Rilasciata nel novembre 2025

Dichiarazione di conformità del software alle normative vigenti

Nome del software: "Concilia EVO"

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 la Suite denominata "Concilia EVO", dichiara che nella versione rilasciata -come da note di rilascio pubblicate sul sito web dedicato alle release software- 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

Descrizione del software, comprese le sue funzionalità e scopi:

Il software applicativo, denominato Concilia EVO, è una soluzione progettata per la gestione completa delle attività sanzionatorie dei Comandi di Polizia Locale. Il sistema consente agli Enti Locali la gestione integrata dell'intero ciclo di vita delle sanzioni amministrative.

Caratteristiche Architetturali e Tecnologiche

Concilia EVO è una soluzione web nativa con le seguenti caratteristiche tecniche e strutturali:

- Modalità di Erogazione: Il software è erogato in modalità SaaS (Software as a Service) e ospitato su infrastruttura Google Cloud Platform (GCP).
- Architettura: La piattaforma si basa su un'architettura a microservizi e adotta la metodologia Domain-Driven Design (DDD) per garantire flessibilità e scalabilità.
- Interfaccia Utente: L'interfaccia, di tipo full responsive e sviluppata in HTML5 su framework Angular, è accessibile tramite i principali browser web (Chrome, Edge, Firefox) da qualsiasi dispositivo, senza necessità di installazioni lato client. È progettata in conformità con le normative di accessibilità (ACN e European Accessibility Act).
- Sicurezza e Autenticazione: La gestione centralizzata di autenticazione e autorizzazione è affidata all'integrazione con la piattaforma open-source Keycloak, che abilita funzionalità di Single Sign-On (SSO).
- Configurazione Multi-Ente: La soluzione supporta nativamente la gestione per enti singoli, unioni di comuni o consorzi, permettendo una tracciabilità dei dati conforme alle specifiche esigenze operative e contabili.

Funzionalità Principali

Il software copre l'intero processo sanzionatorio attraverso moduli integrati e configurabili.

Gestione del Processo Sanzionatorio

- Gestione Violazioni: Il sistema gestisce gli accertamenti di violazioni al Codice della Strada e ad altre normative amministrative. Include l'importazione automatizzata dei flussi dati da dispositivi di rilevamento (es. rilevatori velocità, impianti semaforici, varchi ZTL), la gestione di verbali cartacei e preavvisi, e il supporto per la Firma Elettronica Qualificata (FEQ) dei documenti digitali. Gestisce inoltre le sanzioni accessorie e la decurtazione punti della patente, con trasmissione automatizzata dei dati al D.T.T.S.I.S.
- Notifiche degli Atti: Il modulo permette la preparazione e la generazione di flussi per la notifica, sia in formato cartaceo che digitale. È prevista l'integrazione nativa con la Piattaforma Notifiche Digitali (SEND) gestita da PagoPA S.p.A., con un apposito cruscotto per il monitoraggio dello stato di spedizione.
- Gestione Ruoli e Pre-ruoli: La piattaforma consente la generazione di lettere di pre-ruolo e la creazione dell'elenco dei verbali da iscrivere a ruolo, con verifica dei termini di legge e produzione del tracciato standard per l'agente della riscossione.

Integrazioni e Servizi Digitali

- Interrogazione Banche Dati: Il software si interfaccia con le principali banche dati nazionali ed europee, tra cui D.T.T.S.I.S. (Motorizzazione), ACI-PRA, ANPR (Anagrafe Nazionale della Popolazione Residente), INI-PEC, INAD (Indice Nazionale dei Domicili Digitali) ed EUCARIS (per veicoli stranieri).
- Gestione Pagamenti: È assicurata l'integrazione completa con il circuito di pagamenti PagoPA, con funzionalità per la consultazione, l'associazione ai verbali, la rendicontazione e il monitoraggio in tempo reale degli incassi tramite un apposito cruscotto.

