



CONDIZIONI
SERVIZI APPLICATIVI SaaS
erogati da DEDA NEXT
(Rev. Gennaio 2025)

Sommario

Introduzione	3
Scopo del Documento	3
Descrizione del Servizio SaaS.....	3
Descrizione dettagliata dei Servizi.....	3
Condizioni di Utilizzo	3
Regole e restrizioni sull'uso del servizio	3
Licenze e diritti d'uso	4
Modalità di Erogazione del Servizio:	5
Modalità di Cessazione del Servizio	6
Modalità di Assistenza del Servizio e Livelli di Servizio (SLA)	6
Manutenzione Software	6
Servizio di Customer Care.....	7
Livelli di Servizio (SLA) del Customer Care.....	7
Modalità di Chiusura segnalazioni del Customer Care.....	8
Livelli di Servizio (SLA) del Servizio SaaS.....	9
Sicurezza e Protezione dei Dati:	10
Conformità normativa	10
Misure di sicurezza	11
Crittografia dei Dati	11
Controllo degli Accessi.....	11
Sicurezza della rete	11
Logging e Monitoraggio.....	12
Test di Sicurezza	14
Backup e Ripristino	14
Formazione e Consapevolezza	15
Conformità e Audit	15
Riservatezza di Dati e Informazioni	15
Report e Penali:	16
Responsabilità e Limitazioni:	17
Garanzie e responsabilità	17
Limitazioni di responsabilità:.....	17

Introduzione

Scopo del Documento

Il presente documento ha lo scopo di definire le **Condizioni che regolano l'utilizzo dei servizi SaaS forniti da DEDA NEXT** (di seguito "Fornitore"). Esse stabiliscono i diritti e gli obblighi dei clienti (di seguito "Clienti") e del Fornitore in relazione all'accesso e all'utilizzo dei servizi offerti. Il documento mira a garantire la conformità alle normative vigenti, incluse le disposizioni dell'Agenzia per la Cybersicurezza Nazionale (ACN).

Descrizione del Servizio SaaS

CIVILIA NEXT è la soluzione cloud nativa per la **gestione integrata del Sistema Informativo dei Comuni, qualificata ACN** (Agenzia per la Cybersicurezza Nazionale) alla [Scheda SA-11](#). Progettata per l'ente che vuole organizzare e gestire nella modalità più avanzata ed efficace i processi interni e progettare in modo flessibile, scalabile e moderno i servizi verso il cittadino. Web nativa, in linea con ANPR, integrata con SPID e PagoPA, utilizzabile via Internet da qualsiasi dispositivo fisso o mobile, comprende moduli applicativi che rispondono alle esigenze operative dei Comuni, Gestioni Associate, Unioni e città Metropolitane e si integra con il Portale dei Servizi Online per cittadini e imprese. Ha una struttura modulare, con un'ampia gamma di funzionalità completamente integrate e aperte all'interoperabilità tramite API. Ulteriori info: www.civilianext.it.

Descrizione dettagliata dei Servizi

Per la descrizione di dettaglio dei servizi offerti si rimanda al paragrafo **"Caratteristiche funzionali del servizio"**, di cui alla succitata [Scheda SA-11](#)

Condizioni di Utilizzo

Regole e restrizioni sull'uso del servizio

Gli Utenti sono tenuti a utilizzare i servizi SaaS forniti da DEDA NEXT in conformità con le seguenti regole e restrizioni:

- **Uso Consentito:** Gli Utenti possono utilizzare i servizi SaaS esclusivamente per scopi legittimi e in conformità con le leggi e i regolamenti applicabili.
- **Divieti:** È vietato utilizzare i servizi per:
 - Attività illegali o fraudolente;
 - Trasmettere contenuti dannosi, offensivi, diffamatori o che violino i diritti di terzi;
 - Tentare di ottenere accesso non autorizzato ai sistemi o ai dati di altri utenti;
 - Interferire con il normale funzionamento dei servizi o dei sistemi di DEDA NEXT.
- **Obblighi dei clienti:** Il Cliente si obbliga, nel rispetto dei piani di attivazione concordati, ad impiegare risorse idonee ad assicurare:
 - il supporto del personale dell'Ente necessario a DEDA NEXT per l'attivazione del servizio SaaS;
 - la configurazione dei propri sistemi di sicurezza (firewall, proxy, ecc.) per la connessione al servizio SaaS;

- ogni cautela necessaria alla protezione dei dati mediante l'installazione di programmi sulle proprie postazioni di lavoro volti alla protezione perimetrale, quali antivirus aggiornati, firewall locali, controlli di protezione degli account del PC, e così via;
- la predisposizione dell'ambiente applicativo sulle postazioni di lavoro utente idoneo al funzionamento del servizio SaaS (Personal Computer, Sistema operativo, Web Browser, ecc.);
- la custodia delle credenziali assegnate per l'utilizzo del servizio SaaS, segnalando immediatamente qualsiasi uso non autorizzato del proprio account;
- la garanzia che non consentirà in alcun modo ed in nessuna forma l'utilizzo delle proprie credenziali di autenticazione e accesso a soggetti terzi e/o estranei alla propria organizzazione, salvo specifica e circostanziata autorizzazione espressa e concordata in forma scritta con DEDA NEXT;
- la comunicazione tempestiva, qualora scopra un eventuale errore nel Software, a DEDA NEXT mediante i canali del Servizio di Customer Care (l'eventuale anticipazione telefonica da parte del Cliente dell'errore, benché gradita, non sarà utilizzata per il calcolo dei livelli di servizio), ivi compresa, a richiesta di DEDA NEXT S.R.L, la fornitura di tutti i dati e documentazione necessaria per riprodurre, diagnosticare e correggere l'errore.

