Carta dei servizi

EDAM

Sommario

1 Premessa

1.1 Principi fondamentali della Carta dei Servizi

La presente Carta dei Servizi garantisce la trasparenza del servizio EDAM che Sielte S.p.A. fornisce ai propri clienti interni ed esterni. Il documento riporta dettagliatamente le informazioni riguardanti i diritti di cui godono gli utenti e il livello e la qualità dei servizi che Sielte S.p.A. si assume nell'ambito del suddetto servizio. L'Organizzazione tende a mantenere un sistema di gestione di tale servizio sempre idoneo, adeguato ed efficace, mirando a rispettare i seguenti parametri:

- **Semplificazione e trasparenza** delle informazioni, delle procedure e dei principali aspetti normativi che riguardano il servizio erogato.
- **Uguaglianza, imparzialità e collaborazione.** Sielte S.p.A. si impegna a rispettare tutti i diritti degli utenti, senza che vi sia alcuna distinzione di sesso, razza, lingua, religione e opinioni politiche. Ispirandosi a tale principio di uguaglianza, Sielte S.p.A. tutela il trattamento del servizio erogato all'interno delle diverse aree geografiche di utenza e delle diverse categorie di utenti.
- **Efficacia ed efficienza**. Sielte S.p.A. si impegna costantemente nel migliorare l'idoneità, l'adeguatezza e l'efficacia del servizio EDAM. Il contesto è pertanto continuamente oggetto di osservazioni che tengono presenti le modifiche rispetto alle norme internazionali di riferimento, le nuove richieste degli utenti, gli eventi e gli incidenti rilevati dall'Organizzazione.
- **Facilitazione dei contatti e delle opportunità**, garantita attraverso un cortese e disponibile servizio di assistenza tecnica che permette agli utenti di presentare segnalazioni o eventuali reclami.

- **Continuità e disponibilità del servizio.** L'erogazione di tale servizio, nell'ambito delle modalità stabilite contrattualmente e dalle norme internazionali di riferimento, deve essere continua, regolare e senza interruzioni. I casi di funzionamento irregolare o di interruzione del servizio devono essere espressamente regolati dalle procedure di gestione. In tali casi, i soggetti erogatori devono adottare misure volte ad arrecare agli utenti il minor disagio possibile.

La Carta dei Servizi è disponibile al seguente link: https://www.sielte.it/images/documents/carta-servizi-edam.pdf

1.2 Normativa di riferimento

Il servizio EDAM di Sielte S.p.A. è stato implementato rispettando le procedure internazionali dettate dai seguenti standard di riferimento:

- UNI EN ISO 9001:2015
- UNI EN ISO 27001:2022
- UNI EN ISO 20000-1:2018
- ITIL v4

1.3 Descrizione del Servizio

EDAM è l'acronimo di Enterprise Dynamic Activity Management ed è una piattaforma di Work Order Management, accessibile mediante interfaccia web e deployabile indistintamente su piattaforme Microsoft e Linux based. La web application risponde a criteri di usabilità, dinamicità ed efficienza dettati dal

mercato. L'idea di Sielte è quella di adottare e proporre un sistema capace di essere facilmente compreso e rapidamente utilizzabile dagli utenti, sia da postazioni desktop che mobile. L'interfaccia di EDAM è infatti cucita sul lavoro che l'utente deve svolgere. EDAM, infatti, è la soluzione sviluppata da Sielte che consente di gestire le attività operative. Le principali mansioni consistono in: gestione ordini di lavoro, tracciamento delle azioni in tempo reale, completa storicizzazione dei dettagli di lavorazione. Ogni singola attività operativa all'interno della piattaforma corrisponde ad una pratica. L'evoluzione della pratica, da un suo stato iniziale di lavorazione fino allo stato finale di chiusura, viene gestito mediante un motore di workflow configurabile. Il Cliente è dunque in grado di visualizzare le attività di propria competenza e procedere con la lavorazione delle stesse. Per ciascuna attività è possibile tracciare un'ampia varietà di informazioni quali: note, dati specifici, materiale installati e/o recuperati, ecc.
Ogni nuovo rilascio comprende: nuove funzionalità di business (e/o aggiornamento di funzionalità esistenti); nuove funzionalità tecniche volte ad aumentare le disponibilità, le performance e la resilienza del prodotto; funzionalità mandatorie relative alle normative in ambito sicurezza informatica e privacy.

