

Parma, 03/07/2025

Spett. Comune di Parma
Strada della Repubblica, 1
43121 Parma

c.a. Dott. Nicola Ferioli

Prot.: 2025/280/U
Commessa: 01_2025_034
Referente IT.CITY: Berti Fabio

OGGETTO: Progetto Cyber Security ACN 2024 - CUP: I99B24000040006 – Business Impact Analysis e Business continuity

Facendo seguito alla VS. gentile richiesta Vi sottoponiamo la nostra proposta economica per la fornitura in oggetto, meglio dettagliata nella scheda tecnica in allegato e riepilogata nella seguente tabella:

Descrizione	Q.tà	Tariffa unitaria	Importo
Aggiornamento governance interna secondo lo standard internazionale ISO/IEC 27001:2022			40.000,00
Business Impact Analysis (BIA) e Business Continuity & Disaster Recovery (BC&DR)			50.000,00

Imponibile	€ 90.000,00
Iva 22%	€ 19.800,00
TOTALE	€ 109.800,00

Condizioni di Fornitura

Validità dell'offerta	30 gg data ricevimento
IVA	Gli importi sono al netto dell'IVA
Consegna	60 gg dall'affidamento
Modalità di fatturazione	Al collaudo
Pagamento	30 gg data fattura

In attesa di un Vostro cortese riscontro, siamo a disposizione per ogni eventuale chiarimento.
Distinti saluti.

Sottoscritta digitalmente
IT.CITY S.p.A.
a socio unico

Dott. Pezzuto Fabrizio
Amministratore Unico

IT.CITY S.p.A. dichiara che, nell'ambito delle procedure di acquisizione delle attrezzature hardware, dei relativi accessori, di licenze software e dei pacchetti applicativi, ha provveduto ad esperire le necessarie indagini di mercato al fine di reperire le migliori quotazioni e garantire la massima economicità e che tutta la documentazione acquisita è disponibile in visione negli uffici amministrativi della Società.

Si prega di inserire nella conferma d'ordine il n. commessa IT.CITY della presente offerta.

c_g337.Comune di Parma - Prot. 07/07/2025.0193087.E



SCHEDA TECNICO FUNZIONALE SINTETICA

commessa 01_2025_034

OBIETTIVO: Potenziamento della resilienza cyber - Avviso pubblico n. 08/2024 ACN - CUP: I99B24000040006

CONTESTO DI RIFERIMENTO:

SITUAZIONE ESISTENTE: L'infrastruttura tecnologica e i servizi digitali del Comune di Parma non sono completamente conformi agli standard di resilienza cyber internazionali quali ad esempio l'ISO/IEC 2700 esponendo l'Amministrazione Comunale a potenziali incidenti di sicurezza. Per adeguare i livelli di cyber resilienza, il Comune di Parma ha partecipato all'Avviso pubblico n. 08/2024 dell'Agenzia per la Cybersicurezza Nazionale "Interventi di potenziamento della resilienza cyber - PA" per la presentazione di proposte di interventi di potenziamento della resilienza cyber dei grandi Comuni, dei Comuni capoluogo di Regione, delle Città Metropolitane, delle Agenzie regionali sanitarie e delle Aziende ed enti di supporto al Servizio Sanitario Nazionale, delle Autorità di sistema portuale, delle Autorità del Bacino del Distretto idrografico e delle Agenzie regionali per la protezione dell'ambiente, a valere sul PNRR DIGITALE (MISSIONE 1 COMPONENTE 1) - "INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER - PA" PROMOSSO DALL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE, IN QUALITA' DI SOGGETTO ATTUATORE DELL'INVESTIMENTO 1.5 "CYBERSECURITY" - FINANZIATO DALL'UNIONE EUROPEA NEXT GENERATION EU

SITUAZIONE FINALE: Per rafforzare le infrastrutture e i servizi digitali, e migliorare le competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza, It.City su indicazione e in collaborazione con il Settore Transizione Digitale del Comune di Parma ha sviluppato ed attivato il progetto denominato «L'evoluzione della cyber security a 360°.
Dalla formazione alle tecnologie innovative».

La settima fase delle attività di progetto, riferite all'intervento "Miglioramento dei processi e dell'organizzazione", prevede:

- 1) l'intera rivisitazione e revisione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di It.City in conformità allo standard internazionale ISO/IEC 27001;
- 2) un processo di Business Impact Analysis (BIA) sui Servizi Demografici (Anagrafe, elettorale, stato civile, etc..) e sui Servizi di Protocollo e archivio documentale;
- 3) la redazione della struttura del documento di Business Continuity, dei contenuti essenziali, del supporto e affiancamento in tutte le decisioni da prendere da parte dell'organizzazione, e, a seguito di queste, nella redazione corrette delle parti del documento collegate;
- 4) la redazione del Piano di Disaster Recovery in conformità con le normative vigenti.

La rivisitazione e revisione del SGSI di It.City, in conformità allo standard internazionale ISO/IEC 27001, prevede:

- a) la ridefinizione dell'elenco dei documenti interni (governance) conformi e necessari allo standard internazionale sopra menzionato;
- b) la revisione e riaggiornamento degli attuali documenti ancora conformi e necessari allo standard internazionale sopra menzionato;
- c) la definizione dei documenti mancanti, necessari e richiesti dallo standard internazionale sopra menzionato.

Il processo di BIA prevede le seguenti macro-fasi/ambiti:

1. Pianificazione e avvio: Definizione degli obiettivi, Identificazione del gruppo di progetto
2. Raccolta delle informazioni: Interviste e questionari ai responsabili di funzione
3. Analisi degli impatti: Valutazione degli impatti potenziali in caso di interruzione su base temporale: impatto dopo 4h, 24h, 72h, etc.

4. Determinazione dei parametri critici: MTD (tempo massimo di inattività tollerabile), RTO (tempo entro cui il processo deve essere ripristinato), RPO (perdita massima di dati accettabile)
5. Classificazione e priorità: Classificazione dei processi in base alla criticità, Definizione delle priorità di ripristino
6. Validazione e revisione

Il piano di business continuity prevede le seguenti macro-fasi/ambiti:

1. Garantire la continuità operativa: Assicurare che le funzioni aziendali critiche possano continuare anche durante un'interruzione
2. Minimizzare l'impatto sull'organizzazione: Ridurre al minimo le perdite economiche, reputazionali e operative
3. Proteggere persone e risorse: Salvaguardare la sicurezza dei dipendenti, dei clienti e delle infrastrutture
4. Rispondere in modo coordinato: Fornire un piano strutturato per la gestione delle emergenze e delle comunicazioni

Il piano di disaster recovery prevede le seguenti macro-fasi/ambiti:

1. Ripristinare i sistemi IT: Riattivare rapidamente server, reti, database e applicazioni dopo un disastro
2. Ridurre il downtime: Limitare il tempo di inattività dei sistemi critici (Recovery Time Objective - RTO)
3. Limitare la perdita di dati: Minimizzare la perdita di dati (Recovery Point Objective - RPO) attraverso backup regolari
4. Automatizzare e testare i processi: Implementare soluzioni automatizzate e testare regolarmente i piani di ripristino
5. Supportare la Business Continuity: Fornire il supporto tecnologico necessario per l'attuazione del piano di business continuity

VINCOLI E PREREQUISITI:

REFERENTE PER IL COMUNE DI PARMA: