia OWASP SAMM (Software Assurance Maturity Model) di OWASP (consultabile al link https://owasp.org/www-project-samm/) come standard per i suoi team di sviluppo, un approccio che si estende in modo significativo anche a Appalti & Contratti. Questa scelta strategica mira a garantire un miglioramento continuo delle pratiche di sicurezza del software, intercettando e mitigando le vulnerabilità in ogni fase della progettazione e dello sviluppo del prodotto.
- L'applicazione di SAMM a Appalti & Contratti inizia con una valutazione iniziale (assessment), un passaggio fondamentale per determinare lo stato attuale della sicurezza del software e identificare le aree dove è possibile intervenire per rafforzarla ulteriormente. Sulla base dei risultati di questa valutazione, viene definita una roadmap specifica di miglioramento, che guida gli sforzi futuri per elevare gli standard di sicurezza di Appalti & Contratti.
- La metodologia SAMM suddivide il ciclo di vita del software in cinque funzioni aziendali chiave: Governance, Design, Implementation, Verification e Operation. Per Appalti & Contratti, questo si traduce in un'attenzione scrupolosa alle politiche e alle procedure di sicurezza adottate (Governance), all'integrazione delle pratiche di sicurezza fin dalla fase di progettazione del software (Design), all'applicazione delle migliori pratiche di codifica sicura durante lo sviluppo (Implementation), all'esecuzione di test e verifiche approfondite delle vulnerabilità (Verification), e alla gestione e al monitoraggio della sicurezza del prodotto una volta in produzione (Operation). A ciascuna di queste pratiche, all'interno delle diverse funzioni, viene assegnato un punteggio da 0 a 3, che indica il livello di maturità raggiunto in termini di sicurezza. L'obiettivo primario è progredire costantemente verso livelli di maturità sempre più elevati, assicurando così che Appalti & Contratti sia non solo un prodotto funzionale e performante, ma anche intrinsecamente sicuro e affidabile per i suoi utenti.
- Il processo di gestione e tracciamento di eventuali anomalie prevede l'utilizzo di una piattaforma avanzata per il tracciamento dei bug, integrata con un sistema di help desk. L'obiettivo principale è documentare l'intero ciclo di vita delle segnalazioni generate dal supporto. Questa piattaforma è ulteriormente integrata con un servizio cloud per la gestione del codice, che permette di collegare il codice sorgente alle specifiche segnalazioni. Le risoluzioni di ogni problematica sono pubblicate come "note" su un portale dedicato alle release, condiviso con i cliente, garantendo un monitoraggio continuo e completo di tutte le azioni intraprese per affrontare le vulnerabilità.

Descrizione del software, comprese le sue funzionalità e scopi:

“Appalti & Contratti E-Procurement" è un sistema integrato di prodotti e servizi offerto da Maggioli, progettato per supportare le stazioni appaltanti nella gestione delle procedure d'appalto nell’intero ciclo di vita: programmazione, progettazione pubblicazione, affidamento ed esecuzione.

"Appalti & Contratti E-Procurement" è una piattaforma cloud certificata PAD (Piattaforma Acquisti Digitali). Questa piattaforma è conforme al Codice dei Contratti Pubblici e consente la gestione digitale e teleProtezione dati personalimatica dell'intero processo degli appalti.

Dal 1° gennaio 2024, l'utilizzo di piattaforme e-Procurement certificate è obbligatorio per le stazioni appaltanti e Appalti & Contratti E-Procurement ha ottenuto la certificazione AgID per le componenti di affidamento, pubblicazione ed esecuzione già a fine 2023. La piattaforma è modulare e include moduli per Programmazione, Progettazione, Pubblicazione, Affidamento ed Esecuzione.

Sintesi delle misure tecniche e organizzative generali

- **Gestione Utenti e accessi**

Il sistema di autenticazione degli utenti alle applicazioni in oggetto permette di integrarsi in modo efficace con i sistemi pubblici di identità, in particolare SPID e CIE, oltre al proprio sistema interno di autenticazione può integrarsi ai sistemi dei clienti mediante tecnologie di Single Sign On basate su protocolli standard (es. OAuth2, OpenID, SAML). L'autenticazione degli utenti è prevista una sola volta, al momento dell'accesso all'applicazione. L'applicazione prevede funzionalità di tipo amministrativo, tali da consentire una profilazione centralizzata e granulare degli utenti.

- **Gestione dei Log**

Le applicazioni in oggetto prevedono una completa gestione dei log sia per tracciare e registrare le operazioni svolte dagli utenti che accedono all’applicazione tramite le credenziali attribuite, che per tracciare e registrare le operazioni svolte dagli amministratori di sistema che accedono all’applicazione tramite uno specifico sistema di identificazione a più fattori. Il logging avviene a livello applicativo registrando tutte le operazioni previste dal regolamento e quelle critiche a livello di business, anche a livello di lettura dove necessario. I log prodotti sono consultabili direttamente

dall'ambiente applicativo, semplificando così notevolmente le attività degli amministratori di sistema.

- **Crittografia**

L'applicazione è sviluppata e fornita in conformità con le linee guida e i requisiti in materia di crittografia stabiliti dall'Agenzia per la Cybersicurezza Nazionale (ACN).

Di seguito si riepilogano le principali tipologie di crittografia adottate in base all'ambiente cloud certificato ANC su cui vengono erogate le soluzioni.

Tipo di crittografia	Descrizione	Dinova	Google Cloud Platform	Microsoft Azure
Crittografia applicata "at rest"	Crittografia dei sistemi di storage a riposo (database/repository/bucket) mediante cifratura simmetrica con chiavi gestite	✅ Servizi IaaS VM con dischi crittografati con AES 256 XTS mode conformi FIPS 140-2 con chiavi gestite da Dinova	✅ Servizi PaaS - Database: servizio gestito con dati criptati con crittografia a 256 bit (AES-256) - Bucket: i bucket sono criptati, non accessibili pubblicamente con crittografia a 256 bit (AES-256). Tutti i dati a livello di archiviazione vengono criptati tramite DEK, che utilizzano AES-256 per impostazione predefinita. Le chiavi DEK sono a loro volta criptate tramite KEK che utilizzano AES-256. La chiavi di crittografia sono gestite da Google.	✅ Servizi PaaS/IaaS - Database: servizio gestito con dati criptati con crittografia in transito e "at rest" (AES-256) - Storage account: encryption at rest La chiavi di crittografia sono gestite da Microsoft.
Crittografia applicata "in transit"	Traffico HTTPS criptato con certificato	✅	✅	✅
Crittografia a livello "applicazione"	Vengono crittografate le password (account utente locale) con algoritmo proprietario. In caso di integrazione con	✅	✅	✅

Tipo di crittografia	Descrizione	Dinova	Google Cloud Platform	Microsoft Azure
	keyclaock e/o AuthService (SPID/CIE) la gestione delle utenze e la crittografia è demandata a questo. Per la gestione delle offerte viene applicata crittografia RSA; viene generata e memorizzata in DB una chiave RSA per ogni tipologia di busta (amministrativa, tecnica, economica); la chiave privata viene protetta con passphrase nota solo all'utente e non conservata nel sistema Gli algoritmi di cifratura usati sono: ● PGP 1024 bit con passphrase per la generazione delle chiavi asimmetriche RSA Kp e Kr ● AES/CBC/PKCS5PADDING 128 bit per la generazione delle chiavi simmetriche di sessione Ks ● AES/GCM/NoPadding 128 bit per la cifratura lato browser			
Crittografia utilizzata per i backup	Servizio di backup gestito dal cloud provider	✅ Replica remota VM con dischi crittografati con AES 256 XTS mode conformi FIPS 140-2 con chiavi gestite da Dinova	✅ Tutti i dati a livello di archiviazione vengono criptati tramite DEK, che utilizzano AES-256 per impostazione predefinita. Le chiavi DEK sono a loro volta criptate tramite KEK che utilizzano AES-256. La chiavi di crittografia sono gestite da Google.	✅ - VM backup criptato automaticamente - DB: backup criptato automaticamente - Storage account: cifratura at rest con protezione soft delete per 14 e 7 giorni, con fileshare in modalità giornaliera e con retention 30gg,

- **Gestione degli incidenti di sicurezza – Violazione dei dati (art. 33 e 34 del GDPR)**

Maggioli S.p.A. ha adottato una procedura di Incident Response per gestire eventi di sicurezza informatica e Data Breach, in linea con il GDPR e le norme ISO, per migliorare la propria sicurezza. Un Data Breach è definito come la perdita di riservatezza, integrità o disponibilità (RID) dei dati personali.
Eventi comuni che possono causare un Data Breach includono furto/smarrimento di dispositivi contenenti dati personali, perdita/modifica di archivi, diffusione impropria di dati (es. email errate), attacchi informatici, divulgazione a persone non autorizzate e violazioni della sicurezza fisica.
Per gestire questi eventi, Maggioli ha istituito un "Team di Crisi", responsabile del rilevamento, contenimento e risoluzione degli incidenti. Il team include DPO, CISO, Ufficio Privacy, Ufficio Legale, Consulente Privacy e Team Security. Ogni area aziendale ha un referente che collabora con il Team di Crisi.

