NIS2 e gare pubbliche: quando intervenire e cosa prevedere nei documenti di gara

La NIS2 è la Direttiva (UE) 2022/2555, recepita in Italia con il D.lgs. 138/2024, che rafforza la sicurezza informatica di determinate categorie di soggetti pubblici e privati. La normativa prevede obblighi di gestione dei rischi, la responsabilità degli organi di amministrazione e direttivi nonché la notifica tempestiva degli incidenti significativi.

Per le Stazioni Appaltanti assume un rilievo centrale la sicurezza della catena di approvvigionamento *(Supply Chain Security)*, ossia la gestione dei rischi cibernetici derivanti dai prodotti e dai servizi forniti da terzi. Ed è proprio questo il punto di collegamento con la redazione delle gare: le esigenze di sicurezza della stazione appaltante devono tradursi, per gli affidamenti interessati, in prescrizioni chiare e vincolanti nel disciplinare, nel capitolato e nel contratto.

Il percorso che segue guida la predisposizione della documentazione di gara, partendo dall'inquadramento della stazione appaltante come soggetto NIS2 e dall'oggetto dell'appalto, fino alla definizione di clausole trasparenti e verificabili durante l'esecuzione del contratto.

1. Verificare se la stazione appaltante è soggetta alla disciplina

Essere una stazione appaltante non comporta, di per sé, l'automatico assoggettamento alla NIS2. Prima di avviare la predisposizione dei documenti di gara, il RUP acquisisce dagli uffici competenti l'esito della verifica sull'applicabilità della NIS2 all'Ente (sulla base dei criteri dimensionali e settoriali di cui agli artt. 3, 6 e Allegati I-IV del D.lg. 138/2024) nonché le pertinenti comunicazioni inviate o ricevute tramite la piattaforma digitale dell'Agenzia per la Cybersicurezza Nazionale (ACN).

È opportuno evidenziare che l'assoggettamento alla normativa NIS2 avviene *ex lege*: la sola assenza di registrazione sul sito ACN o di comunicazione non dimostra, di per sé, l'esclusione della stazione appaltante dal perimetro NIS2.

Se la stazione appaltante rientra nel campo di applicazione della NIS2, il RUP ne accerta anche la specifica classificazione quale Soggetto Essenziale o Soggetto Importante, in quanto da tale qualificazione discende una differente gradazione degli obblighi e delle misure di sicurezza di base emanate dall'ACN. Qualora la procedura sia indetta da una Centrale di Committenza, la verifica andrà condotta nei confronti delle Stazioni Appaltanti o degli Enti beneficiari della fornitura.

Se invece la stazione appaltante non è soggetta a NIS2, l'inserimento di prescrizioni sulla sicurezza informatica negli atti di gara può comunque rivelarsi necessario o opportuno in ragione dell'oggetto dell'appalto.

In tali ipotesi, tuttavia, le clausole non dovranno essere impropriamente presentate come obblighi derivanti automaticamente dalla NIS2, al fine di evitare prescrizioni prive di idoneo fondamento giuridico o contenziosi in sede di gara.

2. Individuare l'oggetto dell'appalto

Una volta accertato l'assoggettamento della stazione appaltante alla NIS2, l'attenzione del RUP deve concentrarsi sull'individuazione dell'oggetto dell'appalto, verificando il potenziale impatto sulla sicurezza dei sistemi informativi e di rete.

Nello specifico, si deve verificare se si tratta di beni o servizi la cui compromissione può incidere sulla disponibilità, autenticità, integrità o riservatezza dei dati o dei servizi dei sistemi informativi e di

rete dell'Ente. In fase di analisi, occorre valutare gli accessi concessi al fornitore, i dati e i sistemi coinvolti, gli effetti di una eventuale interruzione, i tempi e costi di ripristino. Questa valutazione riguarda le prestazioni concrete, anche quando l'oggetto principale del contratto non è propriamente informatico.

Gli obblighi di sicurezza della NIS2 devono essere considerati già nella fase di progettazione della gara, tenendo conto dei termini di adeguamento applicabili alla stazione appaltante e rendendoli chiari e conoscibili dagli operatori fin dall'avvio della procedura di gara.

3. Collegare le prescrizioni alle prestazioni

La valutazione del rischio delle prestazioni oggetto dell'appalto deve essere documentata e svolta con il supporto degli uffici competenti per la sicurezza informatica, coinvolti fin dalla fase di progettazione della gara. Il RUP recepisce gli esiti di tale analisi nella documentazione di gara, individuando con precisione le singole prestazioni interessate e i corrispondenti obblighi del fornitore.