Strumenti Operativi e Componenti Aggiuntive

- Monitoraggio e Reportistica: Dispone di strumenti per il tracciamento delle attività utente (log), un cruscotto per il monitoraggio delle lavorazioni massive asincrone e un sistema per l'estrazione di elenchi, report e statistiche personalizzabili.
- Applicazione Mobile: La soluzione è completata dal modulo Concilia EVO Mobile, un'applicazione nativa per dispositivi Android che permette l'accertamento delle violazioni su strada, l'interrogazione in tempo reale delle banche dati e la stampa

degli atti tramite stampanti portatili, con generazione di QR code per il pagamento.
- Supporto Utente: Il sistema è corredato da una documentazione ipertestuale (Wiki) e da un assistente virtuale (chatbot) basato su Intelligenza Artificiale.

La suite Concilia EVO è presente anche nel catalogo ACN (https://www.acn.gov.it/portale/w/sa-4250) ed ha un livello di qualificazione QC1.

Architettura ad alto livello

L'architettura di **Concilia Evo** si fonda su un modello **modulare, stratificato e a microservizi**, progettato per garantire scalabilità, resilienza e facilità di evoluzione nel tempo. Tale approccio consente di disaccoppiare le singole componenti applicative, permettendo a ciascun modulo di svilupparsi ed essere aggiornato in maniera autonoma, senza impattare sull'intero sistema. Questo principio architetturale rende la piattaforma particolarmente adatta a gestire l'elevata complessità e la continua evoluzione normativa che caratterizzano l'ambito sanzionatorio.

Il **back-office** rappresenta il cuore gestionale della soluzione e mette a disposizione degli operatori un motore di workflow per il governo dei processi, un sistema documentale integrato per l'archiviazione e la gestione dei fascicoli digitali, strumenti di notifica e reporting avanzati, nonché l'integrazione nativa con PagoPA e con i sistemi esterni istituzionali (Ministero, MIT, Prefettura, ANPR, ecc.). L'obiettivo è supportare in maniera completa tutte le fasi del ciclo di vita della sanzione, dalla rilevazione fino alla fase esecutiva.

Il **front-office** si concretizza in un portale digitale, accessibile sia ai cittadini sia agli operatori, realizzato come **Single Page Application**. Questa scelta tecnologica consente un'esperienza utente fluida e reattiva, eliminando la necessità di continui ricaricamenti delle pagine. L'interfaccia è progettata nel pieno rispetto delle **Linee Guida di accessibilità AgID** e delle **WCAG 2.1**, garantendo così inclusività e usabilità anche per gli utenti con

disabilità.

Per quanto riguarda le **integrazioni**, Concilia Evo espone servizi applicativi attraverso **API REST**, permettendo la cooperazione con sistemi terzi e garantendo l'interoperabilità con le piattaforme ministeriali e regionali. Questo approccio consente inoltre di estendere le funzionalità e di adattare il sistema alle esigenze dei singoli enti senza compromettere la coerenza complessiva della soluzione.

La **persistenza dei dati** è realizzata mediante l'uso congiunto di database relazionali **PostgreSQL**, utilizzati per la gestione dei dati strutturati e transazionali, e di database non relazionali **MongoDB**, deputati all'archiviazione di grandi volumi di informazioni e contenuti non strutturati. Questa combinazione consente di coniugare l'affidabilità del modello relazionale con la flessibilità dei sistemi NoSQL, garantendo al contempo performance elevate e resilienza.

Per garantire scalabilità, affidabilità e durabilità, Concilia Evo adotta inoltre soluzioni di **cloud storage,** che consentono di archiviare e gestire in maniera sicura i file multimediali legati al fascicolo sanzionatorio (immagini provenienti da velox, video di varchi ZTL, scansioni di documenti, ecc.). Questo approccio permette di disaccoppiare la logica applicativa dalla gestione fisica dei contenuti, favorendo l'integrazione con diversi provider di servizi cloud e assicurando la disponibilità dei dati anche in scenari distribuiti o multi-ente.