Il processo di gestione degli incidenti si articola in quattro fasi:

1. Scoperta: Segnalazione dell'incidente e compilazione del registro.
2. Qualificazione: Il Team di Crisi valuta l'evento.
3. Valutazione: CISO, Team di Crisi e DPO decidono la risposta proattiva.
4. Azione: Implementazione di misure correttive a breve e lungo termine.

L'Ufficio Privacy è il punto di contatto iniziale per tutte le segnalazioni. Il CISO e il DPO, in collaborazione con l'Ufficio Privacy, qualificano l'evento come Data Breach o semplice evento di sicurezza. Il registro dell'incident report deve essere finalizzato entro 8 ore dalla presa in carico dell'evento e trasmesso al Team di Crisi, il quale valuta anche l'evento e il rischio per gli interessati, decidendo se è necessaria una notifica al Garante o al cliente.

Le tempistiche di notifica variano, sempre in ottemperanza con quanto previsto agli art. 33 e 34: se Maggioli è Titolare del trattamento, la notifica all'Autorità Garante deve avvenire entro 72 ore, salvo improbabile pregiudizio per i diritti degli interessati, mentre invece se Maggioli è Responsabile del trattamento, le tempistiche sono stabilite dal Titolare, generalmente 24-48 ore per la trasmissione di una relazione tecnica

Sintesi delle misure tecniche ed organizzative per la protezione dei dati personali relative ad installazioni con Container orchestrator

- Configurazione Sicura: sono state implementate procedure secondo i principi di sicurezza by design e hardening della configurazione dell'orchestratore
- Autenticazione e Autorizzazione: sono stati implementati metodi di autenticazione e autorizzazione applicando il principio del minimo privilegio su utenti, service account e workload.
- Sicurezza dei Container: Vengono utilizzate e mantenute aggiornate immagini ufficiali, firmate, minimizzate. Le immagini vengono sottoposte a scansione per rilevare vulnerabilità.
- Crittografia delle Comunicazioni: Uso di protocolli sicuri per le connessioni esterne
- Cifratura e Protezione dei Dati: E' abilitato l' encryption at rest per volumi e secrets
- Logging e Monitoring: Log degli eventi e audit log attivi con alerting su eventi critici e anomali
- Aggiornamenti e Patch: Sono stati implementati automatismi e procedure per mantenere tutti i componenti aggiornati con le ultime patch di sicurezza.
- Controllo delle Risorse: Sono stati previsti e applicati limiti alle risorse in modo da poter prevenire attacchi DoS.
- Sicurezza dello Storage: L'accesso ai volumi persistenti è stato opportunamente hardenizzato e configurato in sicurezza.
- Controllo della Supply Chain: Sono state verificare e gestire le dipendenze di terze parti in modo da limitare attacchi e minacce.
- Backup e Disaster Recovery Sicuri: Backup policy versionata con test di restore automatizzati
- Formazione e Consapevolezza: formazione del personale su best practice e minacce

Audit e monitoraggio del software

È posto in essere un monitoraggio continuo sui software, in quanto vengono eseguiti VA/PT annuali/ semestrali a rotazione sugli applicativi.

Servizio di assistenza clienti

L'assistenza viene garantita mediante un servizio di help-desk, per fornire il supporto tecnico-operativo agli utenti dell'Ente interessati alla fruizione dei servizi dell'infrastruttura tecnologica ed applicativa. Il servizio di help-desk eroga le sue attività agli utenti al fine di risolvere le problematiche che si manifestano e per le quali il personale dell'Ente non sia autonomo nella soluzione. Il servizio di help desk viene erogato da personale altamente qualificato, preparato e di comprovata esperienza nel settore della Pubblica Amministrazione ed è in grado di risolvere in modo rapido e puntuale il problema segnalato.

Compiti ed attività del servizio di Help desk sono tali da:

- fornire direttamente la soluzione attraverso il canale telefonico e/o con collegamento da remoto, avvalendosi in caso di necessità del supporto del 2° Livello e/o del reparto di Sviluppo software.
- attivare su richiesta del Cliente, previo acquisto di giornate, l'assistenza on site di personale in modalità affiancamento nel caso di esigenza specifica dell'ente.