CITTA' DI TORINO

DIPARTIMENTO SERVIZI INTERNI
DIVISIONE SISTEMI INFORMATIVI
S. INFRASTRUTTURE E CYBERSECURITY

ATTO N. DD 5335 **Torino, 08/09/2026**

DETERMINAZIONE DIRIGENZIALE

OGGETTO: TRATTATIVA PRIVATA MEPA N. 6540710 AI SENSI DELL'ART. 50, COMMA 1, LETTERA B) DEL D.LGS. 36/2023 E S.M.I- COMPLETAMENTO DELLE ATTIVITA' DI SUPPORTO AGLI ADEMPIMENTI DELLA DIRETTIVA NIS 2 SULLA CYBERSECURITY. INDIZIONE E AFFIDAMENTO A EY ADVISOR SP.A. P. IVA 13221390159 IMPORTO 168.360,00 (IVA 22% INCLUSA) CIG BCDFF25CA3

Premesso che l'articolo 8, comma 4 del Regolamento Comunale per la Disciplina dei Contratti della Città di Torino n. 411, approvato con Deliberazione del Consiglio Comunale n. 730/2024, esecutiva dal 29 dicembre 2024, attribuisce al Servizio scrivente la competenza per la negoziazione relativa al gruppo merceologico oggetto del presente provvedimento;
Considerata l'esigenza di garantire il completamento delle attività di supporto agli adempimenti della Direttiva NIS2 sulla cybersecurity, mediante il rafforzamento delle capacità di resilienza operativa e cyber, attraverso la revisione del piano di continuità operativa, l'estensione dell'analisi del rischio cyber unitamente all'implementazione del processo di gestione del rischio delle terze parti e la valutazione dei fornitori rilevanti, è necessario provvedere all'acquisto del servizio in oggetto;
Considerato che i beni/servizi in oggetto non sono reperibili nelle Convenzioni Consip attive ma, a seguito di verifica sul sito www.acquistinretepa.it, sono presenti sul Mercato Elettronico della Pubblica Amministrazione nel Bando "SERVIZI" categoria merceologica "Servizi informatici: consulenza, sviluppo di software, Internet e supporto"- CPV 72000000-5;
Si ritiene pertanto opportuno procedere tramite il Mercato Elettronico della Pubblica Amministrazione (di seguito MEPA), ai sensi del combinato disposto dell'art. 48, comma 3 del D.Lgs. 36/2023 e s.m.i. e dell'art. 1, comma 450, della L. 296/2006 e s.m.i. e dell'art. 50, comma 1, lett. b) del D.Lgs. 36/2023 e s.m.i., ed è stato pertanto acquisito il relativo CIG BCDFF25CA3 con il quale è stata conclusa la trattativa diretta MEPA n. 6540710 a favore della ditta EY ADVISORY S.P.A P. Iva 13221390159 in quanto l'operatore economico identificato, con riguardo in particolare al principio di risultato, all'esperienza pregressa dell'operatore economico e alla congruità del prezzo, garantisce la migliore scelta considerato che si tratta di un'attività di completamento di un

