Milano, 19 LUGLIO 2024

 *Spett.le*

***ASA***

***Livorno***

**Oggetto: Offerta economica NIS2 GAP ANALYSIS-ASA**

In riferimento ai colloqui intercorsi, sottoponiamo alla Vostra attenzione la stima d’impegno e la valutazione economica per la fornitura di servizi di cui all’oggetto.

In caso di accettazione, Vi preghiamo di volerci inoltrare copia della presente firmata o, in alternativa, Vi preghiamo di citare nel Vostro ordine Oggetto e Riferimento indicati nell’intestazione del presente documento.

Distinti Saluti

**Avv. Valentina Frediani**

1. **Introduzione**
	1. **Chi siamo**

La SocietàColin & Partners è titolare del network [**www.consulentelegaleinformatico.it**](http://www.consulentelegaleinformatico.it), fondato nel 2002 dall’Avv. Valentina Frediani.

Per consultare la brochure, [clicca qui.](https://www.consulentelegaleinformatico.it/brochure-servizi/)

La Societàsvolge attività di consulenza aziendale altamente qualificata nell’ambito della compliance al diritto delle nuove tecnologie, dove il punto di forza riconosciuto è il connubio delle conoscenze legali con quelle informatiche.

Il supporto è di tipo strategico e trasversale sulle aree aziendali, con la capacità di inserirsi negli equilibri di realtà articolate, garantendo un supporto al management aziendale funzionale ad un vantaggio competitivo aziendale, favorendo ed ottimizzando le esigenze di business in modo pragmatico e con tempistiche legate alle strategie del Committente.

L’azienda è conforme alla norma ISO 9001:2015 

* 1. **Il contesto e le esigenze espresse**

La Direttiva NIS2 ha come obiettivo quello di prevedere misure volte a garantire un livello comune elevato di cybersicurezza nell’Unione, in modo da migliorare il funzionamento del mercato interno, garantendo agli operatori dello stesso mercato di prevenire, mitigare e – se del caso – reagire ad incidenti di natura informatica.

La Normativa NIS2 entra in vigore il 18 ottobre 2024 e stabilisce lo scenario di riferimento per le misure di gestione dei rischi di cybersicurezza e gli obblighi di segnalazione in tutti i settori che rientrano nel suo ambito di applicazione.

Tenuto conto del proprio settore di riferimento, il Committente ha valutato di rientrare nell’Allegato alla normativa indicata tra i destinatari della stessa e di aderire all’offerta di gap analysis lato legale rispetto alla NIS2.

Le attività saranno svolte sulla base del vigente testo normativo.

L’analisi lato tecnologico sarà valutata e svolta autonomamente dal Committente rilasciando i risultati a Colin & Partners eventualmente entro 15 gg. lavorativi decorrenti dall’ordine. Nessuna attività tecnica è a carico di Colin & Partners (a titolo meramente esemplificativo e non esaustivo: VA, PEN TEST, ecc).

1. **I servizi offerti**

**Presupposti organizzativi e struttura del Progetto**

Individuazione di un Referente: ai fini organizzativi del progetto si rende necessario avere un Referente del Committente, che avrà la funzione di veicolare COLIN all’interno dell’azienda, autorizzare i cronoprogrammi, e vagliare la documentazione prodotta.

**Analisi**

Nella tabella di seguito vengono indicate le fasi del Progetto.

|  |  |  |  |
| --- | --- | --- | --- |
| **Fase** | **Modalità** | **Decorrenza**  | **Figure** |
| Startup di progetto *(se richiesta dal Committente)*  | Presentazione di sintesi della normativa NIS 2 e dei risvolti sostanziali rilevanti sull’azienda, al fine di rendere edotti i vertici aziendali delle implicazioni del progetto | L’incontro sarà stabilito secondo le disponibilità del Board | Board Referente  |
| Gap Analysis Legale  | Interviste con i referenti aziendali che verranno individuati in base all’ultima versione dell’organigramma o sulla base delle funzioni  | La programmazione sarà concordata entro 7 gg. decorrenti dall’ordine  | Referente ITUffici da concordare secondo organigramma |
| Redazione della Relazione e presentazione del NIS-2 Compliance Program  | In seguito alle interviste si procederà alla elaborazione delle informazioni raccolte ed alla predisposizione della Relazione - così come indicata nel paragrafo successivo – con correlata presentazione del programma di adeguamento  | Redazione entro 15 gg. lavorativi decorrenti dalla chiusura della raccolta delle informazioni e presentazione entro i successivi 10 gg  | Referente  |

I macro-temi oggetto di analisi sono i seguenti.

|  |  |
| --- | --- |
| ***TEMA***  | ***ATTIVITÀ***  |
| **Governance Cybersecurity**  | Analisi dei seguenti documenti e correlate informazioni: * organigramma interno;
* procure/deleghe di funzioni risultanti dallo statuto o da atti notarili;
* attribuzioni di incarichi operativi interni all’organizzazione.
 |
| **Individuazione del Perimetro tecnologico NIS2**  | La definizione del perimetro è un’attività propedeutica di rilevanza primaria e che deve essere attentamente ponderata, in quanto spetterà poi al Committente dover dimostrare rispetto allo stesso la corretta attuazione delle misure tecniche, organizzative ed operative attuate ai sensi della NIS 2, nonché la gestione dei fornitori critici rispetto a tale perimetro. Al riguardo verrà fissata una riunione dedicata a stabilire quali sono i sistemi informatici rilevanti ai fini dell’erogazione della fornitura critica, e che, se attaccati, potrebbero compromettere le attività di somministrazione.Sono ricompresi nel perimetro: * ambienti di produzione;
* ambienti di test e di sviluppo;
* software e applicazioni;
* devices;
* aree di backup.
 |
| **Procedure cybersecurity e prassi** | Formeranno oggetto di analisi:* le certificazioni attive ritenuti funzionali al progetto
* le procedure
* le policy
* in generale, la documentazione formalmente approvata e in uso presso il Committente sui temi attinenti operations relativamente alle modalità di concreta messa a disposizione della fornitura al Committente/utente finale;
* prassi aziendali, con ciò intendendo la reiterazione costante di comportamenti che si traducono in procedure *de facto* e che di per sé devono essere considerate rispetto alla gestione della cybersecurity presso il Committente (es. riunioni periodiche sui rischi informatici; modalità di disattivazione degli accessi degli amministratori di sistema in caso di scadenza del contratto; modalità di modifica dei profili dei dipendenti in caso di cambi mansioni ecc.).
 |
| **Normative specifiche funzionali all’analisi**  | Alcune normative possono prevedere documenti e/o modalità operative incidenti o concomitanti con l’applicazione della NIS2.Costituiranno in particolare oggetto di acquisizione finalizzata a valutare l’impatto sul modello NIS2, sia documento privacy di natura procedurale che organizzativa nonché alcune procedure di prevenzione dei reati ex 231. Si precisa che la loro analisi non sarà volta a verificare la conformità normativa del documento bensì il contributo che il contenuto dello stesso potrà dare rispetto all’applicazione della NIS2.  |
| **Controlli ed audit**  | Vengono acquisite le informazioni con cui viene monitorato e/o sottoposto ad audit il cyber-rischio esistente  |
| **Supply Chain**  | A seguito della compilazione del file MAPPATURA FORNITORI da parte del Committente, saranno individuate le tipologie di fornitori rientranti nel perimetro NIS2, alle quali applicare successivamente l’adeguamento.Rispetto al tema costituiscono inoltre oggetto di analisi: * il processo di acquisto;
* i criteri di selezione;
* le clausole standard attuali sulla cybersicurezza
* eventuali accordi inter-company
 |

Sulla base dell’organigramma analizzato, le aree sicuramente coinvolte nelle interviste sono:

* IT/OT
* Acquisti e/o rapporti con fornitori

con acquisizione di alcune informazioni funzionali all’analisi da parte dei soggetti competenti rispetto alle aree:

* risorse umane
* DPO
* Qualità ricerca e sviluppo

La prima riunione sarà organizzata da remoto per una presentazione di sintesi a tutte queste figure del progetto, al fine di calendarizzare gli incontri on site e finalizzare la raccolta delle informazioni e dei documenti oggetto di analisi.

L’effort aziendale che coinvolgerà le risorse non supererà comunque le cinque giornate uomo in totale (particolarmente concentrate sulle prime due direzioni indicate).

La Relazione di Gap analysis conterrà una **Tabella di Sintesi Finale** con i seguenti elementi:

|  |  |  |  |
| --- | --- | --- | --- |
| **MISURA** | **STATUS** | **APPLICAZIONE** | **NOTE** |
| *VOCE OGGETTO DI ANALISI*  | * *IMPLEMENTATA*
* *PARZIALMENTE IMPLEMENTATA*
* *NON IMPLEMENTATA*
* *NON APPLICABILE*
 | * *OBBLIGATORIA*
* *RACCOMANDATA*
* *NON OBBLIGATORIA*
 | *OSSERVAZIONI RISPETTO ALLA MISURA*  |

La Relazione si concluderà con il **NIS Compliance Program** contenente gli step di **adeguamento** e le **azioni migliorative**, determinate sulla base della combinazione dei criteri:

* effort
* rischio
1. **GANTT**

**Le attività si svolgeranno in queste tempistiche:**

|  |  |
| --- | --- |
| **ATTIVITÀ** | **INIZIO** |
| RIUNIONE DI PROGRAMMAZIONE | 7 GG LAVORATIVI DECORRENTI DALL’ORDINE  |
| INTERVISTE E RACCOLTA DOCUMENTALE | 20 GG LAVORATIVI DECORRENTI DALL’ORDINE |
| PRESENTAZIONE NIS2 COMPLIANCE PROGRAM | 30 GG. LAVORATIVI DECORRENTI DALL’ORDINE |

1. **Figure Professionali coinvolte nei servizi oggetto della fornitura e tempistiche**

Per lo svolgimento delle attività Colin & Partners S.r.l. ha individuato come Referente Progetto, le figure di riferimento di seguito elencate:

* **Avv. Valentina Frediani** vfrediani@consulentelegaleinformatico.it
1. **Vincoli e prerequisiti**

Sarà compito del Committente predisporre un ambiente adeguato allo svolgimento delle attività sopra descritte.

É responsabilità del Committente identificare una persona di riferimento con il compito di svolgere le seguenti attività:

* Mantenere i contatti con Colin & Partners S.r.l. e concordare il dettaglio delle attività;
* Fornire le informazioni e/o le risorse necessarie allo svolgimento delle attività;
* Coinvolgere il personale interno in funzione delle esigenze che possano presentarsi anche mediante il Referente individuato;
* Coinvolgere eventuali fornitori esterni;
* L’uso della documentazione prodotta ivi incluse le personalizzazioni richieste dalla legge, è limitata alla persona giuridica cui l’offerta si riferisce;
* La documentazione verrà redatta in italiano;
* La comunicazione della documentazione o la sua diffusione su canali di comunicazione esterni all’azienda, è permessa solo laddove sia richiesto dalla Legge, oppure se necessario per adempiere agli obblighi che a essa discendono. Qualsiasi altra comunicazione dovrà essere preventivamente autorizzata per iscritto da COLIN.
1. **Condizioni economiche**

Sulla base di quanto concordato, la presente offerta identifica e valorizza l’impegno di Colin & Partners S.r.l. come segue:

€ 8.500/00 (OTTOMILACINQUECENTO/00)

* 1. **Condizioni di Fornitura**

Le condizioni di fornitura del servizio sono le seguenti:

* Le attività indicate nell’apposita tabella sopra riportata, non usufruite nel corso dell’incarico, si esauriranno al termine dell’incarico stesso, senza che il Committente abbia null’altro avere o a pretendere.
* Tutti i prezzi si intendono IVA esclusa;
* La data di decorrenza è quella indicata nella presente offerta;
* La validità dell’offerta è di 30 giorni solari a partire dalla data di decorrenza.
* Le attività saranno svolte durante l’orario di lavoro 9.00 – 18.00 dei giorni feriali lunedì/giovedì e 9.00 – 13.00 del venerdì;
* La fatturazione avverrà secondo il seguente schema:
* Fattura a 30 gg. data ordine, con pagamento a 60 gg d.f.f.m.