2 Qualità del servizio

2.1 Risk Assessment

Il risk assessment è il processo che consente l'analisi delle minacce che impattano sui processi che Sielte utilizza per erogare servizi ai propri Clienti. Con cadenza almeno annuale o quando si verificano cambiamenti significativi, le minacce ed i relativi rischi vengono analizzati, aggiornati e correlati ai processi aziendali. Le

minacce che generano rischi a impatto per il Cliente vengono trattate secondo programmazione aziendale ovvero incluse nel piano di miglioramento.

2.2 Monitoring

Sielte utilizza tecniche proattive e preventive di monitoraggio dell'infrastruttura e dei servizi erogati. Tutti i componenti dell'infrastruttura sono monitorati attraverso trigger opportunamente configurati.

Tipologia di Allarmi

2.2.1 *Generici tipi di Allarmi*

- Allarme rientrato
- Allarme di livello informativo: non impatta sulle prestazioni, solo per alcuni tipi di metriche.
- Allarme di livello basso: non impatta sulle prestazioni e sulla fruibilità del servizio.
- Allarme di livello alto: pregiudica le prestazioni o la fruibilità del servizio.
- Allarme di livello disastro: interruzione di servizio.

Il Service Desk verifica tutti gli allarmi del monitoraggio e garantisce copertura lunedì-venerdì dalle 07:30 alle 18:30 e il sabato dalle 08:30 alle 17:30.

2.3 Incident Management

L'Incident Management è gestito dal Service Desk. Il processo di gestione degli Incident, mira a ripristinare la normalità di servizio nella maniera più veloce possibile,

con la minima interruzione di servizio al business, assicurando che i migliori livelli di servizio e disponibilità siano mantenuti. Sono considerati incident tutte le segnalazioni di anomalie effettuate dai Clienti, rilevate internamente e/o dai sistemi di monitoring.

Il Service Desk ha principalmente il compito di:

- Raccogliere le segnalazioni provenienti dagli utenti, e dopo aver stabilito se si tratti o meno di un incidente, effettuare le operazioni di categorizzazione, classificazione e assegnazione priorità sul sistema di ticketing.
- Dare supporto iniziale agli utenti e fare il primo tentativo di offrire una soluzione workaround.
- Mantenere gli utenti aggiornati sullo stato delle loro richieste.
- Coinvolgere le parti interessate in base alla tipologia di incidente, inoltrando tutte le richieste che non possono essere risolte direttamente ai gruppi di secondo livello e monitorarne lo stato.
- Fornire informazioni sulle necessità formative degli utenti dei servizi IT e dei servizi Cloud rispetto ai servizi stessi.
- Confermare agli utenti l'effettiva risoluzione degli incidenti.

È possibile segnalare un incident chiamando dal lunedì al venerdì dalle 7:30 alle 18:30 e il sabato dalle 08:30 alle 17:30 al numero di telefono 095.2291711 oppure scrivendo una mail a supporto@sielte.it.

Funzione	Giorni	Festivi	Orario
Helpdesk	LUN/VEN	NO	07:30-18:30
Helpdesk	SAB	NO	08:30-17:30

Sulla base della valutazione di impatto che l'incidente potrebbe avere sui sistemi ICT e sull'erogazione dei servizi di Sielte, gli incidenti di sicurezza delle informazioni sono classificati su 4 livelli di criticità:

Valore	Criticità dell'incidente	tipologia impatto
1	POCO SIGNIFICATIVA	Impatto irrilevante o modesto, possibilità di incontrare piccoli inconvenienti, superabili senza alcun problema
2	QUASI SIGNIFICATIVA	Impatto moderato, ma che richiede interventi mirati da parte dell'Organizzazione, possibilità di incontrare inconvenienti significativi, che dovrebbero essere superabili a dispetto di alcuni problemi (costi aggiuntivi, impossibilità di accesso a servizi, ecc.)
3	SIGNIFICATIVA	Impatto significativo, con possibili conseguenze rilevanti che dovrebbero essere superabili anche se con gravi difficoltà (inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, ecc.)
4	MOLTO SIGNIFICATIVA	Impatto molto significativo, compromesso con necessità di interventi immediati, con conseguenze irreversibili, quindi potrebbero non essere superabili

Il grado di urgenza dell'incidente è valutato sulla base di quanto a lungo un incidente abbia un impatto sull'erogazione dei servizi.

Urgenza		Tipologia di incidente
D	Basso	Incidente gestibile. Potenzialmente irritante, ma non incide in modo sostanziale sull'azienda.
C	Medio	Incidente preoccupante. Timori per le scadenze non rispettate e per i modelli di business significativamente modificati.
B	Alto	Incidente critico. Attività seriamente compromessa, scadenze non rispettate; rischio di incorrere in sanzioni.
A	Urgente	Incidente disastroso. Capacità di continuare l'attività seriamente minacciata. Violazione di norme legali e statutarie, danno d'immagine

Dall'intersezione della criticità con il grado di urgenza si definisce la priorità dell'incidente:

Urgenza \ Criticità	Poco significativo	Quasi significativo	Significativo	Molto significativo
Basso	P4	P4	P3	P3
Medio	P4	P3	P3	P2
Alto	P3	P3	P2	P2
Urgente	P3	P2	P2	P1

A seconda della priorità attribuita all'incidente di sicurezza, vengono coinvolte le figure che possiedono delle responsabilità ben definite per la gestione dell'incidente, se ricade nella propria sfera di competenza.

2.4 Segregation & Networking

La segregazione degli ambienti è garantita dalla caratteristica di EDAM di essere multi-tenant: nello specifico, EDAM è progettato in modo tale che i dati siano logicamente e fisicamente separati, al fine di garantire ad ogni Cliente (tenant) un ambiente virtualmente dedicato.

I dati di ogni tenant sono salvati su un database dedicato ed ogni Cliente può lavorare solamente sui propri dati.

La multi-tenancy di EDAM garantisce che in nessuno scenario i dati di un Cliente possano essere visibili ad utenti terzi o ad altri clienti.

2.5 Log Management

La raccolta dei log, in conformità a quanto previsto dal Provvedimento del Garante della Privacy del 27/11/2008, è centralizzata nei server dello strumento di log

management adottato per la registrazione degli stessi, accessibile solo da parte degli Amministratori di Sistema (quindi personale autorizzato). Le registrazioni (access log) presentano caratteristiche di completezza ed inalterabilità.

2.6 Change Management

Il Cliente, attraverso i canali a sua disposizione, può richiedere una Change Request. Le CR possono essere valutate come manutenzione correttiva del prodotto/servizio o come richiesta di manutenzione evolutiva. La manutenzione correttiva ha la peculiarità di dover essere gestita nella modalità più semplice, efficace e rapida possibile riguardando la rimozione di malfunzionamenti, comunque evidenziati, che sono d'impedimento all'esecuzione o al corretto funzionamento del software applicativo. Nel caso in cui la CR venisse valutata come manutenzione evolutiva, si procede ad avanzare richiesta di autorizzazione al referente del Cliente, al fine di approvare la modifica al sistema e/o ai suoi componenti e la soluzione di massima che è stata individuata in fase di valutazione e di accettare il costo necessario alla sua applicazione.

È possibile richiedere operazioni di Change Management inviando una mail a supporto@sielte.it o chiamando lo 095 2291711.

Tale assistenza viene fornita da personale esperto, coinvolto nelle diverse fasi del progetto stesso. I servizi offerti comprendono le attività di:

- Manutenzione evolutiva limitata, ovvero attività richieste dal cliente, che hanno l'obiettivo di ampliare le funzionalità di EDAM.
- Manutenzione correttiva, mirata all'eliminazione delle anomalie e/o malfunzionamenti rilevati durante la fase di esercizio.
- Gestione degli aggiornamenti critici.
- Supporto e assistenza di utilizzo.

2.7 User Rights Provisioning

EDAM mette a disposizione del Cliente una web application accessibile mediante browser web e connessione ad Internet. Gli utenti potranno accedere sia da dispositivi desktop che da dispositivi mobile. Ogni Cliente dispone di una credenziale di accesso personale che lo identifica all'interno del sistema.