percorso già intrapreso, i cui documenti sono conservati agli atti del Servizio scrivente.
Il Comune di Torino, a partire da dicembre 2022, ha avviato un percorso strutturato di definizione del Piano strategico e della roadmap evolutiva delle iniziative in ambito cybersecurity, con l'obiettivo di rafforzare progressivamente il livello di protezione della propria security posture. Nel corso del biennio successivo, l'Ente ha realizzato numerose iniziative finalizzate al consolidamento dei presidi di sicurezza, alla razionalizzazione dei processi e al rafforzamento del modello di governance cyber. Nel corso del 2026 si da continuità al rafforzamento delle attività già avviate nel 2025, che hanno riguardato la definizione di un modello operativo per la gestione degli adempimenti NIS2 e la revisione di ulteriori documentazioni.
Attestato pertanto che l'operatore economico selezionato risulta in possesso di idonee e documentate esperienze pregresse evincibili da apposita documentazione conservata agli atti del Servizio ai sensi dell'art. 50, comma 1, lett. b) del D.Lgs. 36/2023 e s.m.i;
L'avvio del procedimento di affidamento non vincola la Civica Amministrazione alla conclusione del medesimo e alla stipulazione del contratto, essendo entrambe subordinate alla effettiva disponibilità di risorse economiche adeguate;
A seguito della verifica del preventivo pervenuto dall'operatore economico, agli atti del Servizio scrivente, che ammonta ad Euro 138.000,00 oltre ad Euro 30.360,00 per IVA al 22%, per una spesa complessiva di Euro 168.360,00, con il presente provvedimento si procede dunque all'approvazione dell'affidamento diretto ai sensi del combinato disposto dell'art. 48, comma 3 del D.Lgs. 36/2023 e s.m.i., dell'art. 1, comma 450, della L. 296/2006 e s.m.i. e dell'art. 50, comma 1, lett. b) del D.Lgs. 36/2023 e s.m.i. del servizio in argomento;

I prezzi di affidamento saranno impegnativi per tutta la durata del servizio per l'affidabilità del fornitore;
Dato atto che è stato reinvitato il contraente uscente ai sensi dell'art. 49, comma 4 del D.Lgs. 36/2023, in quanto, considerata la scadenza normativa del 31 ottobre 2026, è emersa la necessità di consolidare e completare il percorso di adeguamento già avviato, indirizzando prioritariamente gli interventi richiesti dal framework NIS2. In considerazione del percorso pluriennale svolto e della conoscenza maturata sul contesto organizzativo, sui processi e sulle iniziative già realizzate, nonché per il consolidamento di alcuni interventi avviati nel corso dei precedenti incarichi, è stato richiesto ai professionisti EY di garantire continuità al supporto specialistico fornito per garantire la piena Compliance alla Direttiva NIS2*;*
Si dà atto che l'operatore economico ha accettato l'impegno all'osservanza sia del Patto di Integrità della Città di Torino, di cui all'allegato 1.1 al Regolamento Comunale per la Disciplina dei Contratti della Città di Torino n. 411, sia del Codice di Comportamento della Città;
Si attesta che i controlli in relazione alla verifica del possesso dei requisiti di carattere generale di cui agli artt. 94 e 95 del D.Lgs. 36/2023 e s.m.i. hanno dato esito positivo

Si da atto che, ai sensi dell'art. 55, comma 2 del D.Lgs. 36/2023 e s.m.i. non si applica il termine dilatorio previsto dall'art. 18, comma 3, lett. d), perché trattasi di affidamento di contratti di importo inferiore alla soglia di rilevanza europea e pertanto si procederà alla stipula del contratto nei modi di cui all'art. 18 del citato Decreto;
Si dà atto che l'esigibilità delle obbligazioni riferita all'impegno di spesa avverrà entro il 31/12/2026;
Richiamati i principi contabili in materia di imputazione delle spese di cui al D.Lgs. 118/2011, così come integrati e corretti con il D.Lgs. 126/2014;
Si dà atto che il presente provvedimento è rilevante ai fini della pubblicazione nella sezione "Amministrazione Aperta".

Tutto ciò premesso,

IL DIRIGENTE

- Visto l’art. 107 del Testo Unico delle leggi sull’Ordinamento degli Enti Locali, approvato con D.Lgs 18 agosto 2000 n. 267
- Visto l’art. 74 dello Statuto della Città;
- Visti gli artt. 182, 183 e 191 del D.Lgs. 267/2000 e s.m.i.;
- Visto l'art. 3 del D. Lgs 118/2011 e s.m.i.;
- Richiamato il principio contabile della gestione finanziaria di cui all'allegato 4/2 del D.Lgs. 118/2011 e s.m.i.;
- Visto il vigente Regolamento comunale di contabilità armonizzata;
- Nell'ambito delle risorse finanziarie assegnate;

