Rilasciata nel novembre 2025

Dichiarazione di conformità del software alle normative vigenti

Nome del software: Suite “Sicraweb 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 “Sicraweb”, 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:

La suite è composta da una serie di verticali modulari, realizzati sulle esigenze di ogni singolo ufficio dell'Ente Locale tra di loro integrati, in linea con le disposizioni AgiD, necessaria per gli Enti locali che hanno come obiettivo l'efficienza di gestione, l'evoluzione dei processi e l'erogazione di nuovi servizi a cittadini e imprese. La suite Sicraweb EVO è presente anche nel catalogo ACN.

Sicraweb Evo offre diversi moduli applicativi, tra cui:

- **IRIDE Evo**: Sistema informativo per la gestione dei flussi documentali e dei procedimenti amministrativi
- **SERFIN Evo**: Sistema informativo per la digitalizzazione dei procedimenti amministrativi contabili
- **SMART Evo**: Sistema informativo per il controllo di gestione e la valutazione delle performance
- **TRIB Evo**: Sistema informativo per la gestione delle entrate locali e dei servizi a domanda individuale
- **DEMOS Evo**: Sistema informativo per la digitalizzazione dei Servizi Demografici
- **CIM Evo**: Sistema informativo per la digitalizzazione dei Servizi Cimiteriali
- **PERS Evo**: Sistema informativo per la gestione delle risorse umane
- **PE Evo**: Sistema informativo per la gestione delle pratiche edilizie
- **AUT Evo**: Sistema informativo per la gestione delle pratiche autorizzatorie
- **TER Evo**: Sistema informativo per la gestione della cartografia
- **COM Evo**: Sistema informativo per la gestione delle attività economiche
- **SUAP Evo**: Sistema informativo per la gestione delle attività produttive

Ogni modulo è specializzato in un'area specifica ma condivide informazioni con gli altri, semplificando il lavoro degli operatori e migliorando l'efficienza dell'amministrazione.

Architettura ad alto livello

L'architettura di Sicraweb EVO ha una fisionomia stratificata e fortemente orientata alla modularizzazione di componenti e servizi software. Ogni livello è organizzato a moduli dedicati a specifiche funzionalità applicative permettendo al sistema complessivo di poter evolvere con agilità e flessibilità. Questo disaccoppiamento architetturale definito by design garantisce infatti ad ogni modulo di beneficiare di tutti gli aggiornamenti e integrazioni progressivamente implementate nel resto della Suite. Nello specifico, Sicraweb EVO presenta ad alto livello tre livelli principali risultato della business logic implementata dai servizi di back office, i dati visualizzati e gestiti dai servizi di front office e la persistenza del dato implementata grazie ad un database relazionale e repository locali o remoti per l'archiviazione documentale.

Il back-office è costruito su una piattaforma applicativa che rappresenta la Suite integrata dei servizi messi a disposizione di tutte le componenti funzionali. I moduli di Suite offrono un motore di Workflow, Scheduler, Gestione Documentale, Gestione Utenti con relativa profilatura, Bus di comunicazione interna, servizi di Notifica Push e Messaggistica. La piattaforma applicativa beneficia a sua volta dei servizi dell'application server (J2EE Compliant) che garantiscono le funzionalità fondamentali di un'applicazione enterprise come Transaction Manager, Repository, Code e Cache.

Su questi moduli infrastrutturali insistono quindi i moduli applicativi verticali che realizzano i servizi di business messi a disposizione degli operatori e le API implementate con protocolli SOAP e REST. La business logic resta infatti unica e le varie interfacce di utilizzo, siano esse relative a sessioni interattive o di cooperazione applicativa, sono realizzate tramite specifici connettori che espongono il risultato delle elaborazioni richieste permettendo anche di semplificare (facade pattern) o adattarne (adapter pattern) il contenuto.

La sicurezza è gestita trasversalmente a tutti i livelli del back-office. Le comunicazioni vengono gestite tramite protocollo TLS e ogni richiesta deve essere accompagnata da un token JWT per verificarne validità e relative autorizzazioni. Il sistema di audit e logging è centralizzato in modo da raccogliere tutte le informazioni su eventi e accessi in un unico punto la cui consultazione è opportunamente profilata. La piattaforma applicativa mette a disposizione inoltre un keystore per conservare in modo sicuro dati critici come secrets e certificati.

Sicraweb EVO è dotato di diversi strumenti per il reporting ed esportazioni dati che permettono di coprire tutte le casistiche che vanno dal report pixel perfect alla stampa unione con sostituzione di segnalibri sino a stampe con script in meta-linguaggio per avere controllo completo sul risultato finale. Per le esportazioni è possibile configurare vari parametri come la schedulazione e la destinazione delle operazioni di esportazione.