Licenze e diritti d'uso

- **Concessione della Licenza:** DEDA NEXT concede ai Clienti una licenza limitata, non esclusiva, non trasferibile e revocabile per accedere e utilizzare i servizi SaaS in conformità con i presenti Termini e Condizioni.
- **Proprietà Intellettuale:** DEDA NEXT è legittima titolare del Software Civilia e del CIVILIA NEXT, della documentazione tecnica, del relativo know-how, delle metodologie e delle tecniche di elaborazione dei dati impiegati ed è titolare di ogni altro diritto di proprietà industriale inerente i propri Servizi oggetto di un Contratto. Il Cliente si obbliga a:
 - limitare al proprio personale - che ne abbia la necessità per motivi di servizio - la conoscenza e l'uso del Software, dei Servizi e della documentazione, e adottare tutte le misure atte ad assicurarne e garantirne la necessaria segretezza e riservatezza, in modo che non siano pregiudicati i diritti di proprietà intellettuale di DEDA NEXT;
 - non consentire l'uso dei Software, dei Servizi e/o della documentazione a terzi.
- Il Cliente si impegna, anche ai sensi dell'art. 1381 c.c. per ciascun utente, ad utilizzare i Software e gli aggiornamenti e sviluppi nei limiti della licenza d'uso conferita e nel rispetto dei diritti di proprietà intellettuale di DEDA NEXT o di terzi. Pertanto, a titolo esemplificativo e non esaustivo e fatti in ogni caso salvi gli inderogabili limiti di Legge, il Cliente non potrà:
 - aggirare le limitazioni tecniche e le misure tecnologiche di protezione presenti nel software, ivi incluso il sistema di autenticazione;
 - decodificare, decompilare o disassemblare il software;

- riprodurre, modificare, adattare, personalizzare il software o crearne lavori derivati;
 - eseguire o far eseguire copie del software;
 - commercializzare a qualsivoglia titolo il software.
- Restano in capo a DEDA NEXT (e/o, se del caso, ai terzi proprietari) tutti i diritti sui marchi, loghi, nomi, nomi a dominio e altri segni distintivi comunque associati al Software, all'infrastruttura cloud e/o ai servizi cloud.
 - **Restrizioni sulla Licenza:** Gli Utenti non possono:
 - Modificare, copiare, distribuire, trasmettere, visualizzare, eseguire, riprodurre, pubblicare, concedere in licenza, creare opere derivate, trasferire o vendere qualsiasi informazione, software, prodotto o servizio ottenuto tramite i servizi SaaS;
 - Decompilare, disassemblare o effettuare il Reverse Engineering del software utilizzato per fornire i servizi SaaS.
 - **Durata della Licenza:** La licenza concessa agli Utenti è valida per la durata che sarà esplicita nell'eventuale contratto da stipularsi fra le parti, salvo risoluzione anticipata in conformità con i presenti Termini e Condizioni.

Modalità di Erogazione del Servizio:

Il servizio SaaS di CIVILIA NEXT viene erogato **via Web** attraverso la rete Internet avviene all'interno di una **connessione criptata** tramite il protocollo crittografico **HTTPS** (HyperText Transfer Protocol over Secure Socket Layer) da DEDA NEXT mediante attestazione su **Cloud Microsoft Azure con livello ACN di adeguamento 2** (da ora in poi **"Provider"**): **IN-28**. A fronte di sottoscrizione di un contratto di vendita, viene effettuata l'attivazione da parte del personale di DEDA NEXT dell'Ente in CIVILIA NEXT, cui sussegue l'attivazione di un account di amministrazione per l'Ente, che gli fornisce la possibilità poi di gestire le configurazioni dei diversi moduli applicativi e di assegnare ad essi i relativi utenti applicativi.

L'autenticazione al sistema avviene per mezzo di strumenti di autenticazione del Provider, basati Security Assertion Markup Language (**SAML 2.0**) e OpenID Connect (**OIDC**). È inoltre previsto l'autenticazione a due fattori MFA.

La gestione delle autorizzazioni e dei livelli di accesso è realizzata mediante modello **RBAC** (Role Based Access Control) tramite la definizione di gruppi e l'assegnazione di ruoli o permessi secondo il criterio del minimo privilegio.

È responsabilità del Cliente la sicurezza delle proprie credenziali di accesso con obbligo di segnalazione immediata per qualsiasi uso non autorizzato del proprio account.

CIVILIA NEXT è inoltre compatibile al Modello di interoperabilità, definito da AgID con API in formato "Machine Readable" compatibile con le indicazioni del modello d'interoperabilità e per la precisione in **OpenAPI3**, anch'esse soggette a modello di autenticazione e autorizzazione **OAuth2**.

I Datacenter del Provider, su cui sono attivate le applicazioni e memorizzati i dati del Cliente, sono collocati nell'Unione Europea.

Modalità di Cessazione del Servizio

Il Cliente è tenuto a comunicare per iscritto a DEDA NEXT a mezzo **PEC** l'intenzione di rinnovare oppure di cessare di fruire del servizio SaaS per l'annualità successiva **entro il 30 settembre dell'anno in corso**. In caso di:

- richiesta di rinnovo del servizio SaaS: entro la scadenza del periodo contrattuale, nelle modalità previste, il Cliente deve sottoscrivere unicamente gli allegati contenenti le condizioni specifiche della fornitura. **È garantita la continuità operativa;**
- richiesta di recesso dal servizio SaaS: sino al giorno della scadenza del Contratto, DEDA NEXT continua ad erogare il servizio SaaS senza soluzione di continuità, garantendo gli SLA e mantenendo ferme le condizioni economiche vigenti. Entro **15 giorni** dalla data di ricezione della comunicazione di recesso, DEDA NEXT trasmette a mezzo PEC al Cliente il documento che descrive il processo di disattivazione del servizio SaaS che esplicita il piano temporale ed il formato con cui vengono consegnati i dati di cui il Cliente è titolare; il Cliente è tenuto a sottoscrivere il predetto documento entro 15 giorni lavorativi dall'invio dello stesso da parte di DEDA NEXT; in caso di mancata sottoscrizione nei termini, il documento si intende approvato e si procederà alle attività di cessazione del Servizio di seguito descritte. La cessazione del servizio SaaS prevede la restituzione dei dati al Cliente in un massimo di due cicli successivi di invio. Qualora il Cliente richieda assistenza da parte di specialisti DEDA NEXT finalizzata alla dismissione del servizio SaaS per il passaggio ad altra soluzione, verrà predisposta una specifica offerta per le attività di supporto. In ogni caso, fino alla scadenza del contratto, DEDA NEXT presta l'assistenza necessaria secondo correttezza e buona fede, allo scopo di consentire al Cliente l'ordinato trasferimento dei dati di cui è titolare. I dati di cui il cliente è titolare vengono conservati **per un periodo massimo di 180 giorni successivi** alla scadenza dei servizi, e ciò al fine di consentire la corretta esecuzione della procedura di cessazione; il corrispettivo dei servizi include la conservazione dei predetti dati. Decorso tale periodo, in assenza di ulteriori tempestive comunicazioni da parte del Cliente, i dati vengono distrutti. I dati correlati e conseguenti all'erogazione del servizio SaaS (quali, a titolo esemplificativo, i log) vengono conservati nei sistemi DEDA NEXT secondo i tempi previsti dalla qualificazione ACN. Le suddette modalità hanno lo scopo di consentire un'adeguata ed efficiente organizzazione dei servizi di DEDA NEXT ed il rispetto da parte della stessa degli standard di settore e della normativa di riferimento, nonché il diritto del Cliente di avere il pieno possesso dei propri dati.

Modalità di Assistenza del Servizio e Livelli di Servizio (SLA)

DEDA NEXT offre un Servizio di Assistenza e Supporto che si compone dei seguenti tre ambiti.

Manutenzione Software

Esso comprende:

- La **manutenzione correttiva** finalizzata alla "rimozione" di eventuali malfunzionamenti del Software e alla predisposizione di una nuova release, comprensiva della descrizione delle correzioni apportate, che DEDA NEXT renderà disponibile a tutti i clienti;
- La **manutenzione normativa** che prevede l'"aggiornamento" del Software necessario per adeguarsi a mutate disposizioni legislative, regolamentari o amministrative intervenute nel periodo

contrattuale. DEDA NEXT renderà disponibile a tutti i Clienti una nuova release, comprensiva della descrizione delle mutate funzionalità;

- La **manutenzione migliorativa** per il “potenziamento” del Software, consistente nella predisposizione di quei miglioramenti e/o implementazioni che DEDA NEXT renderà di sua iniziativa ed a suo insindacabile giudizio disponibili per tutti i Clienti.

Per il servizio SaaS ciascun rilascio sarà documentato, comunicato preventivamente e attivato centralmente da DEDA NEXT e immediatamente disponibile.

Servizio di Customer Care

Tale servizio sarà erogato da DEDA NEXT (anche tramite propri incaricati), previo ricevimento di una dettagliata richiesta scritta che il Cliente dovrà inviare accedendo al Servizio di Customer Care raggiungibile al link presente in Next Community. I servizi di assistenza e manutenzione di CIVILIA NEXT sono organizzati secondo la metodologia **ITIL V4** e sono conformi allo standard **ISO20000**. L'Assistenza consiste nella comunicazione mediante il **sistema di Trouble-Ticketing del Customer Care** di ogni opportuno chiarimento o suggerimento in merito alle caratteristiche del Software, alle istruzioni necessarie per il corretto uso e per l'individuazione di eventuali disfunzioni o malfunzionamenti.

Il Cliente potrà essere contattato da DEDA NEXT, via telefono o e-mail, a sua discrezione, sulla base del merito della richiesta; eventuali chiarimenti, suggerimenti o istruzioni saranno forniti da DEDA NEXT purché di rapida e semplice comprensione. Qualora la richiesta comporti un'attività riconducibile a formazione o ad una specifica esigenza di configurazione funzionale, DEDA NEXT proporrà al Cliente la pianificazione di un intervento dedicato.

Il Servizio comprende le sole prestazioni sopra elencate in relazione all'ultima release del Software resa disponibile da DEDA NEXT. A titolo esemplificativo e non esaustivo, risultano escluse le seguenti prestazioni:

- modifiche del Software richieste dal Cliente;
- formazione al personale del Cliente comprensiva di fornitura di video-pillole (servizio NEXT COMMUNITY GOLD);
- attività di data entry;
- i costi di telefonia sostenuti dal Cliente;
- i costi per la connessione ad Internet sostenuti dal Cliente;
- le eventuali attività conseguenti alla modifica della configurazione del Software difforme a quanto descritto nei manuali operativi effettuata dal Cliente o da qualsiasi terzo per lui.

Conseguentemente, qualsiasi altro intervento richiesto dal Cliente che non rientri in quanto sopra descritto precedenti dovrà essere valutato da DEDA NEXT ed oggetto di specifica intesa con il Cliente.

Livelli di Servizio (SLA) del Customer Care

Il Servizio di Customer Care viene erogato nei soli **giorni lavorativi, da lunedì a venerdì, dalle ore 8:00 alle ore 18:00 in modalità da remoto**. Previa richiesta scritta da parte del Cliente sarà possibile estendere la

finestra di servizio ad altri orari (ad es.: il sabato mattina); tale richiesta dovrà essere valutata da DEDA NEXT ed oggetto di specifica intesa fra le parti.