DETERMINA

- di attestare che la fornitura/il servizio oggetto dell’affidamento rientra nelle competenze d’acquisto attribuite dall’articolo 8, comma 4 del Regolamento Comunale per la Disciplina dei Contratti della Città di Torino n. 411 approvato con Deliberazione del Consiglio Comunale n. 730/2024, esecutiva dal 29 dicembre 2024;
- di attestare che la fornitura/il servizio in oggetto non è reperibile nelle Convenzioni Consip attive, ma è presente sul Mercato Elettronico della Pubblica Amministrazione nel seguente Bando: “BENI/SERVIZI”- Categoria merceologica: “Servizi informatici: consulenza, sviluppo di software, Internet e supporto”- CPV 72000000-5;
- di dare atto che è stato reinvitato il contraente uscente ai sensi dell’art. 49, comma 4 del D.Lgs. 36/2023, in quanto, considerata la scadenza normativa del 31 ottobre 2026, è emersa la necessità di consolidare e completare il percorso di adeguamento già avviato, indirizzando prioritariamente gli interventi richiesti dal framework NIS2. In considerazione del percorso pluriennale svolto e della conoscenza maturata sul contesto organizzativo, sui processi e sulle iniziative già realizzate, nonché per il consolidamento di alcuni interventi avviati nel corso dei precedenti incarichi, è stato richiesto ai professionisti EY di garantire continuità al supporto specialistico fornito per garantire la piena Compliance alla Direttiva NIS2*;*
- di dare atto dell’insussistenza di un interesse transfrontaliero certo ex art. 48, comma 2 del D.Lgs. 36/2023 e s.m.i, per il modesto valore dell’affidamento;
- di dare atto che il presente provvedimento non è pertinente alle disposizioni in materia di valutazione dell'impatto economico;
- di affidare, per le motivazioni espresse in narrativa, la fornitura/il servizio in oggetto mediante mercato elettronico MEPA, ai sensi del combinato disposto dell’art. 48, comma 3 del D.Lgs. 36/2023 e s.m.i. e dell’art. 1, comma 450, della L. 296/2006 e s.m.i. e dell'art. 50, comma 1, lett. b) del D.Lgs. 36/2023 e s.m.i., attraverso lo strumento della Trattativa Diretta, alla ditta EY ADVISORY S.P.A sita in Via Meravigli 14, 20123 Milano (MI) - p. IVA 13221390159 per un importo complessivo di Euro 138.000,00 oltre ad Euro 30.360,00 per IVA al 22%, per una spesa complessiva di Euro 168.360,00, imputando la stessa come da dettaglio economico finanziario;
- di attestare che non è stata richiesta la garanzia definitiva per l'affidabilità del fornitore;
- di dare atto che è stata acquisita la dichiarazione dell’operatore economico del rispetto della clausola di *pantouflage*o *revolving doors* in attuazione dell’art. 53, comma 16-ter del D.Lgs. 165/2001 e s.m.i.;

- di dare atto che l'operatore economico ha dichiarato di essere in regola con il versamento contributivo e assicurativo;
- di dare atto che, ai sensi dell'art. 55, comma 2 del D.Lgs. 36/2023 e s.m.i., al presente affidamento non si applica il termine dilatorio di cui all'art. 18, comma 3 lett. d) del citato decreto, trattandosi di affidamento di contratti di importo inferiore alla soglia di rilevanza europea;
- di autorizzare la stipula del contratto nei modi di cui all'art. 18 del citato Decreto e la successiva emissione dell'ordine di acquisto a favore della ditta EY ADVISORY S.P.A P. Iva 13221390159;
- di dare atto che il Responsabile Unico del Progetto è il Dirigente del Servizio dott. Massimo Massimo;
- di attestare che l'esigibilità delle obbligazioni riferite all'impegno di spesa avverrà entro il 31/12/2026;
- di dare atto che, per quanto riguarda le transazioni relative ai pagamenti che verranno effettuati a favore della ditta affidataria verranno rispettate le disposizioni dell'art. 3 della Legge 136/2010 e s.m.i. in materia di tracciabilità dei flussi finanziari;
- di attestare che la presente determinazione è stata sottoposta al controllo di regolarità amministrativa ai sensi dell'art. 147-*bis* TUEL e che con la sottoscrizione si rilascia parere di regolarità tecnica favorevole;
- di dichiarare, ai sensi dell'art. 6 *bis* della L. n. 241/1990 e delle disposizioni del Codice di Comportamento della Città, l'insussistenza di cause di conflitto di interesse, anche potenziale in capo al sottoscritto/alla sottoscritta Dirigente *(***qualora le figure non coincidano)* e al RUP.