Un ulteriore principio architetturale adottato è il **CQRS (Command Query Responsibility Segregation)**, che separa la gestione delle operazioni di scrittura (*command*), tipicamente transazionali e soggette a vincoli di integrità, dalle operazioni di lettura (*query*), orientate alla consultazione e all'analisi dei dati. Questa scelta consente di ottimizzare entrambi i flussi: da un lato, le **operazioni critiche di business** (come la registrazione di una violazione, l'associazione di documenti al fascicolo sanzionatorio o la registrazione di un pagamento) sono garantite da transazioni affidabili sui database relazionali; dall'altro, le **operazioni di consultazione** (ad esempio l'accesso al fascicolo digitale, la generazione di report o la visualizzazione di dashboard statistiche) possono essere gestite in maniera scalabile e

performante, attingendo da viste materializzate, indici ottimizzati o database specializzati in lettura. L'adozione del pattern CQRS migliora la **scalabilità orizzontale**, consente una più efficiente distribuzione dei carichi e rende possibile estendere la piattaforma verso architetture di tipo **event-driven**, con l'eventuale introduzione di sistemi di *event sourcing* per la tracciabilità completa delle operazioni.

La **sicurezza** è un aspetto trasversale che permea ogni livello architetturale. L'autenticazione è centralizzata e gestita attraverso **Keycloak**, che garantisce il supporto ai principali sistemi di identità digitale nazionali (SPID, CIE, CNS) e alle modalità di accesso avanzate come la Multi-Factor Authentication (MFA). Tutte le comunicazioni avvengono tramite protocollo **TLS**, mentre l'accesso ai servizi applicativi è regolato da **token JWT** che assicurano validità e profilazione delle autorizzazioni. Un sistema di **logging e auditing centralizzato** consente di monitorare eventi e accessi, fornendo tracciabilità completa e garantendo la conformità ai requisiti normativi e di sicurezza.

Nel complesso, l'architettura di Concilia Evo rappresenta una piattaforma moderna e affidabile, capace di adattarsi alle diverse modalità di erogazione, supportare carichi crescenti e assicurare agli enti locali un sistema robusto, sicuro e orientato al futuro.

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 Concilia EVO. 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 Concilia EVO 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 Concilia EVO.

- La metodologia SAMM suddivide il ciclo di vita del software in cinque funzioni aziendali chiave: Governance, Design, Implementation, Verification e Operation. Per Concilia EVO, 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 Concilia EVO 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.
- Per garantire la stabilità e l'affidabilità del software nel tempo, al processo di collaudo classico dove esperti funzionali verificano che le nuove funzionalità siano compliance a quanto previsto, è stato implementato un sistema di test automatici di non regressione. Questo processo consente di verificare che le funzionalità esistenti continuino a comportarsi correttamente anche dopo l'introduzione di nuove modifiche o aggiornamenti. Questo sistema riproduce in modo controllato una serie di scenari d'uso critici per l'applicazione, simulando le interazioni dell'utente con l'interfaccia. Questi test vengono eseguiti ciclicamente in fase di sviluppo e ogni volta che viene distribuita una nuova versione. Il risultato di ogni esecuzione viene analizzato automaticamente: se viene rilevata un'anomalia rispetto al

comportamento atteso, il processo segnala l'errore, bloccando il rilascio della versione fino alla risoluzione del problema. Questo approccio consente di ridurre drasticamente il rischio di regressioni, migliorare la qualità del software e velocizzare il ciclo di rilascio, mantenendo alto il livello di affidabilità percepito dagli utenti.

Sintesi delle misure tecniche e organizzative generali

La sicurezza rappresenta un elemento trasversale e imprescindibile di **Concilia Evo**, concepita sin dalle prime fasi di progettazione secondo i principi del *security by design* e del *privacy by default*.