L'accesso ad EDAM, in termini di security, è garantito mediante autenticazione a due fattori con TOTP (Time-Based On-Time Password).

Di seguito, una breve descrizione del processo:

- Il Cliente immette il nome utente e la password per accedere al proprio account.
- È richiesta, come secondo fattore di verifica, la password monouso a scadenza breve (TOTP).
- L'utente fornisce il fattore richiesto, generato in automatico da una applicazione di terze parti che implementa RFC 6238 e che si basa su informazioni dell'utente fornite in precedenza al momento della creazione dell'account

Nei limiti contrattuali è possibile creare, modificare, sospendere ed eliminare le credenziali, contattando il Service Desk, inviando una mail a supporto@sielte.it o chiamando lo 095 2291711.

2.8 Backup & Restore

2.8.1 *Modalità di erogazione del servizio*

Sielte effettua i backup specifici di dati/informazioni/contenuti trattati dal Cliente attraverso tool di backup di livello enterprise. L'applicativo, al fine di non inficiare e

saturare le risorse delle VM, crea dapprima uno snapshot, successivamente utilizza lo stesso per effettuare il backup.
La crittografia degli stessi viene effettuata direttamente dal software di backup.
Il formato dei dati è quello proprietario dell'applicativo: vengono utilizzati un file descrittore ed un file con estensione wbk per i full e vib per gli incrementali, il quale contiene i dati di backup.

È possibile richiedere la variazione della politica di backup o la restore di un servizio attraverso una Change Request inviando una mail a supporto@sielte.it.

2.8.2 *Conservazione dei backup*

Il backup incrementale viene effettuato ogni giorno, il full con cadenza settimanale.

- Vengono conservati gli ultimi 6 backup incrementali giornalieri.
- Viene conservato l'ultimo backup settimanale full.
- Viene conservato l'ultimo backup mensile full.

La locazione dei backup è su una infrastruttura diversa (storage) rispetto all'ambiente di produzione.

Sia i backup full che quelli incrementali vengono ciclicamente conservati ogni settimana su nastro e riposti dentro cassaforte ignifuga dentro locali Sielte.

I nastri in cassaforte vengono poi sovrascritti a rotazione con un "retention time" di quattro settimane.

2.8.3 *Integrità dei backup*

L'applicativo garantisce l'integrità del dato e la sua consistenza attraverso delle metodologie e delle logiche proprietarie di backup. Inoltre, due volte l'anno Sielte

effettua delle simulazioni di ripristino, al fine di verificare se l'immagine ripristinata sia integra e consistente.

Le tempistiche di ripristino si attestano sulle sei ore circa per l'intera infrastruttura, circa 30 minuti per VM.

2.9 Temporary files

Il prodotto non genera file temporanei.

2.10 Vulnerability Assessment / Penetration Test

Sono necessarie periodiche attività di VA/PT sul sistema EDAM. Il software, il firmware e l'hardware utilizzati per il sistema vengono riesaminati regolarmente, al fine di rilevare le vulnerabilità nel sistema stesso e di risolvere tali vulnerabilità e i difetti. La verifica di vulnerabilità del sistema (Vulnerability Assessment) avviene con cadenza trimestrale. Sono altresì previsti Penetration Test per i sistemi esposti su rete pubblica con cadenza almeno semestrale.

2.11 Patching

Sielte garantisce ai propri Clienti il patching (SW e OS) secondo best practices dei vendor.

2.12 SLA Management

Gli SLA del servizio EDAM vengono esplicitati all'interno della Scheda d'Ordine sottoscritta dal Cliente.

2.12.1 *Casi che non fanno parte della garanzia SLA*

- Manutenzione programmata del datacenter.

- Malfunzionamenti della connettività del Cliente.
- Altri problemi non derivanti da un malfunzionamento dei datacenter del fornitore.

2.12.2 *SLA*

Lo SLA è basato sul servizio ed è valido per tutti i Clienti.