Si dà atto che il presente provvedimento è rilevante ai fini della pubblicazione nella sezione internet "Amministrazione Aperta".

Dettaglio economico-finanziario

Si impegna la somma di euro 168.360,00 con la seguente imputazione:

Importo	Anno Bilancio	Missione	Programma	Titolo	Macro Aggregato	Capitolo Articolo	Servizio Responsabile	Scadenza obbligazione
168.360,00	2026	01	03	1	03	026900003003	027	31/12/2026
Descrizione capitolo e articolo		*SISTEMI INFORMATIVI - ACQUISTO DI SERVIZI - SERVIZI DI SUPPORTO SPECIALISTICO PER LA TRASFORMAZIONE DIGITALE - settore 027*						
Conto Finanziario n°		Descrizione Conto Finanziario						
U.1.03.02.19.011		*Processi trasversali alle classi di servizio*						

Si dichiara, ai sensi dell'art.6 bis della L. n. 241/1990 e s.m.i. e delle disposizioni del Codice di Comportamento della Città, l'insussistenza di cause di conflitto di interesse, anche potenziale, in capo al/alla sottoscritto/a

IL DIRIGENTE
Firmato digitalmente
Massimo Massimino

NIS2: attività di supporto agli adempimenti normativi

Proposta di estensione attività cyber

Luglio 2026

The better the question. The better the answer. The better the world works.

Shape the future with confidence

Comprensione del contesto e necessità



Contesto

Il Comune di Torino, a partire da dicembre 2022, ha avviato un percorso strutturato di definizione del Piano strategico e della roadmap evolutiva delle iniziative in ambito cybersecurity, con l'obiettivo di rafforzare progressivamente il livello di protezione della propria security posture.

Nel corso del biennio successivo, l'Ente ha realizzato numerose iniziative finalizzate al consolidamento dei presidi di sicurezza, alla razionalizzazione dei processi e al rafforzamento del modello di governance cyber.

Alla luce dell'evoluzione del contesto normativo, e in particolare dell'entrata in vigore della Direttiva NIS2 e delle determinazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN), il Comune ha individuato l'esigenza di proseguire nel percorso di miglioramento continuo, orientando le attività verso un rafforzamento strutturale della compliance e della resilienza operativa.

Obiettivi

Supportare il Comune di Torino nel percorso di adeguamento alla normativa NIS2 mediante il rafforzamento delle capacità di resilienza operativa e cyber, attraverso la revisione del piano di continuità operativa, l'estensione dell'analisi del rischio cyber unitamente all'implementazione del processo di gestione del rischio delle terze parti e la valutazione dei fornitori rilevanti.

Percorso di adeguamento alla Direttiva NIS2

A partire da Dicembre 2022, il Comune di Torino ha introdotto un percorso di adeguamento ai requisiti della Direttiva NIS2, attraverso programmi strutturati, finalizzati all'identificazione di aree di miglioramento e delle relative priorità di intervento.



ATTIVITÀ 2023/2024

Nel corso del 2023 e del 2024 è stato avviato un percorso di affiancamento volto alla valutazione del livello di maturità in ambito cyber.

L'attività ha consentito di individuare i principali ambiti di miglioramento volte al rafforzamento della struttura organizzativa e al monitoraggio delle performance dei presidi di sicurezza.