A titolo esemplificativo, la tabella seguente illustra come la natura dell'affidamento guidi l'individuazione delle clausole da inserire:

Affidamento	**Aspetti da esaminare per costruire le clausole**
Software gestionale con manutenzione e assistenza remota	Disciplina degli accessi del fornitore, aggiornamenti, procedura di notifica di incidenti e tempi di ripristino del servizio.
Impianto di videosorveglianza collegato alla rete dell'Ente	Gestione delle credenziali, configurazioni, manutenzione e collegamenti alla rete dell'Ente.
Manutenzione di impianti tecnologici con telecontrollo	Regolamentazione connessioni remote, autorizzazione degli interventi e gestione delle interruzioni.
Servizi di pulizia presso locali tecnici/data center	Regole di accesso fisico, tracciabilità degli accessi, protezione delle apparecchiature, calibrate sul rischio effettivo.

Gli esempi evidenziano come non sia ammissibile l'applicazione automatica delle medesime clausole: le prescrizioni vanno calibrate sulle singole prestazioni oggetto della gara. Nei contratti con componenti eterogenee o con oggetto complesso, gli obblighi di sicurezza devono essere espressamente raccordati alle sole attività che li giustificano. Analogamente, anche per i raggruppamenti e i consorzi, le misure tecniche e operative vanno riferite ai componenti che eseguono le prestazioni con impatti sulla sicurezza informatica, ferme restando le regole sulla responsabilità solidale previste dal D.lgs. 36/2023.

4. Scrivere obblighi verificabili nei documenti di gara

Per garantire l'efficacia delle tutele e la tenuta giuridica della gara, le prescrizioni di sicurezza non possono essere rinviate a momenti successivi all'aggiudicazione. Le specifiche dell'ACN richiedono espressamente di inserire nei documenti di gara e nei contratti i requisiti di sicurezza individuati per le forniture interessate (salve motivate e documentate ragioni tecniche o normative). In concreto, la stazione appaltante deve esplicitare con precisione cosa deve fare il fornitore per proteggere sistemi e dati, entro quali tempi e con quali modalità operative verrà verificato l'adempimento.

A tal fine, i documenti di gara devono operare in perfetta sinergia, evitando sovrapposizioni o prescrizioni contrastanti:

- il disciplinare/lettera d'invito deve definire i requisiti di ammissibilità e capacità tecnica (es. possesso della certificazione ISO/IEC 27001 o compilazione preventiva della Checklist di Vendor Due Diligence), disciplinare gli eventuali criteri di valutazione dell'Offerta Tecnica (es. la premialità di 8 punti ex L. 90/2024 per tecnologie UE/NATO corredate dalla Bill of Materials - BOM CycloneDX v1.6) e chiarire quali documenti produrre in gara;
- il capitolato deve descrivere nel dettaglio le prestazioni, i requisiti minimi e tempi di attuazione delle prescrizioni, evidenziando anche gli adempimenti esecutivi;
- lo schema di contratto deve disciplinare comunicazioni, verifiche, il diritto della stazione appaltante ad effettuare audit e ispezioni, il ribaltamento degli obblighi sui subfornitori (flow-down), nonché il regime sanzionatorio, le penali e le clausole di risoluzione espressa.

Definire questi contenuti prima dell'avvio dell'affidamento risponde a un preciso dovere di trasparenza e parità di trattamento: gli operatori economici devono poter conoscere l'esatto perimetro degli impegni richiesti per valutarne i costi e formulare un'offerta congrua e sostenibile. Un rinvio generico al "rispetto della NIS2" o a misure da concordare a gara conclusa non assicura tale trasparenza e compromette la regolarità dell'affidamento.

Il controllo del RUP deve riguardare, quindi, il raccordo tra rischio individuato, prestazione richiesta, termine di adempimento e modalità di verifica. È proprio questo raccordo che rende gli impegni del fornitore comprensibili in gara e controllabili durante l'esecuzione.

5. Un esempio pratico: acquisto di un software gestionale con assistenza da remoto

Consideriamo l'acquisto, da parte di una stazione appaltante soggetta alla NIS2, di un software gestionale installato sui propri sistemi, che preveda servizi di manutenzione e assistenza da remoto. La preventiva valutazione tecnica del rischio ha quindi individuato la necessità di presidiare accessi, tempestività degli aggiornamenti di sicurezza e gestione degli incidenti cibernetici.

Le clausole seguenti illustrano un esempio di clausole da inserire nei documenti di gara.

Nel disciplinare: cosa presentare in offerta e cosa produrre in esecuzione

Il Disciplinare può richiedere una relazione tecnica sulla sicurezza informatica per verificare la conformità dell'offerta, precisando come sarà utilizzata e, ove previsto, il punteggio qualitativo.