Tipologia SLA	Tipo	TTO (Time to own)	TTR (Time to resolve)
SLA01	Incident *Assistenza per risoluzione di problemi tecnici*	Entro **8** ore lavorative	Entro **3** giorni lavorativi nel 90% dei casi su base annuale
SLA02	Richieste di Supporto *Assistenza per informazioni*	Entro **3** giorni lavorativi	Entro **5** giorni lavorativi nel 95% dei casi su base annuale

Legenda:

TTO (Time to own): Tempo di presa in carico

TTR (Time to resolve): Tempo di risoluzione

Nota: TTO e TTR misurati dall'istante di apertura dell'incident/richiesta di supporto.

2.12.3 *Uptime*

Come dichiarato all'interno del cap. 16 della Scheda d'Ordine sottoscritta dal Cliente, dove sono presenti maggiori dettagli e approfondimenti, SIELTE si impegna a mettere in atto la massima disponibilità della sua infrastruttura garantendo una continuità di servizio e rispetto degli SLA in una percentuale non inferiore al 99,7%, su base annuale.

L'Uptime sopra indicato può essere scorporato nei seguenti parametri:

- Alimentazione elettrica e della climatizzazione.

- Accessibilità tramite rete Internet.
- Disponibilità dell'infrastruttura fisica.

2.13 Criptography

Sielte garantisce lo scambio crittografato dei dati attraverso protocolli di sicurezza standard.

EDAM è una applicazione multi-tenancy: i dati dei clienti sono raccolti sullo stesso schema di EDAM ma su database separati.

La protezione degli account utente viene garantita attraverso la crittografia HMACSHA512 messa a disposizione dal framework ASP.Net core. In questo modo tutte le password utente vengono offuscate sul database e la codifica hmacsha512 rende ardua la decodifica.

A livello di trasporto, la sicurezza viene garantita attraverso l'utilizzo del protocollo https con standard TLS 1.3.

2.14 Policy sviluppo sicuro

Sielte stabilisce, documenta, manutiene e applica ai suoi progetti e ai suoi servizi IT i principi per l'ingegnerizzazione dei sistemi sicuri.

Al fine di garantire la massima sicurezza e disponibilità degli ambienti di sviluppo di modifiche ai servizi IT, viene implementata una netta separazione degli ambienti di sviluppo dagli ambienti di test e staging (preproduzione). Lo sviluppo viene effettuato mediante l'uso di opportuni ambienti di Dev.

In tutte le fasi di pianificazione, progettazione e transizione di servizi IT viene dato particolare peso alla gestione dei dati personali, utilizzando misure e tecniche

organizzative per la loro tutela, basandosi sui principi della privacy by design e by default.

- Data Protection by design: valutare e analizzare sin dalle fasi di progettazione gli strumenti e le corrette impostazioni a tutela dei dati personali, al fine di prevenire ogni forma di rischio; utilizzare tecniche di pseudonimizzazione o minimizzazione dei dati.
- Data Protection by default: utilizzare i dati personali solo per le finalità previste; utilizzare i dati personali solo per il periodo necessario alla finalità prevista.

Vengono adottati i principi di sviluppo del codice sicuro e sono eseguite, infatti, delle verifiche periodiche sia per quanto riguarda il controllo statico del codice sorgente sia mediante le attività pianificate di VA/PT per l'ambiente di produzione.

2.15 La tutela degli utenti

Sielte S.p.A. si impegna a trattare i dati personali ricevuti nell'ambito del servizio di EDAM nel rispetto del principio di necessità e delle altre garanzie fissate dall'Informativa sul trattamento in materia di dati personali (D.L. vo n. 196/2003) e dal Regolamento UE n.679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR).

Sielte S.p.A. garantisce di ricorrere a sistemi affidabili e protetti da eventuali alterazioni, volti alla memorizzazione dei dati in maniera verificabile.

2.16 Gestione dei reclami e delle non conformità

La gestione e delle non conformità viene strutturata e gestita secondo quanto previsto dalle procedure aziendali in materia.

A seconda delle esigenze quali, veicolare i reclami, avere supporto o chiedere informazioni si può scegliere una tra le seguenti modalità di contatto:

- Attraverso il sito istituzionale si possono inoltrare reclami o richieste di informazioni, compilando l'apposito form.
- È a disposizione degli utenti un servizio di Call Center con operatore disponibile dal lunedì al venerdì, dalle ore 7:30 alle ore 18:30 e il sabato dalle 08:30 alle 17:30, raggiungibile al numero 095 2291711.