ATTIVITÀ 2025

Attraverso l'introduzione della Direttiva NIS2, nel corso del 2025 sono state avviate delle attività volte all'identificazione dello stato di conformità rispetto ai requisiti NIS2.

Sulla base dell'identificazione sono state avviate delle prime attività di adeguamento, tra cui l'analisi del rischio cyber, la verifica del corpus documentale e la formazione verso il top management.



ATTIVITÀ 2026

Nel corso del 2026 si da continuità al rafforzamento delle attività già avviate nel 2025, che hanno riguardato la definizione di un modello operativo per la gestione degli adempimenti NIS2 e la revisione di ulteriori documentazioni.

*Considerata la scadenza normativa del **31 ottobre 2026**, è emersa la necessità di consolidare e completare il percorso di adeguamento già avviato, indirizzando prioritariamente gli interventi richiesti dal framework NIS2.*

*In considerazione del **percorso pluriennale svolto e della conoscenza maturata sul contesto organizzativo**, **sui processi e sulle iniziative già realizzate, nonché per il consolidamento di alcuni interventi avviati nel corso dei precedenti incarichi,** è stato richiesto ai professionisti EY di garantire continuità al supporto specialistico fornito per garantire la piena Compliance alla Direttiva NIS2.*

01

Proposta attività EY

Programma Cybersecurity – Attività Compliance NIS2

*Si riportano di seguito, a titolo riepilogativo, le **4 iniziative** sulle quali il **Comune di Torino**, anche a seguito dei precedenti Piani dei Fabbisogni e dello svolgimento degli assessment (trasversale e verticale), ha richiesto un ulteriore supporto qualificato:*

Piano continuità operativa

Valutazione e revisione del piano di continuità operativa per applicazioni e sistemi critici/rilevanti, tramite censimento, raccolta e documentazione delle strategie esistenti, con identificazione di gap e azioni di aggiornamento

1

Analisi del Rischio Cyber

Estensione dello svolgimento dell'analisi del rischio cyber, sulla base della metodologia definita, al fine di definire il livello di rischio dei 6 sistemi rilevanti rimanenti

2

Formazione NIS2
Vertici aziendali

Esecuzione di due sessioni formative dedicate ai vertici aziendali finalizzate ad aggiornare il management sullo stato di avanzamento del percorso di compliance alla Direttiva NIS2, con approfondimento dei principali requisiti normativi applicabili, degli adempimenti previsti, delle responsabilità degli organi di governance e delle attività necessarie per garantire il mantenimento della conformità nel tempo.

5

Processo di gestione terze parti
(TPRM-Process)

Predisposizione di criteri e strumenti per la gestione del rischio fornitori, con aggiornamento di requisiti per gara/contratti, impostazione dei controlli di conformità e pianificazione di audit periodici supportati da linee guida interne

3

Self-Assessment terze parti
(TPRM-Assessment)

Esecuzione di un self-assessment basato su checklist per 2 fornitori, con l'obiettivo di verificare la loro aderenza alle misure di sicurezza previste e valutarne la conformità agli standard principali in ambito Security e Privacy..

4

1: Piano di continuità operativa

L'attività è finalizzata all'analisi e all'aggiornamento del Piano di Continuità Operativa al fine di verificarne l'adeguatezza rispetto ai requisiti NIS2 e assicurare la copertura degli applicativi critici e rilevanti, in coerenza con le risultanze della BIA e con i requisiti di RTO/RPO.