L'**autenticazione e la gestione degli utenti** sono affidate a un sistema di Identity Management centralizzato basato su **Keycloak**, che supporta sia l'integrazione con i protocolli standard di federazione dell'identità (SAML, OAuth2, OpenID Connect) sia l'utilizzo delle principali identità digitali nazionali, quali **SPID, CIE e CNS**. Grazie a questa architettura, l'accesso ai servizi è sicuro e profilato, con possibilità di abilitare meccanismi di **autenticazione a più fattori (MFA)** per i contesti più sensibili.

La **protezione dei dati personali** è garantita a più livelli. Tutte le comunicazioni avvengono tramite cifratura **TLS**, mentre i dati a riposo possono essere protetti attraverso **Transparent Data Encryption (TDE)** e sistemi di cifratura applicativa. Durante lo sviluppo vengono eseguiti regolari controlli di **SAST (Static Application Security Testing)**, attività di **secret detection** per individuare eventuali credenziali esposte e **dependency scanning** per monitorare la sicurezza delle librerie di terze parti. La piattaforma è inoltre sottoposta periodicamente a **test di Vulnerability Assessment e Penetration Testing (VA/PT)**, condotti sia da team interni sia da soggetti specializzati esterni.

I **requisiti minimi di sicurezza**, definiti dalle **Linee Guida AgID** e dalle raccomandazioni dell'**Agenzia per la Cybersicurezza Nazionale (ACN)**, sono integralmente recepiti. Tali requisiti vengono applicati non solo ai meccanismi di autenticazione, ma anche alle logiche di profilazione degli utenti e all'assegnazione granulare dei permessi, garantendo così un

sistema capace di adattarsi a strutture organizzative complesse.

La gestione delle attività è tracciata da un sistema di **log e audit trail centralizzato**, che registra accessi, operazioni critiche e modifiche ai dati. L'accesso ai log è rigidamente profilato, così da assicurare integrità, riservatezza e disponibilità delle informazioni raccolte.

La **crittografia** adottata da Concilia Evo è conforme agli standard indicati dall'ACN e garantisce sia la protezione dei dati in transito sia quella dei dati a riposo.

- **Requisiti minimi di sicurezza**

I requisiti minimi di sicurezza previsti dalle Linee Guida per la sicurezza informatica prevedono tutta una serie di misure atte a garantire la protezione dei sistemi informativi e dei dati gestiti dalle Pubbliche Amministrazioni. Si sottolinea come il tema non riguardi esclusivamente la privacy del dato ma anche la sua integrità e disponibilità. Per mitigare il rischio di incorrere in problematiche di questo tipo è introdotta una sezione dedicata alla valutazione RID sin dalla fase di analisi delle funzionalità (correttive, adeguative ed evolutive) prima di introdurle all'interno della catena produttiva. Questo permette di esaminare preventivamente gli impatti di una modifica software su dati potenzialmente sensibili e di focalizzare le fasi di collaudo sui punti più critici.

A livello funzionale, i requisiti minimi di sicurezza sono recepiti sia in fase di autenticazione sia in fase di profilatura. In fase di autenticazione. In fase di profilatura, il sistema mette a disposizione un cruscotto di assegnazione permessi strutturato su gerarchie di gruppi logici/ruoli estremamente granulare. Completa il catalogo di misure dedicate alla protezione del dato il sistema delle ACL che assegna permessi a specifici utenti o gruppi di utenti a livello di singolo record.

- **Audit**

Concilia EVO integra un sistema completo di tracciamento delle operazioni suddiviso in diversi livelli:

1. **Log tecnici**: registrano eventi a basso livello legati al funzionamento della piattaforma, come errori di sistema, accessi ai servizi, operazioni sulle tabelle di

sistema e dettagli di infrastruttura.

2. **Audit log funzionali**: tracciano le operazioni effettuate dagli utenti sulle funzionalità applicative, includendo le modifiche ai dati (CRUD) sulle macroentità, con registrazione dei valori **pre-update** e **post-update**. Questo livello garantisce piena tracciabilità e auditabilità delle azioni a livello business.
3. **Audit log in architettura CQRS**: in contesti basati su **Command Query Responsibility Segregation**, viene mantenuta una separazione tra **comandi** (modifiche ai dati) e **query** (letture/interrogazioni), assicurando che sia possibile ricostruire sia le operazioni di scrittura che quelle di lettura in modo chiaro e strutturato.

