



CITTA' DI ROVATO (Provincia di Brescia)

AVVISO PUBBLICO DI PREINFORMAZIONE PER RICHIESTA
DI OFFERTA SU SINTEL PORTALE ARCA DELLA REGIONE LOMBARDIA.

MANIFESTAZIONE DI INTERESSE PER LA SELEZIONE DI DITTE DA INVITARE A GARE TELEMATICHE
PER IL SERVIZIO DI DIGITALIZZAZIONE.

Allegato Tecnico

Il sistema software dovrà essere in grado di gestire le revisioni parziali e totali del Manuale di Gestione (ai sensi dell'art. 5 del DPCM 03/12/2013 – “Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005”) impostato sulla base dello schema individuato dalla Soprintendenza Archivistica della Lombardia ed impostato orientativamente sui seguenti documenti:

- Testo del Manuale;
- Glossario;
- Normativa di Riferimento;
- Atti di: istituzione Area organizzativa Omogenea - nomina Responsabile Servizio per la tenuta del protocollo informatico, della gestione documentale e degli archivi - nomina Responsabili della Conservazione dei documenti aziendali;
- Piano di Organizzazione;
- Abilitazioni all'accesso al sistema di gestione documentale e protocollo informatico;
- Piano di conservazione archivi analogici;
- Titolario di classificazione e Massimario di scarto;
- Caselle posta elettronica certificata (PEC);
- Documenti esclusi dalla protocollazione e registrazioni particolari;
- Linee guida di scrittura per la protocollazione;
- Registro di emergenza;
- Linee guida per la predisposizione, formalizzazione e consultazione dei provvedimenti amministrativi informatici;
- Linee Guida per le pubblicazioni all'Albo on-line;
- Trasmissioni telematiche e servizi on-line per il cittadino;

- Criteri generali per la formazione dei fascicoli e Piano di fascicolazione.

Il Sistema dovrà inoltre consentire di elencare, descrivere e collegare ai relativi fascicoli tutti i procedimenti amministrativi/affari/attività effettuate dall'ente, le istanze e le altre tipologie documentarie contenute nei singoli fascicoli.

Il sistema dovrà essere in grado di produrre tutta la documentazione richiesta dal D.Lgs. 196/2003, "Codice in materia di protezione dei dati personale" ed in particolare:

- Elencazione e descrizione del trattamento dei dati personali;
- Elaborazione e redazione delle lettere d'incarico per tutti i soggetti che a vario titolo effettuano trattamenti di dati personali, con esplicita indicazione dei compiti affidati;
- Descrizione delle procedure di backup e ripristino dati, comprese le modalità di custodia dei supporti di backup: redazione dei documenti inerenti le procedure per il backup, la verifica e il ripristino dei dati con eventuali proposte di adeguamento
- Descrizione dei sistemi di protezione logici e fisici adottati per proteggere la struttura informatica (firewall, antivirus, antispyware, antispam, cifratura dei collegamenti, armadio di rete, etc.);
- Elaborazione e redazione delle Informativa previste dall'Articolo 13 del D.Lgs. 196/2003;
- Analisi, elaborazione e redazione dei moduli personalizzati per il conferimento del consenso per il trattamento dei dati personali;
- Redazione della documentazione necessaria inerente i siti web prevista dalla normativa (Informativa ai sensi dell'Articolo 13 del D.Lgs. 196/2003) con particolare attenzione alle procedure di pubblicazione di atti e documenti amministrativi effettuati per finalità di pubblicità (Albo on-line) e trasparenza (Amministrazione trasparente);
- Elaborazione e redazione di istruzioni e individuazione degli ambiti di incarico dei soggetti che trattano dati personali (dipendenti e collaboratori);
- Elaborazione, redazione e consegna di istruzioni (vademecum) sul corretto utilizzo degli strumenti elettronici (personal computer, notebook, tablet, smartphone, etc.) e della documentazione cartacea in relazione al trattamento dei dati personali;

Il sistema dovrà essere in grado di produrre il Piano della sicurezza informatica, volto alla delineazione e descrizione di tutte le procedure tecnico-informatiche relative alla formazione, gestione, trasmissione,

interscambio, accesso e conservazione dei documenti informatici, secondo quanto disposto dalle recenti Regole tecniche in materia di protocollo informatico (DPCM 3 dicembre 2013).