Nel complesso, il layer di back-office è quindi una piattaforma funzionalmente completa e tecnologicamente avanzata nativamente integrata in tutti i suoi moduli applicativi in modo da garantire trasversalità e consistenza nella gestione degli oggetti di business dell'applicativo.

Il front-office di Sicraweb EVO si configura come una Single Page Application (SPA) che sfrutta un meccanismo di routing proprietario e la flessibilità dei web components per un'interazione utente fluida e immediata senza necessità di ricaricare l'intera pagina. Questo approccio consente transizioni rapide e una navigazione continua, migliorando l'esperienza d'uso e i processi di lavoro. I componenti della user interface vengono, infatti, caricati in modalità lazy attraverso un meccanismo proprietario, che ottimizza il consumo delle risorse e riduce i tempi di inizializzazione, allocando le risorse solo quando effettivamente necessarie.

Al centro del layer di front-office è presente il container web, responsabile del caricamento dei componenti e gestore dello loro ciclo di vita. Il container web si occupa in maniera centralizzata della gestione dell'autenticazione, assicurando un accesso sicuro e personalizzato per ogni utente, e della comunicazione interna tramite un bus dedicato che facilita lo scambio di informazioni tra i componenti. Contestualmente, vengono implementati rigorosi meccanismi di sicurezza e accessibilità, conformi alle Linee Guida per la Sicurezza Informatica della Pubblica Amministrazione. Sul fronte dell'accessibilità, l'interfaccia utente rispetta le direttive WCAG 2.1, segue le Linee Guida AgID per l'Accessibilità dei Siti e Strumenti Digitali e recepisce le indicazioni dell'Accessibility Act. In aggiunta, il container integra un sistema di messaggistica che recepisce le notifiche push del back-office tenendo gli utenti costantemente aggiornati su eventi e modifiche in tempo reale.

Ogni componente ha una struttura interna a sua volta stratificata in cui la presentation logic è ben disaccoppiata dalla view del componente e dal relativo stile. La coerenza grafica e di user experience dell'interfaccia utente sono garantite dall'adozione di un framework base comune a tutte le applicazioni verticali. Grazie a questa uniformità, ogni

elemento delle view rispetta linee guida condivise per l'interazione, migliorando la facilità d'uso per l'utente finale. L'impiego di Angular per la gestione della presentation logic consente inoltre di sfruttare funzionalità avanzate e di organizzare il codice in maniera modulare, favorendo l'innovazione e la scalabilità dell'intero sistema.

La persistenza dei dati e file è gestita disaccoppiando la comunicazione con i DBMS e i sistemi di storage dalla logica di business tramite una logica a plugin. Questo approccio consente una gestione indipendente e trasparente delle operazioni di persistenza. Attualmente, la nostra piattaforma integra i principali database, tra cui PostgreSQL, Oracle e SQL Server. Parallelamente, il sistema supporta soluzioni di storage basate su NFS e repository remoti, inclusi bucket S3 compliant.

La logica a plugin permette di estendere facilmente il catalogo dei sistemi integrati aggiungendo nuove tecnologie. In questo modo, ogni nuova integrazione avviene senza impattare la logica di business assicurando una rapida adattabilità alle evoluzioni tecnologiche e alle nuove esigenze normative nel contesto della Pubblica Amministrazione.

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 Sicraweb 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 Sicraweb 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 Sicraweb EVO.
- La metodologia SAMM suddivide il ciclo di vita del software in cinque funzioni aziendali chiave: Governance, Design, Implementation, Verification e Operation. Per

Sicraweb 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 Sicraweb 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

- **Gestione Utenti e accessi**

L'autenticazione è gestita tramite un modulo di piattaforma dedicato la cui responsabilità è quella di identificare l'utente che sta tentando di connettersi al sistema e di crearne una sessione di lavoro nel caso in cui l'utenza sia riconosciuta e verificata. Il modulo propone, oltre all'implementazione di login nativa basata su credenziali, un catalogo di integrazioni che vanno da quella nativa con LDAP / Active Directory ad Identity Provider (IdP) esterni compliant con protocolli di autorizzazione quali SAML, OAuth2.0 e OpenID. Grazie a questi protocolli standard e utilizzando la tecnica della federazione tra IdP, Sicraweb EVO è in grado di integrare l'autenticazione dei vari sistemi previsti da normativa come ovviamente SPID, CIE, CNS così accessi eseguiti tramite Multi-Factor Authentication (MFA).