Luogo e Data

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Timbro e Firma Committente per presa visione e accettazione

**Informativa - Articoli 13 e 14 del Regolamento (UE) 2016/679**

**Privacy notice (o informativa essenziale) Clienti**

|  |  |  |
| --- | --- | --- |
| **Chi è il titolare del trattamento?** | Colin & Partners S.r.l. a Socio Unico | Indirizzo: Milano, Via Privata Maria Teresa, 7 Tel.: 057278166email: privacy@consulentelegaleinformatico.it   |
| **Dov’è contattabile il responsabile della protezione dei dati?** | dpo@consulentelegaleinformatico.it Tel.: 057278166 |
| **Chi sono i destinatari?** | responsabili esterni del trattamento ed eventuali ulteriori titolari e/o contitolari | società di revisione e certificazione del bilancio; società di rilevazione e certificazione della qualità; istituti bancari per la gestione di incassi e pagamenti; società e studi legali per la tutela dei diritti contrattuali e/o che si occupano di recupero del credito; società di elaborazione dati e di servizi informatici (es. web hosting, data entry, gestione e manutenzione infrastrutture e servizi informatici, ecc.). La comunicazione può avvenire anche nei confronti dell’amministrazione finanziaria, degli enti pubblici di vigilanza e controllo nei confronti dei quali il Titolare deve adempiere a specifici obblighi. |

|  |
| --- |
| **Cosa sarà fatto dei tuoi dati personali?** |
| **I dati personali saranno trattati:**  | **Il trattamento avviene in base a:** | **I dati personali che ti riguardano sono:** |
| per l’esecuzione e la gestione del rapporto contrattuale instaurato, nonché per la fatturazione, il pagamento, nonché per l’adempimento di obblighi di legge dipendenti dal rapporto contrattuale | * attività preordinate alla conclusione del contratto
* contratto
* adempimento di attività conseguenti al rapporto instaurato e regolamentate per il settore di riferimento del titolare del trattamento
* obblighi di legge, fiscali e contabili
 | * nome, cognome
* codice fiscale o partita iva
* luogo e data di nascita
* indirizzo fisico e telematico
* numero di telefono fisso e/o mobile
* numero conto corrente
* relativi all’ attività commerciale e/o professionale
 |
| per l’invio del questionario di qualità ISO 9001 al fine di verificare il livello del servizio stesso | * Legittimo interesse del Titolare
 | * Nome, cognome
* ruolo
* Indirizzo e-mail
 |
| per l’archiviazione e la conservazione | * contratto, per tutta la sua durata
* adempimento di obblighi conseguenti al rapporto instaurato, quali (tenuta della contabilità ed esercizio dei diritti dipendenti dal contratto)
 | * nome, cognome
* codice fiscale o partita iva
* numero di conto corrente
* relativi all’attività professionale e/o commerciale
 |
| per la comunicazione a destinatari e/o terzi in dipendenza del rapporto contrattuale e degli obblighi che ne derivano | * adempimento di obblighi discendenti dal rapporto instaurato
* legittimo interesse del titolare del trattamento o di terzi e destinatari
 | * nome, cognome
* codice fiscale o partita iva
* indirizzo fisico e telematico
* numero di telefono fisso e/o mobile
* numero conto corrente
* relativi all’ attività commerciale e/o professionale
 |
| per attività di marketing aventi ad oggetto prodotti e servizi del titolare | * Legittimo interesse del Titolare (c.d. *soft spam*)
 | * nome, cognome
* indirizzo telematico
 |
| per l’adempimento degli obblighi di sicurezza informatica | * adempimento di obblighi discendenti dal rapporto instaurato
* legittimo interesse del titolare del trattamento o di terzi e destinatari
 | * accessi logici
* dati relativi ai profili di autorizzazione nel caso assegnati
* dati di traffico (connessione alla rete pubblica e/o aziendale)
 |

|  |
| --- |
| **Quali dati personali che verranno trattati non sono stati ricevuti da te?** |
| * nome, cognome
* indirizzo fisico e telematico
 |

|  |
| --- |
| **Quali sono le fonti presso cui è avvenuta la raccolta dei dati personali che ti riguardano?** |
| La raccolta avviene prevalentemente in seguito ad una tua richiesta diretta. In certi casi Colin & Partners S.r.l. riceve i tuoi dati da altri titolari del trattamento che in occasione della tua partecipazione ad eventi o convegni hanno ottenuto il tuo consenso alla comunicazione.  |

Ti informiamo che puoi esercitare in qualsiasi momento il diritto di reclamo all’Autorità competente e gli altri diritti previsti dagli artt. 15 e ss. del Regolamento Europeo (UE) 2016/679.

Per maggiori informazioni consulta l’informativa completa al seguente link <http://www.consulentelegaleinformatico.it/informativa-clienti/> o contattaci tramite privacy@consulentelegaleinformatico.it