Piano di informatizzazione

La Legge 11 agosto 2014, n. 114, che ha convertito, con modificazioni, il D.L. 90/2014 ha introdotto il comma 3-bis all'art. 24 che stabilisce che "...le amministrazioni statali, il Governo, le regioni e gli enti locali devono adottare un piano di informatizzazione delle procedure per la presentazione di istanze, dichiarazioni e segnalazioni che permetta la compilazione on line con procedure guidate accessibili tramite autenticazione con il Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese. Le procedure devono permettere il completamento della procedura, il tracciamento dell'istanza con individuazione del responsabile del procedimento e, ove applicabile, l'indicazione dei termini entro i quali il richiedente ha diritto ad ottenere una risposta. Il piano deve prevedere una completa informatizzazione".

Il sistema dovrà essere in grado di realizzare il piano di informatizzazione come previsto dal legislatore in modo da indicare per ogni procedimento le modalità e le tempistiche per la digitalizzazione dei servizi di front office e di back office.

Il riferimento normativo inerente la materia della continuità operativa è l'art. 50 bis del CAD il quale recita quanto segue:

Art. 50-bis. Continuità operativa. 1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività. 2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento. 3. A tali fini, le pubbliche amministrazioni definiscono: a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale; b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione. 4. I piani di cui al comma 3 sono adottati da

ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA. 1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività. 2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento. 3. A tali fini, le pubbliche amministrazioni definiscono: a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale; b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione. 4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA”

Il sistema dovrà essere in grado di produrre lo studio di fattibilità, il piano di continuità operativa ed il piano di disaster recovery i quali descrivano le soluzioni tecnologiche e le soluzioni tecniche adottate dall'ente in tale materia per garantire l'operatività di sistemi e servizi. Le materie specifiche trattate dal piano dovranno essere:

- I servizi in ambito nello SFT
- La sintesi del parere di AgID
- Variazioni eventuali nel numero dei servizi e relative criticità
- Matrice servizi/organizzazione (responsabilità)
- Matrice servizi/infrastruttura tecnologica

Predisposizione all'emergenza

- La struttura organizzativa
- Comitato di crisi ICT
- Responsabile della Continuità Operativa ICT
- Strutture tecniche
- Composizione, ruoli, procedure operative
- Gestione delle reperibilità

Soluzione di continuità

- Interrelazioni del servizio/i con entità esterne all'amministrazione
 - Dati logistici generali
 - Dati logistici specifici
 - Infrastrutture di continuità e protezione fisica
 - Controllo fisico degli accessi (impianti e procedure)
 - Ambiente logistico (interno) per la continuità
 - Apparati hw e postazioni di lavoro
 - Sw ambiente
 - Sw applicativo
 - Rete interna
 - Rete esterna
- Istruzioni operative di start up
- Gestione dei sistemi hw,sw, di rete in situazioni di normalità
- Scenari di emergenza applicabili

- Fase di reazione all'emergenza
- Fase di gestione dell'emergenza e riattivazione dei servizi
- Fase di ritorno alla normalità

Fattori critici e di rischio, descrizione dei casi di disastro

- Eventi riconducibili al comportamento umano
- Eventi riconducibili agli strumenti informatici
- Eventi riconducibili al contesto fisico-ambientale infrastrutturale

Piano di prevenzione della corruzione

Il P.T.P.C rappresenta lo strumento attraverso il quale l'amministrazione sistematizza e descrive il processo finalizzato a definire una strategia di prevenzione del fenomeno corruttivo. In esso si delinea un programma di attività derivante da una preliminare fase di analisi che, in sintesi, consiste nell'esaminare l'organizzazione, le sue regole e le sue prassi di funzionamento in termini di "possibile esposizione" al fenomeno corruttivo.

Il P.T.P.C. è un programma di attività, con indicazione delle aree di rischio e dei rischi specifici, delle misure da implementare per la prevenzione in relazione al livello di pericolosità dei rischi specifici, dei responsabili per l'applicazione di ciascuna misura e dei tempi.