Tutte le funzionalità di Sicraweb EVO sono regolamentate da permessi. Un permesso è un'informazione legata, direttamente o indirettamente, all'utente attualmente connesso al sistema. Il software controlla i permessi prima di consentire ad un utente di eseguire una certa operazione. La gestione e la possibilità di configurazione è molto articolata proprio per andare incontro alle esigenze organizzative più complesse. Oltre a poter assegnare un permesso direttamente ad un utente è possibile assegnare un permesso ad un gruppo (entità logica) il quale a sua volta può contenere uno o più utenti o altri gruppi. L'utente contenuto nel gruppo erediterà i permessi del gruppo che lo contiene. Legata all'organigramma, c'è la possibilità di creare dei Ruoli ai quali assegnare permessi. In questo modo un utente potrà operare come appartenente a più uffici ed avere permessi diversi a seconda del ruolo che ricopre nell'ufficio. Inoltre è prevista la possibilità di specificare delle ACL (Access Control List). Grazie a queste sarà possibile inibire letture, modifiche, cancellazioni di singoli record ad utenti che non sono in possesso di questi permessi. Grazie a questa funzione si riesce a normare le operazioni di cui sopra con un dettaglio estremamente fine.

- **Protezione dati personali**

La protezione dei dati è gestita a vari livelli. A livello tecnico la confidenzialità dei dati è garantita da un modello di comunicazione basato sul protocollo TLS (Transport Layer

Security) sia front-office e servizi di back-office e tra i servizi stessi e il layer di persistenza dei dati.

Inoltre si prevede una sezione del DB criptata, dove vengono inserite:

Le chiavi personali degli utenti: keystore o chiamato anche portachiavi.

Le chiavi di sistema: Security Key Ring.

Ove supportata, è possibile applicare anche la TDE (Transparent Data Encryption) del database. Questa soluzione permette di mantenere un elevato livello funzionale permettendo ricerche complesse anche parziali e di proteggere i file dati a riposo utilizzando la crittografia nativa del DBMS. Seguendo il principio shift left, in aggiunta a queste misure applicate sugli ambienti di installazione del sistema, si adottano tecniche di controllo e verifica del software direttamente in fase di sviluppo. Nello specifico, le pratiche di sicurezza adottate includono regolari analisi SAST (Static Application Security Testing) per identificare vulnerabilità a livello di codice. Vengono inoltre eseguite rilevazioni di segreti esposti attraverso il Secret Detection e uno scanning delle dipendenze per individuare eventuali vulnerabilità nelle librerie esterne. Per garantire costante aderenza agli standard di sicurezza, applichiamo la politica di "No New Security Findings", evitando così l'introduzione di nuove vulnerabilità durante la fase di sviluppo e garantendo un codice sempre conforme agli standard di sicurezza.

Inoltre Sicraweb EVO è sottoposto periodicamente a test di sicurezza approfonditi di tipo VA/PT (Vulnerability Assessment and Penetration Testing), eseguiti sia da un team interno dedicato che da aziende specializzate in cybersecurity, per identificare e mitigare eventuali vulnerabilità.

Dal punto di vista funzionale, Sicraweb EVO offre un sistema di permessi estremamente granulare che permette di profilare le figure amministrative identificate dall'ente per analizzare i log degli accessi e degli eventi del sistema e definire in autonomia gruppi, ruoli, la relativa gerarchia tra essi e portafoglio permessi così come le assegnazioni degli utenti.

- **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, nel caso in cui si adotti il sistema di accesso nativo di Sicraweb EVO basato su credenziali, vengono verificate la lunghezza minima, complessità aging e history della password (entrambi configurabili). In fase di profilatura, il sistema mette a disposizione un cruscotto di assegnazione permessi strutturato su gerarchie di gruppi logici e 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.

- **Gestione dei Log**

La Suite SicraWeb Evo include un sistema di log che registra le operazioni di CRUD (creazione, lettura, aggiornamento ed eliminazione) delle macroentità su tabelle di sistema. Per le modifiche, vengono tracciati sia i dati pre-update che post-update.

I log generati dai sistemi di Maggioli S.p.A. sono gestiti con specifiche politiche di retention, delineate per garantire la conformità normativa, la sicurezza e la piena tracciabilità delle operazioni. La conservazione è delimitata tenendo conto della tipologia di moduli applicativi utilizzati, e quindi dei conseguenti trattamenti. A tal proposito, per maggiori specifiche, si può contattare Maggioli S.p.A.

- **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 Sicraweb 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 della suite Sicraweb 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 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. 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 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

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

Audit e monitoraggio del software

Il software registra in modo sistematico tutte le operazioni rilevanti, tra cui:

- Accessi degli utenti e operazioni critiche effettuate;
- Modifiche a configurazioni o dati sensibili;
- Errori o comportamenti anomali

Questi log sono conservati in modo sicuro e consultabili per eventuali verifiche, facilitando il rispetto di requisiti normativi, la gestione degli incidenti e la diagnosi dei problemi.

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.