- **Crittografia**

Le metodologie crittografiche adottate sono pienamente conformi alle linee guida e ai requisiti stabiliti dall'Agenzia per la Cybersicurezza Nazionale (ACN).

Le specifiche implementazioni della crittografia, inclusi gli algoritmi utilizzati, la gestione delle chiavi e i protocolli di sicurezza, sono intrinsecamente legate al Cloud Provider selezionato per l'erogazione dei servizi Concilia EVO. Ogni fornitore di servizi cloud adotta soluzioni crittografiche proprie che vengono integrate e sfruttate a pieno nelle nostre architetture.

Per una disamina completa e dettagliata delle misure crittografiche specifiche per ciascun abbinamento di Concilia EVO e per il relativo Cloud Provider, si rimanda alle schede tecniche dedicate. Tali documenti, disponibili a seguito della sottoscrizione degli accordi contrattuali, forniranno tutte le informazioni necessarie a comprendere le modalità di protezione dei dati in relazione alla specifica infrastruttura di erogazione scelta.

- **Gestione utenti e profilazione**

Concilia EVO adotta un approccio di **controllo accessi granulare** (Granular Access Control,

GAC) per gestire in modo preciso e sicuro i diritti degli utenti. Questo modello consente di assegnare permessi specifici a utenti o gruppi, garantendo loro accesso solo alle risorse o ai dati necessari per le loro funzioni, senza esporli a rischi derivanti da accessi non autorizzati.

La granularità dei profili utente si articola su più livelli:

> **Livello funzionale**: ogni profilo è associato a specifiche funzionalità del sistema, limitando l'accesso a moduli o sezioni in base al ruolo dell'utente.
>
> **Livello operativo**: all'interno di ciascuna funzionalità, i permessi possono essere ulteriormente dettagliati per singole operazioni (ad esempio, creazione, lettura, aggiornamento, eliminazione di dati), seguendo il principio del **least privilege**.

Questo approccio permette di ridurre al minimo i rischi associati a accessi non autorizzati o eccessivi, migliorando la sicurezza complessiva del sistema e facilitando la conformità a normative come il GDPR.

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

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. Vengono utilizzati RBAC + IAM per segregare l'accesso a risorse e servizi.
- Sicurezza dei Container: vengono utilizzate e mantenute aggiornate immagini ufficiali, firmate, minimizzate. Sono state implementate pod security policies e le immagini vengono sottoposte a scansione per rilevare vulnerabilità.
- Crittografia delle Comunicazioni: uso di protocolli sicuri per le connessioni esterne, con rotazione automatica dei certificati
- Cifratura e Protezione dei Dati: è abilitato l' encryption dei 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

Per ulteriori approfondimenti si rimanda alla relativa scheda tecnica, che verrà condivisa a seguito della sottoscrizione degli accordi contrattuali

Monitoraggio del software

Il sistema attraverso l'ambiente da cui viene erogato, permette di effettuare il seguente monitoraggio:

- malfunzionamenti o rallentamenti;
- metriche di utilizzo (performance, carico, tempi di risposta);
- notifiche automatiche in caso di condizioni anomale;

Questo approccio consente di intervenire tempestivamente in caso di problemi e di ottimizzare il funzionamento dell'applicazione in base all'effettivo utilizzo.

Sempre in stretta sinergia con l'ambiente di erogazione, possono essere attivi meccanismi di monitoraggio continuo della sicurezza, con l'obiettivo di rilevare tempestivamente comportamenti anomali, tentativi di intrusione o eventi potenzialmente dannosi. Attraverso l'analisi dei log di sistema e dell'applicazione infatti è possibile individuare accessi sospetti, escalation di privilegi o pattern di attacco.

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 Locale 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.