Il sistema consente la realizzazione del piano e di tutti gli allegati correlati rispetto ai seguenti temi:

- Le aree di rischio obbligatorie
- Altre aree di rischio
- Modalità di valutazione delle aree di rischio
- Misure di prevenzione utili a ridurre la probabilità che il rischio si verifichi
- Formazione generale
- Formazione specifica

- Indicazione dei criteri di rotazione del personale
- Indicazione delle disposizioni relative al ricorso all'arbitrato con modalità che ne assicurino la pubblicità e la rotazione
- Elaborazione della proposta di regolamento per disciplinare gli incarichi e le attività non consentite ai pubblici dipendenti
- Elaborazione di direttive per l'attribuzione degli incarichi dirigenziali con la definizione delle cause ostative al conferimento e verifica dell'insussistenza di cause di incompatibilità
- Definizione di modalità per verificare il rispetto del divieto di svolgere attività incompatibili a seguito della cessazione del rapporto
- Elaborazione di direttive per effettuare controlli su precedenti penali ai fini dell'attribuzione degli incarichi e dell'assegnazione ad uffici
- Adozione di misure per la tutela del whistleblower
- Predisposizione protocollo di legalità per gli affidamenti
- Realizzazione del sistema di monitoraggio del rispetto dei termini, previsti dalla legge o dal regolamento, per la conclusione dei procedimenti
- Realizzazione di un sistema di monitoraggio dei rapporti tra l'amministrazione e i soggetti che con essa stipulano contratti e indicazione delle ulteriori iniziative nell'ambito dei contratti pubblici
- Indicazione delle iniziative previste nell'ambito dell'erogazione di sovvenzioni, contributi, sussidi, ausili finanziari nonché attribuzione di vantaggi economici di qualunque genere
- Indicazione delle iniziative previste nell'ambito di concorsi e selezione del personale
- Indicazione delle iniziative previste nell'ambito delle attività ispettive

Funzionalità specifiche del sistema

- Al fine di consentire la realizzazione di quanto descritto nel paragrafo precedente il sistema dovrà contenere le seguenti sezioni tematiche:

- Organigramma dell'ente (POA) – dovrà consentire l'inserimento delle singole unità organizzative aziendali, descrivere i rapporti gerarchici/funzionali tra le stesse e descriverne ogni altra caratteristica;
- Personale dell'ente (con relativi ruoli) – dovrà consentire di elencare tutto il personale dell'ente descrivendone caratteristiche contrattuali e ruoli
- Titolare – tipologie di fascicoli – tipologie di documenti – dovrà consentire l'inserimento e la gestione del titolare aziendale con i relativi rapporti gerarchici tra i diversi livelli dello stesso, il collegamento del titolare con le tipologie di fascicoli e registri utilizzati dall'Azienda, le tipologie di documenti che saranno legati ai singoli fascicoli o ai singoli registri
- Procedimenti/affari/attività – descrizione dei procedimenti/affari/attività svolte dall'ente con le relative caratteristiche
- Trattamenti dati personali – descrizione dei trattamenti di dati personali svolti dall'ente
- Strumenti tecnologici – dovrà consentire di mappare e descrivere la struttura informatica dell'Azienda attraverso i dati necessari al fine della realizzazione del Piano della Sicurezza Informatica di cui al DPCM 03/12/2013 (“Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005”)
- Software – dovrà consentire di elencare e descrivere i software utilizzati dall'ente
- Mail – dovrà consentire di elencare tutte le caselle di PEO e di PEC in utilizzo presso l'Azienda
- Strutture fisiche (sedi ed uffici) – dovrà consentire di mappare e descrivere tutte le caratteristiche delle sedi e degli uffici aziendali
- Enti esterni – dovrà consentire di elencare e descrivere i soggetti giuridici esterni aventi accesso ai sistemi informativi aziendali.

Le diverse sezioni sopra elencate dovranno collegarsi le une con le altre al fine di rendere un quadro completo della struttura e dell'attività dell'ente secondo il seguente schema:

- Organigramma dell'ente (POA) – per ogni livello gerarchico/funzionale dell'organigramma, oltre alle caratteristiche specifiche che il sistema dovrà consentire di mappare in modo dinamico (cioè su indicazione dell'Azienda che verrà fornita in fase di installazione e configurazione del sistema) sarà necessario collegare al livello stesso le seguenti entità: personale collegato all'unità organizzativa, strutture fisiche (sedi ed uffici) nei quali l'unità organizzativa esercita la propria attività, elenco delle

mail/PEC utilizzate dall'unità organizzativa, elenco dei Procedimenti/affari/attività svolte dall'unità organizzativa, tipologie di documenti prodotti/ricevuti dall'unità organizzativa, strumenti informatici attraverso i quali l'unità organizzative esplica le proprie funzioni;