DEDA NEXT garantisce i **seguenti livelli di servizio (SLA)** per la **Manutenzione Software Correttiva**:

La classificazione avviene secondo le seguenti categorie di priorità:

- **P1:** Incidenti che causano un'interruzione totale del servizio o un impatto significativo su un gran numero di utenti. Richiede un'azione immediata; fanno parte di questa casistica gli incidenti di sicurezza quali ad esempio un Data Breach. **(Problem)**
- **P2:** Incidenti che causano una riduzione moderata della qualità del servizio e impattano un numero limitato di utenti. Richiede una risposta tempestiva. **(Incident)**
- **P3:** Incidenti che causano un impatto minimo e possono essere risolti senza urgenza. **(Near Miss)**

Priorità	
P1	Alta
P2	Media
P3	Bassa

Impatto	Alto	P2	P2	P1
	Medio	P3	P2	P2
	Basso	P3	P3	P2
		Bassa	Media	Alta
		Urgenza		

PRIORITA'	PRESA IN CARICO (hh)	RISOLUZIONE MIN (hh)	RISOLUZIONE MAX (hh)
P1	1	8	8 (*) - 16
P2	1	16	40
P3	1	40	120

(*) Si precisa che il tempo di Risoluzione Max di 16 ore è da considerarsi sempre pari ad 8 ore in caso di Servizio SaaS completamente o parzialmente bloccato.

La soluzione del problema potrà avvenire temporaneamente anche tramite l'adozione di workaround.

Modalità di Chiusura segnalazioni del Customer Care

Alla chiusura della segnalazione è prevista sempre **una nota** che descrive brevemente le attività svolte, per l'evasione della stessa con notifica da parte del sistema di Customer Care al Cliente con aggiornamento del documento di **"Incident Report"** se necessario con eventuale notifica anche **via mail/PEC** della chiusura della segnalazione. Se l'incidente rientra tra quelli che debbono essere obbligatoriamente notificati al **CSIRT** (<https://www.csirt.gov.it/>), il Responsabile del "Security Incident Response Team" di DEDA NEXT, previa notifica alla Direzione Organization & Compliance, **procede alla notifica telematica**. La Direzione Organization & Compliance, fornisce inoltre supporto nella valutazione di quali altre Autorità od Organi di controllo sia opportuno o necessario informare, in adempimento alla normativa vigente e a tutela della società e del Cliente (quali a titolo di esempio: l'Autorità Nazionale per la Cybersicurezza, il Garante per la protezione dei dati personali; Polizia Postale – C.N.A.I.P, ...)

Oltre all'approccio reattivo, il servizio di Customer Care può intervenire in maniera **preventiva**:

- se la segnalazione necessita di un Hot-Fix per essere risolta e il rilascio non è immediato, ma è noto un Workaround, predispone un messaggio che compare nella home page del sistema di Trouble-Ticketing del Customer Care;
- se il problema è relativo ad un malfunzionamento di una piattaforma di terzi, messaggio che compare nella home page del sistema di Trouble-Ticketing del Customer Care per avvisare tutti gli operatori degli Enti;

Tema importante seguente alla chiusura di un incidente è la fase di “**Lesson Learned**”, che permette di identificare quali azioni potrebbero evitare il ripetersi in futuro e/o limitare gli impatti di simili incidenti, compresi eventuali attività di Change Management o investimenti in interventi software, formazione. Di seguito le fasi previste:

- **Analisi Post-Incidente:** Revisione post-incidente per identificare le lezioni apprese e migliorare i processi di sicurezza.
- **Aggiornamento delle Procedure:** Aggiornamento delle procedure e dei piani di risposta agli incidenti in base alle lezioni apprese
- **Follow-up:** verifica dell'adeguatezza delle procedure di gestione degli incidenti con identificazione dei possibili punti di miglioramento.

Livelli di Servizio (SLA) del Servizio SaaS

Il **servizio SaaS di CIVILIA NEXT** è disponibile **24 ore al giorno per 365 giorni all'anno**, salvo finestre di manutenzione, con **SLO pari al 99,0%**, dove la disponibilità è intesa come la **percentuale di tempo in un mese** in cui il servizio cloud risulta essere accessibile e usabile, specificando che il tempo totale del periodo di riferimento, che funge da base di calcolo del dato percentuale, non tiene conto degli eventi catastrofici (per eventi catastrofici si intendono eventi che rendono indisponibili per un periodo di tempo prolungato le infrastrutture impiegate per l'erogazione del servizio e al verificarsi dei quali è attivata la soluzione di Disaster Recovery).

Sono previste delle specifiche **finestre di manutenzione programmate**:

- Aggiornamenti del sistema per Rilasci Major e Minor Release
- Attività di manutenzione sistemistica
- Eventuali interventi straordinari per la risoluzione di malfunzionamenti bloccanti)

che sono **al di fuori dell'orario “normale” di operatività degli Enti** (giorni lavorativi dal lunedì al venerdì dalle ore 8:00 alle ore 18:00). Tali attività vengono comunicate con almeno **3 giorni di anticipo** sia mediante l'applicazione “Megafono” disponibile in CIVILIA NEXT che mediante sistema di Trouble-Ticketing di Customer Care, che permette di inserire messaggi di manutenzione programmata nella relativa Home Page disponibile agli Enti.

Il supporto tecnico per “**emergenze**” è a disposizione **24 ore al giorno, 7 giorni a settimana** per tutto l'anno.

Per “emergenze” correlate alla tecnologia si intendono eventi come interruzioni del servizio, interruzioni della rete, errori del server e violazioni della sicurezza. Questi eventi sono causati da un'ampia gamma di forze, ad esempio:

- Calamità naturali, come uragani e terremoti.

- Errori di tecnologia e interruzioni dell'alimentazione.
- Cyberattacchi, ad esempio ransomware.
- Errore utente.
- Pandemie ed epidemie.

Per fare fronte ad eventi di questo tipo si utilizzano metodi, procedure e tecnologie che riguardano l'ambito del "Backup e Recovery" così come del "Disaster Recovery".

A tale scopo CIVILIA NEXT è disponibile nelle "Region" del Provider situate all'interno della Comunità Europea che garantiscono ridondanza di tipo "Geo e/o Zone Redundancy" relativamente ai dati. Il Disaster recovery garantisce il ripristino del servizio SaaS alle seguenti condizioni:

- (i) **RPO: max 36 ore** per tutti i dati. Il RPO (Recovery Point Objective) rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso;
- (ii) **RTO: max 36 ore** per tutti i servizi. Il RTO (Recovery Time Objective) rappresenta la durata di tempo e di un livello di Servizio entro il quale un Business Process (ovvero il Sistema Informativo primario) deve essere ripristinato dopo un disastro o una condizione di emergenza (o interruzione), al fine di evitare conseguenze inaccettabili.