Esempio clausola per il nostro acquisto: "*L'offerta tecnica descrive le modalità proposte per gli accessi remoti, gli aggiornamenti di sicurezza e la gestione degli incidenti, evidenziando la rispondenza ai requisiti minimi del capitolato. Gli elementi oggetto di punteggio e le modalità di valutazione sono esclusivamente quelli indicati nella griglia (riferimento). I nominativi del personale incaricato, i recapiti operativi e le evidenze dell'attivazione delle misure sono prodotti dall'aggiudicatario prima dell'avvio delle relative prestazioni, nei termini del capitolato.*"

La relazione non è un documento imposto in via generale dalla NIS2: è una scelta della stazione appaltante, da coordinare con la procedura scelta e con il criterio di aggiudicazione. I requisiti minimi devono essere distinti dagli eventuali miglioramenti premiati; l'effettiva attivazione delle misure esecutive va richiesta come previsto dal capitolato.

Prescrizioni analoghe possono essere appropriate per lo stesso acquisto, effettuato da una stazione appaltante non soggetta alla NIS2, in ragione dei rischi del servizio e alle altre disposizioni applicabili ma non diventano, per questo, obblighi NIS2 generalizzati.

Nel capitolato: prestazioni e misure di sicurezza

Nel Capitolato Speciale d'Appalto le esigenze di sicurezza della stazione appaltante si traducono in regole esecutive chiare, misurabili e vincolanti per l'aggiudicatario. Nel nostro esempio, una formulazione tipo da inserire è la seguente:

"Il servizio comprende manutenzione, aggiornamenti di sicurezza e assistenza da remoto. Gli accessi sono consentiti al solo personale autorizzato, mediante utenze nominative e limitatamente alle attività necessarie al servizio, secondo le modalità di autenticazione, autorizzazione e tracciamento dell'Allegato tecnico. L'affidatario applica gli aggiornamenti entro i termini dell'Allegato, graduati per criticità, coordinando gli interventi che possono interrompere il servizio. Prima dell'attivazione dell'assistenza remota, comunica il personale incaricato e documenta l'attuazione delle misure di accesso. Segnala le variazioni del personale ai fini della tempestiva modifica o revoca delle abilitazioni."

Nello schema di contratto: comunicazioni, controlli e conseguenze degli inadempimenti

Nello Schema di Contratto una formulazione tipo da inserire è la seguente:

"*Prima dell'avvio del servizio, l'affidatario comunica il referente per la sicurezza e i relativi recapiti. Gli incidenti relativi alla prestazione che possano compromettere dati, sistemi o servizi dell'amministrazione sono comunicati a (referente), tramite (canale), senza ingiustificato ritardo e comunque entro (tot ore) dalla conoscenza. L'affidatario trasmette le informazioni disponibili su evento, impatti e interventi avviati, le aggiorna con cadenza (indicare) e collabora alla gestione e al ripristino secondo il capitolato. L'amministrazione verifica il rispetto delle prescrizioni con periodicità (indicare) e in occasione di incidenti o anomalie pertinenti al servizio. L'affidatario fornisce entro (tot giorni) i rapporti sugli aggiornamenti e le evidenze relative agli accessi, nei limiti necessari alla verifica e con modalità che ne tutelino la riservatezza. Le non conformità sono contestate per iscritto. L'affidatario presenta un piano correttivo entro [tot giorni] e attua gli interventi nei termini dell'Allegato, graduati per gravità, ferme le misure urgenti ivi previste. I ritardi imputabili all'affidatario sono assoggettati alle penali dell'articolo (●), previa contestazione e valutazione delle controdeduzioni. Restano ferme le ipotesi di risoluzione dell'articolo (●) e della normativa applicabile."*

Le penali devono essere chiare, proporzionate e definite con presupposti oggettivi, importi o criteri di calcolo precisi e nei limiti della disciplina applicabile. Il termine di comunicazione degli incidenti deve lasciare alla stazione appaltante il tempo necessario per adempiere ai propri obblighi: la segnalazione del fornitore non sostituisce le notifiche alle autorità eventualmente dovute dall'Ente. Se per l'esecuzione è previsto il ricorso a subaffidatari, occorre disciplinare gli obblighi di sicurezza pertinenti alle attività loro affidate e le relative verifiche.

6. Il fornitore deve essere "iscritto NIS2"?

No, fornire una prestazione ad una stazione appaltante soggetta a NIS2 non rende automaticamente l'operatore economico soggetto alla disciplina. Gli obblighi contrattuali di sicurezza possono riguardare anche fornitori che autonomamente non rientrano nell'ambito di applicazione della NIS2. Non va quindi richiesto un requisito generalizzato di "iscrizione NIS2" per il solo assoggettamento della stazione appaltante alla disciplina. Resta distinta la verifica degli obblighi che gravano sul fornitore in ragione delle proprie attività e caratteristiche.