OBIETTIVI

- Verificare l'adeguatezza del Piano di Continuità Operativa rispetto ai requisiti NIS2 applicabili
- Assicurare la copertura degli applicativi critici e rilevanti, in coerenza con BIA e classificazioni di impatto
- Rafforzare la resilienza operativa e la capacità di risposta a scenari di indisponibilità No building, no people, no ICT, no supplier.
- Garantire un approccio strutturato, documentato e periodicamente aggiornabile per i sistemi in perimetro

DELIVERABLE

- Piano di Continuità Operativa aggiornato in ottica NIS2, contenente:
  - Mappatura delle strategie di continuità per applicativi rilevanti
  - Evidenze di coerenza degli indicatori RTO/RPO identificati e misure di continuità operativa

ATTIVITA' PREVISTE

1. ***Analisi del Piano di Continuità operativa***
2. ***Verifica della copertura degli applicativi critici e rilevanti***
3. ***Valutazione della coerenza con BIA e requisiti RTO/RPO***
4. ***Identificazione dei principali gap rispetto alla NIS2***
5. ***Aggiornamento del Piano di Continuità Operativa***

2: Analisi del rischio cyber

L'attività è finalizzata all'esecuzione periodica dell'analisi del rischio cyber, sulla base della metodologia definita, al fine di valutare il livello di rischio dei nuovi 6 asset rientrati in perimetro, identificando gap e definendo le priorità di mitigazione.

OBIETTIVI

- Ottenere una visione strutturata del livello di rischio cyber associata ai nuovi applicativi/asset critici in perimetro
- Identificare gap e aree di miglioramento prioritarie, utili a indirizzare interventi mirati.
- Prioritizzare le azioni di remediation in base al rischio cyber associato e supportare la pianificazione delle azioni correttive.

DELIVERABLE

- Livello di rischio per i 6 applicativi/sistemi (output strutturato per i sistemi in scope).
- Evidenze tecniche e organizzative raccolte a supporto dell'analisi e delle valutazioni.
- Report contenente le risultanze emerse, priorità e piano di rimedio

ATTIVITA' PREVISTE

1. ***Condivisione del file di compilazione con Referenti Business***
2. ***Raccolta delle informazioni***
3. ***Inserimento delle informazioni al portale***
4. ***Definizione e aggiornamento del piano di trattamento***

3: Processo di gestione delle terze parti

L'attività di Third Party Risk Management è volta a strutturare la gestione del rischio cyber dei fornitori, attraverso criteri di classificazione, presidi contrattuali, strumenti operativi e attività di audit periodico, a supporto del percorso di adeguamento NIS2 dell'Ente.

OBIETTIVI

- Definire un modello strutturato per classificare i fornitori in base alla loro rilevanza cyber per l'Ente.
- Supportare una gestione centralizzata e più tracciabile delle forniture rilevanti dal punto di vista cyber.
- Integrare presidi contrattuali coerenti con il livello di rischio cyber e con la tipologia di fornitura.
- Formalizzare un processo interno chiaro per la gestione dei fornitori.
- Introdurre un presidio periodico di verifica sui fornitori rilevanti, per monitorare rischi cyber e conformità.

DELIVERABLE

- Modello/criteri di classificazione della rilevanza cyber dei fornitori.
- Tool centralizzato a supporto della gestione dell'intero ciclo di vita della fornitura.
- Set di clausole contrattuali Cyber aggiornato.

ATTIVITA' PREVISTE

1. ***Definizione del processo di gestione delle terze parti e dei criteri di rilevanza.***
2. ***Aggiornamento e formalizzazione del disciplinare di gara.***
3. ***Definizione del tool di gestione delle terze parti.***
4. ***Creazione di una linea guida interna per la gestione dei fornitori.***

4: Self-Assessment su fornitori

L'attività è finalizzata all'esecuzione di un assessment di sicurezza su due fornitori selezionati, applicando il processo di Third Party Risk Management definito e utilizzando il questionario CLUSIT, al fine di valutare il livello di rischio cyber della supply chain e individuare eventuali azioni di mitigazione.