Sicurezza e Protezione dei Dati:

Conformità normativa

CIVILIA NEXT è la soluzione cloud nativa per la **gestione integrata del Sistema Informativo dei Comuni**, **certificata qualificata ACN** alla [Scheda SA-11](#).

In conformità al Regolamento generale sulla protezione dei dati personali (Regolamento (UE) 2016/679, "GDPR") e alla relativa normativa di attuazione (di seguito congiuntamente "Normativa Privacy"), il Cliente è (e rimane) unico Titolare del trattamento dei dati personali che potrebbero essere trattati da DEDA NEXT ai fini dell'esecuzione di Contratto fra le parti.

Se nell'ambito delle attività oggetto del Contratto stipulato, è necessario che DEDA NEXT effettui un trattamento di dati personali ai sensi della Normativa Privacy, il Cliente si obbliga sin da ora a

- nominare DEDA NEXT quale Responsabile del trattamento, ai sensi dell'art. 28 del GDPR;
- comunicare a DEDA NEXT le categorie di dati sono oggetto di trattamento. In tal caso, DEDA NEXT opererà secondo le istruzioni e le misure tecniche ed organizzative indicate nel separato atto di nomina a responsabile, che verrà allegato al Contratto e ne diventerà parte integrante e sostanziale.

Misure di sicurezza

Crittografia dei Dati

Le applicazioni Web di CIVILIA NEXT web app utilizzano solo il protocollo **HTTPS** e l'ultima versione di crittografia **TLS 1.2+**. A ognuna di esse è associato un certificato rilasciato da un'autorità certificata di validità annuale.

L'account di archiviazione del Provider crittografa automaticamente i dati in modo permanente nel cloud. I dati in archiviazione vengono crittografati e decrittografati in modo trasparente usando la **crittografia AES a 256 bit**, una delle crittografie a blocchi più solide disponibili ed è conforme a **FIPS 140-2**.

La crittografia di archiviazione è abilitata per tutti i nuovi account di archiviazione e non può essere disabilitata. Poiché i dati sono protetti per impostazione predefinita, non è necessario modificare il codice o le applicazioni per sfruttare la crittografia di archiviazione. Inoltre, tutte le opzioni di ridondanza di archiviazione supportano la crittografia e tutte le copie di un account di archiviazione vengono crittografate. Tutte le risorse di archiviazione vengono crittografate, quali a solo titolo di esempi: inclusi BLOB, dischi, file, code, tabelle, metadati degli oggetti.

Le chiavi per la crittografia sono archiviate e gestite mediante un KEY Vault mediante algoritmo RSA con lunghezza della chiave fino a **4096 bit**. La gestione del ciclo di vita di una chiave nel KEY Vault è stata implementata con la definizione di un 'criterio di rotazione' della chiave questo prevede il rinnovo automatico della chiave in un numero predefinito di mesi con invio di notifica 30 giorni prima della data della scadenza.

Controllo degli Accessi

L'autenticazione al sistema avviene per mezzo di strumenti di autenticazione del Provider, basati Security Assertion Markup Language (**SAML 2.0**) e OpenID Connect (**OIDC**). È inoltre previsto l'autenticazione a due fattori MFA.

La gestione delle autorizzazioni e dei livelli di accesso è realizzata mediante modello RBAC (Role Based Access Control) tramite la definizione di gruppi e l'assegnazione di ruoli o permessi secondo il criterio del minimo privilegio.

È responsabilità del Cliente la sicurezza delle proprie credenziali di accesso con obbligo di segnalazione immediata per qualsiasi uso non autorizzato del proprio account.

Sicurezza della rete

Particolare cura è posta da DEDA NEXT all'impianto e alla sicurezza della rete all'interno del Provider mediante l'utilizzo di Virtual Network (**VNets**) che consentono:

- Isolamento e Segmentazione: Le VNets consentono di segmentare la rete in sottoreti (subnet) per isolare e organizzare le risorse.
- Assegnazione di Indirizzi IP: Le VNets utilizzano intervalli di indirizzi IP privati definiti dall'utente, consentendo un controllo completo sulla configurazione IP.
- Connessioni sicure: Le VNets supportano diverse forme di connessioni sicure, come VPN (Virtual Private Network), ExpressRoute (connessioni private ad alta velocità) e collegamenti punto-punto (VNet Peering).

- Controllo del traffico in ingresso e uscita: Utilizzando Network Security Groups (NSG), Application Security Groups (ASG), e firewall/web application firewall (WAF), è possibile controllare il traffico tra subnet e verso l'esterno.
- Routing personalizzato: Le tabelle di routing possono essere personalizzate per gestire la direzione del traffico verso appliance di rete o altre risorse.

Vengono inoltre utilizzati **Endpoint Privati**, che permettono di stabilire connessioni sicure e provate fra i servizi SaaS e le risorse delle VNets utilizzando IP privati. In tal modo si isola e protegge il traffico, evitando il transito su Internet e migliorando la sicurezza delle connessioni tra le risorse all'interno del Provider. In tal modo si riduce il rischio associato a potenziali attacchi su connessioni pubbliche.

Nell'architettura di rete di CIVILIA NEXT sono stati creati Endpoint privati per molteplici risorse, fra cui si evidenziano:

- Key Vault;
- Database;
- Storage;
- Cache;
- Ricerca;
- Web App.

Infine, il servizio SaaS è protetto da **diversi strumenti di sicurezza di rete**, quali sempre a titolo di esempio, firewall/WAF con funzioni anti-DDoS, NAT gateway, antivirus, anti-malware, security e compliance manager, protezione della superficie d'attacco e così via.