- Personale dell'ente: per ogni persona inserita nell'elenco, oltre alle caratteristiche specifiche che il sistema dovrà consentire di mappare in modo dinamico (cioè su indicazione dell'Azienda che verrà fornita in fase di installazione e configurazione del sistema) sarà necessario collegare la persona stessa alle seguenti entità: all'unità organizzativa alla quale la risorsa è stata assegnata, alle sedi ed agli uffici nei quali svolge la propria attività, agli strumenti informatici in dotazione, ai procedimenti/affari/attività nei quali è coinvolto, ai software ai quali è autorizzato ad accedere;
- Titolare – tipologie di fascicoli – tipologie di documenti. Per ogni fascicolo, oltre alle caratteristiche specifiche che il sistema dovrà consentire di mappare in modo dinamico sarà necessario collegare il fascicolo stesso alle seguenti entità: procedimenti/affari/attività dai quali deriva la produzione documentaria che verrà archiviata nel fascicolo. Per ogni tipologia documentaria oltre alle caratteristiche specifiche che il sistema dovrà consentire di mappare in modo dinamico (cioè su indicazione dell'Azienda che verrà fornita in fase di installazione e configurazione del sistema) sarà necessario collegare la tipologia stessa alle seguenti entità: software attraverso il quale la tipologia documentaria verrà prodotta, unità organizzative collegate al ciclo di vita della tipologia documentaria esaminata;
- Strumenti tecnologici - oltre alle caratteristiche specifiche che il sistema dovrà consentire di mappare in modo dinamico (cioè su indicazione dell'Azienda che verrà fornita in fase di installazione e configurazione del sistema) sarà necessario collegare lo strumento stessa alle seguenti entità: alle installazioni software connesse allo strumento, al personale autorizzato ad utilizzare lo strumento, agli enti esterni aventi accesso alla risorsa tecnologica ed alle unità organizzative assegnatarie delle strumenti;
- Software - oltre alle caratteristiche specifiche che il sistema dovrà consentire di mappare in modo dinamico, sarà necessario collegare il software stesso alle seguenti entità: soggetti titolari di credenziali di accesso al software, soggetti esterni titolari di credenziali di accesso al software, tipologie documentarie realizzate con il software;
- Mail - oltre alle caratteristiche specifiche che il sistema dovrà consentire di mappare in modo dinamico, sarà necessario collegare l'indirizzo mail stesso alle seguenti entità: al personale ed alle unità organizzative titolato ad utilizzare l'account;
- Enti esterni: i collegamenti tra gli enti esterni e le altre entità sono descritti e desumibili dai punti precedenti

Una volta terminata la fase di redazione iniziale della documentazione oggetto del presente incarico il software dovrà proporre procedure guidate per l'aggiornamento dei contenuti dei documenti al verificarsi degli eventi modificativi della struttura organizzativa e tecnologica aziendale.

Licenza d'uso del sistema

La licenza d'uso del sistema dovrà avere le seguenti caratteristiche:

- Periodo di validità illimitato nel tempo;
- Numero di utenti illimitato.

Installazione

Il sistema software dovrà essere installato presso i sistemi server del fornitore ed accessibile da remoto mediante collegamento protetto.

Attività di installazione, configurazione, popolamento ed assistenza

L'attività di installazione e configurazione iniziale del sistema sarà a carico del fornitore, così come l'assistenza e l'aggiornamento dello stesso per tutta la durata del rapporto definita dalla presente procedura.

L'attività di popolamento iniziale del sistema, sarà a carico del fornitore, una volta terminata la fase di popolamento iniziale le successive modifiche saranno effettuate dai responsabili dell'ente.

Al termine del presente incarico la licenza d'uso acquistata dall'Ente rimarrà di proprietà dello stesso il quale deciderà se stipulare apposito contratto di assistenza / manutenzione / aggiornamento.

Assistenza giuridica ed archivistica

Nel percorso di avviamento e popolamento del software viene richiesta al fornitore una assistenza non solo di carattere tecnico-informatico ma anche di natura giuridica ed archivistica specialistica volta alla impostazione delle scelte di fondo necessarie alla predisposizione dei documenti prodotti dal sistema software.

L'attività di assistenza giuridica dovrà essere prestata da soggetti specializzati in ambito archivistico ed in materia di tutela dei dati personali/data protection.

Valore del servizio.

Il contratto ha un valore **stimato** complessivo pari a € 12.000,00 oltre iva 22%.

Il Responsabile del procedimento
ing. Giuseppe Tripani
(documento firmato digitalmente)