OBIETTIVI

- Applicare il processo di Third Party Risk Management definito per valutare concretamente il rischio cyber associato a fornitori selezionati
- Valutare il livello di maturità e di rischio cyber dei due fornitori in relazione ai servizi erogati e all'accesso a sistemi e dati
- Verificare l'effettiva adozione delle misure di sicurezza dichiarate dai fornitori, in coerenza con i requisiti NIS2
- Supportare la gestione del rischio della supply chain e l'identificazione di eventuali azioni correttive e di mitigazione

DELIVERABLE

- Report di TPRM Assessment per ciascuno dei due fornitori analizzati
- Evidenze, risultati e raccomandazioni del questionario CLUSIT

ATTIVITA' PREVISTE

1. ***Selezione dei fornitori***
2. ***Predisposizione e somministrazione del questionario di Assessment CLUSIT***
3. ***Raccolta e analisi delle evidenze***
4. ***Valutazione del rischio e identificazione dei gap***
5. ***Sintesi dei risultati e raccomandazioni***

5: Formazione NIS2 ai vertici aziendali

L'attività mira a consolidare la conoscenza del quadro normativo NIS2 e del ruolo degli organi di governance, supportando il management nell'esercizio delle proprie responsabilità e nel rafforzamento della resilienza di sicurezza informatica dell'Ente.

OBIETTIVI

- Indurre i livelli strategici a prendere decisioni informate ed efficienti durante situazioni di crisi cybersecurity
- Sviluppare maggiore consapevolezza nei dirigenti non responsabili della sicurezza in merito al modus operandi e agli impatti di un attacco informatico
- Aumentare la prontezza del Management per una risposta efficace agli incidenti informatici

DELIVERABLE

- Deck formativo comprensivo di report dello status degli adempimenti NIS2
- Questionario con domande di fine corso
- Report delle presenze

ATTIVITA' PREVISTE

1. ***Analisi del status di compliance NIS2 dell'Ente***
2. ***Predisposizione del materiale formativo***
3. ***Condivisione e finalizzazione***
4. ***Pianificazione e somministrazione del materiale formativo***

02

Piano delle attività ed economics

Ipotesi Macro-piano di progetto

Ambito	Attività	Lug				Ago				Sep				Ott				Nov			
		w1	w2	w3	w4	w1	w2	w3	w4	w1	w2	w3	w4	w1	w2	w3	w4	w1	w2	w3	w4
Piano di continuità Operativa NIS2	1) Analisi del piano																				
	2) Verifica della copertura degli applicativi critici e rilevanti																				
	3) Valutazione della coerenza con BIA e requisiti RTO/RPO																				
	4) Identificazione GAP																				
	5) Aggiornamento del piano																				
Analisi del rischio cyber	1) Condivisione e supporto del file di compilazione con Referenti Business																				
	2) Raccolta delle informazioni e inserimento al portale																				
	3) Definizione e aggiornamento del piano di trattamento																				
Processo di gestione delle terze parti	1) Metodologia TPRM																				
	2) Criteri di rilevanza e clausole (disciplinare di gara)																				
	3) Definizione del tool																				
	4) Linee guida e piano di verifiche																				
Self-Assessment su fornitori	1) Selezione fornitori e somministrazione del questionario																				
	2) Raccolta e analisi delle evidenze																				
	3) Reportistica dei risultati																				
Formazione ai vertici	1) Pianificazione ed esecuzione delle attività di formazione																				

Economics

Sulla base delle informazioni in nostro possesso, abbiamo ipotizzato l'effort per l'esecuzione delle attività progettuali descritte e vi proponiamo la seguente stima di onorari.

Iniziativa	Prezzo
Analisi e revisione piano continuità operativa	20.000,00 €
Esecuzione analisi del rischio cyber	38.000,00 €
Processo di gestione delle terze parti	40.000,00 €
Esecuzione Self-Assessment terze parti	20.000,00 €
Formazione ai vertici aziendali	20.000,00 €
Totale	**138.000,00 €**

Si dichiara che sono parte integrante del presente provvedimento, gli allegati riportati a seguire [1], pubblicati come file separati dal testo del provvedimento sopra riportato:

1. OE_NG6540710_L0_NP3510465.pdf.p7m 

1 L'impronta degli allegati rappresentata nel timbro digitale QRCode in elenco è quella dei file pre-esistenti alla firma digitale con cui è stato adottato il provvedimento