Logging e Monitoraggio

CIVILIA NEXT dispone di **diversi sistemi di logging**; la registrazione di eventi effettuata su file di log o tabelle da parte di componenti sistemistiche o applicative soddisfa le seguenti finalità:

- Registrazione per adempimenti normativi e di auditing;
- Registrazione di eventi per vincoli di natura sistemistica;
- Registrazione di eventi per garantire la protezione dei dati (attività proattive di cyber security);
- Registrazione della sequenza di eventi generati dagli utenti nell'ambito di un processo amministrativo al fine di supportare l'attività di ricostruzione e verifica;
- Verifica del reale utilizzo del servizio o di un utilizzo coerente con le finalità d'uso previste ed autorizzate;
- Per rendicontazione interna ai fini amministrativi;
- Registrazione di eventi a supporto per garantire il regolare funzionamento dei servizi (Troubleshooting).

A solo titolo di esempio si elencano i seguenti sistemi di Log:

- Autenticazione e SSO per tutti gli accessi Web;
- Navigazione dell'utente nelle applicazioni Web;
- Audit Log del DB e dello storage;

- Log applicativo.

I log sono archiviati in modalità “Immutable” per **24 mesi**, dell’account di archiviazione; l’accesso è gestito mediante RBAC. È disponibile a richiesta da parte degli enti la funzionalità di ricerca attraverso applicativo per gli utenti strettamente autorizzati dall’ente.

Il monitoraggio della piattaforma applicativa CIVILIA NEXT avviene mediante l’utilizzo appositi strumenti volti a migliorare le prestazioni, l'affidabilità e la qualità delle applicazioni. Essi possono essere divisi in tre categorie:

- **Strumenti per l’indagine:**
 - Dashboard dell'applicazione: fornisce una valutazione immediata dell'integrità e delle prestazioni dell'applicazione.
 - Mappa delle applicazioni: fornisce una panoramica visiva dell'architettura dell'applicazione e delle interazioni dei componenti.
 - Metriche attive: dashboard di analisi in tempo reale per informazioni dettagliate sulle attività e sulle prestazioni dell'applicazione.
 - Ricerca transazioni: tracciare e diagnosticare le transazioni per identificare i problemi e ottimizzare le prestazioni.
 - Visualizzazione disponibilità: monitorare e testare in modo proattivo la disponibilità e la velocità di risposta degli endpoint dell'applicazione.
 - Visualizzazione prestazioni: esaminare le metriche delle prestazioni dell'applicazione e i potenziali colli di bottiglia.
 - Visualizzazione errori: identificare e analizzare gli errori nell'applicazione per ridurre al minimo i tempi di inattività.
- **Strumenti per il monitoraggio:**
 - Avvisi: consentono di monitorare un'ampia gamma di aspetti dell'applicazione e attivare varie azioni.
 - Metriche: approfondimenti sui dati delle metriche per comprendere i modelli di utilizzo e le tendenze.
 - Impostazioni di diagnostica: configurare l'esportazione in streaming dei log e delle metriche della piattaforma nella destinazione desiderata.
 - Log: recuperare, consolidare e analizzare tutti i dati raccolti nei log di monitoraggio.
 - Cartelle di lavoro: creare report e dashboard interattivi che visualizzano i dati di monitoraggio delle applicazioni.
- **Strumenti di monitoraggio dell’utilizzo:**
 - Utenti, sessioni ed eventi: determinare quando, dove e come gli utenti interagiscono con l'app Web.
 - Funnel: analizzare i tassi di conversione per identificare dove gli utenti progrediscono o si spostano nell'imbuto.
 - Flow: visualizzare i percorsi utente nel sito per identificare aree di coinvolgimento elevato e punti di uscita.
 - Panel: raggruppare gli utenti in base a caratteristiche condivise per semplificare l'identificazione, la segmentazione e la risoluzione dei problemi delle prestazioni delle tendenze.

Inoltre, CIVILIA NEXT mette a disposizione dei propri clienti anche una console dove può verificare autonomamente l’**health status** del Servizio SaaS.

Infine, DEDA NEXT si è dotata mediante il Provider di una soluzione di Security Information and Event Management (**SIEM**) e Security Orchestration, Automation, and Response (**SOAR**), progettata per aiutare a rilevare, prevenire e rispondere a minacce informatiche su larga scala. Si integra con il resto della piattaforma e altri strumenti di sicurezza, raccogliendo dati provenienti da diversi dispositivi, utenti, applicazioni e infrastrutture per fornire visibilità completa sulle attività della rete. I vantaggi principali di tale soluzione sono:

- Integrazione con il cloud.
- Raccolta e analisi di dati su larga scala rilevare minacce e anomalie in tempo reale.
- Analisi delle minacce.
- Automazione delle risposte.
- Collaborazione e risposta agli incidenti.
- Threat Intelligence, integrando diverse fonti di informazioni sulle minacce, permettendo di rafforzare la difesa e rispondere più rapidamente agli attacchi mirati.

I connettori del SIEM/SOAR monitorano a titolo di esempio le seguenti risorse critiche:

- Key Vault;
- Database;
- firewall/WAF.

Test di Sicurezza

Il servizio SaaS erogato da DEDA NEXT è sottoposto a regolati scansioni di test di **vulnerabilità** e di **penetrazione** mediante strumenti di mercato che permettono di evidenziare le debolezze e criticità di security del servizio SaaS. Inoltre, nell'ambito dei test di sicurezza viene effettuata anche l'analisi statica del codice (**SAST**) e quella dinamica (**DAST**).

La pianificazione e eventuale correzione delle criticità è schedulata **3 volte l'anno**.

Backup e Ripristino

Il backup dei dati avviene mediante modalità di tipo Point in Time Restore (**PITR**) che Long Term Retention (**LTR**):

- PITR, che consente la conservazione dei backup a breve termine da 1 a 35 giorni, la periodicità con cui i backup vengono effettuati automaticamente dal Provider è di **5 minuti**. Per CIVILIA NEXT è stato previsto un periodo di conservazione di **35 giorni per gli ambienti di produzione**.
- LTR, per cui è possibile conservare un backup full del database in uno storage ridondato con una retention fino a 10 anni. I backup LTR possono essere ripristinati in un nuovo database. Per CIVILIA NEXT è stata prevista una politica di backup LTR, che prevede un **backup settimanale** con un periodo di conservazione di **6 mesi** per l'ambiente di produzione.

I dati di backup con insieme di credenziali vengono archiviati, in modo che non ci sia accesso diretto a tale archiviazione e al relativo contenuto, garantendo l'isolamento dei dati di backup dall'ambiente di produzione in cui risiede l'origine dati. I dati in transito vengono trasferiti in modo sicuro con i protocolli **HTTPS** e **TLS 1.2+**. Questi dati rimangono in rete interna e separata del Provider. I dati di backup inattivi vengono crittografati per impostazione predefinita usando chiavi gestite dal Provider. Per migliorare la protezione viene inoltre usata l'immutabilità, che impedisce la modifica o l'eliminazione dei dati prima del periodo di

conservazione. Questo approccio solido è volto ad impedire, anche in un ambiente compromesso, che i backup esistenti possano essere manomessi o eliminati da utenti non autorizzati.

Formazione e Consapevolezza

DEDA NEXT si impegna a diffondere la politica e gli obiettivi per la sicurezza delle informazioni a tutto il personale, rendendolo consapevole del proprio contributo all'efficacia del sistema; a tale scopo vengono periodicamente organizzate sessioni di formazione del personale, mediante pillole informative, affinché sia assicurata un'adeguata competenza in materia di sicurezza delle informazioni e dei dati trattati; inoltre, vengono appositamente effettuati test periodici del personale mediante simulazione, quali a titolo di esempio "finte" mail di phishing, smishing o altre tecniche per poi raccogliere il livello di maturità della popolazione aziendali in termini di consapevolezza della cybersecurity.

Conformità e Audit

DEDA NEXT mediante la Direzione Organization & Compliance effettua in **corrispondenza periodica** con la verifica dei requisiti **ISO** anche la corrispondenza con la conformità alle **specifiche ACN**.

DEDA NEXT, inoltre, riconosce al Cliente la possibilità di effettuare una **specificativa attività di audit** finalizzata a verificare il rispetto dei requisiti e degli standard contrattualmente convenuti, nonché la loro puntuale attuazione. Il Cliente si riserva la facoltà di effettuare detta attività utilizzando personale qualificato del Cliente o per il tramite di **soggetti terzi scelti dal Cliente medesimo**, previa sottoscrizione di apposito accordo di riservatezza

Le richieste di accesso devono pervenire per iscritto a DEDA NEXT tramite il Servizio di Customer Care raggiungibile al link presente in Next Community e dovranno essere corredate dall'indicazione dei soggetti incaricati e dei dati/locali interessati.

Al fine di garantire il mantenimento di un adeguato livello di riservatezza e di sicurezza del patrimonio informatico e delle banche dati, nonché della corretta operatività del servizio SaaS, l'attività di cui al presente articolo deve essere organizzata secondo i piani e le modalità da concordare tra le Parti. Le attività devono essere effettuate adottando rigorosamente modalità tali da:

- non pregiudicare la sicurezza, la riservatezza, l'integrità e la disponibilità dei dati (e dei relativi trattamenti) dei quali sono "Titolari" altri utenti;
- non interferire (pregiudicandolo) con il normale e corretto svolgimento delle attività di DEDA NEXT S.R.L.;
- non pregiudicare la riservatezza dell'organizzazione aziendale, commerciale nonché la segretezza delle informazioni aziendali e delle esperienze tecnico-industriali, comprese quelle commerciali, di DEDA NEXT S.R.L.;
- assicurare che gli eventuali accessi vengano effettuati nel rispetto delle misure di sicurezza adottate da DEDA NEXT S.R.L.
- Gli oneri economici connessi agli audit sono carico del Cliente.

Riservatezza di Dati e Informazioni

Cliente e Fornitore, anche successivamente a scioglimento di Contratto, adottano tutte le iniziative organizzative e gli strumenti necessari atti a proteggere la riservatezza dei dati, dei documenti (anche contrattuali) e delle notizie di qualunque natura, attinenti l'attività, l'organizzazione aziendale, i clienti (l'"Informazione", o anche le "Informazioni") e garantiscono reciprocamente che il proprio personale e il

personale di ditte da esse incaricate tratteranno come riservata ogni Informazione della quale venissero a conoscenza durante o in relazione ad ogni attività inerente l'esecuzione del Contratto. In ogni caso il Cliente è responsabile, nei confronti di DEDA NEXT, per fatti e/o omissioni costituenti violazioni dei già menzionati obblighi di riservatezza compiuti dal proprio personale o persone dallo stesso comunque autorizzate a qualsiasi titolo ad accedere ed utilizzare le Informazioni.

L'obbligo di riservatezza riguarda le Informazioni e ogni dato acquisito nello svolgimento delle prestazioni contrattuali a favore del Cliente. In particolare, ciascuna Parte si impegna a:

- garantire che le Informazioni acquisite siano utilizzate unicamente per le finalità di cui al Contratto;
- mantenere riservata e strettamente confidenziale qualsiasi Informazione ricevuta dall'altra Parte e a garantire che nessuna di tali Informazioni venga divulgata a terzi estranei al presente rapporto contrattuale, salvo preventiva autorizzazione scritta da parte dell'altra Parte;
- distruggere o restituire i documenti, le Informazioni e i dati ricevuti e non più necessari ai fini dell'esecuzione del contratto, in caso di richiesta dell'altra Parte e, comunque, dopo la cessazione del rapporto contrattuale, dandone tempestiva comunicazione per iscritto.

Cliente e Fornitore mantengono la titolarità con riferimento alle Informazioni eventualmente comunicate all'altra Parte; in particolare il Cliente mantiene la titolarità connessa ai propri dati, fermo restando quanto disposto dalle leggi in materia.

Non sono considerati riservati i dati e le notizie che sono o divengono di pubblico dominio per causa diversa dalla rivelazione effettuata dalla Parte tenuta al riserbo, dal personale ad essa riferibile, da suoi consulenti o rappresentanti.

DEDA NEXT si impegna a osservare la policy di sicurezza informatica del Cliente, per quanto applicabile; a tal fine, il Cliente mette previamente a disposizione di DEDA NEXT per sua valutazione una copia aggiornata della documentazione relativa alla policy di sicurezza informatica.

DEDA NEXT si impegna a rispettare la propria policy di sicurezza informatica che rende disponibile al cliente a richiesta.

Report e Penali:

Su richiesta del Cliente è prevista la consegna di un report, funzionale alla verifica degli SLA contrattualmente convenuti. La consegna avrà frequenza pari al "periodo di valutazione" fissato su base mensile.

Il calcolo dell'importo delle eventuali penali sarà effettuato esclusivamente sulla base del periodo di valutazione e in base a quanto riportato nel report funzionale. In dettaglio:

- qualora non siano rispettati gli SLA del servizio SaaS per fatto e colpa esclusivi di DEDA NEXT o delle sue terze parti la penale applicabile sarà pari al 25% del corrispettivo relativo al modulo per cui il servizio SaaS non è risultato disponibile rapportato al livello garantito nel periodo di valutazione. L'importo sarà dovuto per scostamenti in diminuzione maggiori/uguali a 3 punti in percentuale sul periodo di valutazione.
- qualora non siano rispettati gli SLA dei servizi professionali a supporto del servizio SaaS per fatto e colpa esclusivi di DEDA NEXT o delle sue terze parti, la penale applicabile sarà pari al 10% del relativo corrispettivo riferito al periodo di valutazione.

Le penali dovranno essere richieste per iscritto dal Cliente entro 15 giorni dalla consegna del relativo report. DEDA NEXT avrà facoltà di sottoporre eventuali giustificazioni scritte entro 15 giorni dalla ricezione della richiesta. Il pagamento di qualsiasi importo eventualmente dovuto avverrà esclusivamente sotto forma di riduzione sui canoni futuri e sarà subordinato all'avvenuto pagamento dei corrispettivi contrattuali per l'anno in corso al momento della violazione.

Responsabilità e Limitazioni:

Garanzie e responsabilità

DEDA NEXT garantisce che il servizio SaaS è erogato con la massima diligenza secondo gli standard stabiliti dalle procedure del sistema di gestione conforme: alla norma UNI EN ISO 9001, alla norma UNI EN ISO 20000, alla norma UNI CEI EN ISO/IEC 27001, alle relative Linee Guida ISO/IEC 27017 e ISO/IEC 27018 nonché alla certificazione etica SA8000. DEDA NEXT non assume alcuna obbligazione oltre a quelle previste da eventuale contratto stipulato.

DEDA NEXT non riconoscerà alcun addebito da parte del Cliente a qualunque titolo per interruzione o mancato adempimento dei Servizi per cause indipendenti dalla propria volontà quali, a titolo esemplificativo, scioperi, calamità naturali, guerra, atti di terrorismo, rivolte o azioni governative, pandemie e altre cause di forza maggiore.

Fatto salvo il caso di dolo o colpa grave per i quali non è previsto alcun limite di responsabilità, DEDA NEXT risponderà dei danni diretti cagionati al Cliente in conseguenza dell'esecuzione di un Contratto e/o delle prestazioni in esso previste entro il limite del corrispettivo annuo del servizio che è oggetto di reclamo. I corrispettivi convenuti per i servizi riflettono tale ripartizione del rischio tra DEDA NEXT ed il Cliente.

Resta inteso che in ogni caso DEDA non è responsabile nei confronti del CLIENTE in relazione al funzionamento o al mancato funzionamento di prodotti software di terze parti o alla fornitura dei relativi servizi, né presta alcuna autonoma garanzia in relazione agli stessi.

Limitazioni di responsabilità:

I Livelli di Servizio non sono applicabili (e conseguentemente non possono essere richieste le relative penali) in caso di problemi di erogazione o indisponibilità:

- derivanti dall'utilizzo di servizi gestiti da altri fornitori, inclusi, a titolo esemplificativo, i problemi causati da larghezza di banda Internet inadeguata o correlati ad Hardware, Software o i servizi di terzi;
- derivanti dall'utilizzo del servizio SaaS da parte del Cliente in modo non conforme alle caratteristiche e alla funzionalità o a quanto descritto nella documentazione o nelle indicazioni pubblicate da DEDA NEXT (ad esempio, tentativi di eseguire operazioni non supportate);
- derivanti dall'esecuzione di attività non autorizzate o dalla mancata esecuzione di attività indicate da DEDA NEXT o dal mancato rispetto delle procedure di sicurezza appropriate (es. impostazione password non conforme ai criteri minimi di sicurezza o diffusione delle stesse);
- derivanti da input, istruzioni o argomenti erranei o da tentativi del Cliente di eseguire operazioni che superino le quote ordinate (es. numero utenti in eccesso) o derivanti dalla limitazione imposta circa i comportamenti offensivi sospetti;

- derivanti all'utilizzo del servizio SaaS durante il periodo di disponibilità ma al di fuori dell'orario garantito delle applicazioni;
- dovuti a fattori al di fuori del ragionevole controllo di DEDA NEXT (ad esempio, calamità naturali, guerra, atti di terrorismo, pandemie, rivolte o azioni governative) oppure a problemi di rete o guasti di dispositivi all'esterno del Provider sia sul sito del Cliente, sia tra il sito del Cliente e il Provider.

Marcello Bova

Market Line Manager – Smart Cities

Deda Next



Stefania
Bentivoglio
01.04.2025
13:16:27
GMT+02:00