Università degli Studi di Catania

Università degli Studi di Catania
“Supporto specialistico per l’adeguamento alla direttiva NIS2”

Capitolato Speciale d’Appalto

Il progettista
Benedetto Bruno

Il RUP
Agatino Di Bella

AGATINO
DI BELLA
15.12.2025
10:25:36
GMT+00:00

Sommario

1 Aspetti generali

1.1 Contesto di riferimento

La Direttiva 2022/2555/UE NIS2 (Network and Information Security Directive 2) è una normativa dell'Unione Europea che aggiorna e rafforza il quadro legislativo in materia di sicurezza informatica, sostituendo la precedente direttiva NIS. Il suo scopo principale è quello di accrescere il livello di sicurezza delle reti e dei sistemi informativi all'interno dell'UE, rispondendo alle nuove sfide poste dall'evoluzione delle minacce digitali e dalla crescente digitalizzazione di settori chiave. NIS2 amplia significativamente il campo di applicazione rispetto alla versione precedente, includendo un numero maggiore di settori considerati essenziali e critici per il funzionamento della società e dell'economia, come la sanità, i fornitori di servizi cloud, le infrastrutture pubbliche, l'energia, i trasporti, la finanza e l'amministrazione pubblica.

Gli obiettivi principali della direttiva sono: rafforzare la resilienza delle infrastrutture critiche, garantire una gestione efficace dei rischi informatici, migliorare la capacità di prevenzione e risposta agli incidenti, e promuovere una maggiore cooperazione tra gli Stati membri. Per raggiungere questi scopi, NIS2 introduce obblighi più stringenti per le organizzazioni, tra cui l'adozione di misure tecniche e organizzative avanzate, la notifica tempestiva degli incidenti di sicurezza alle autorità competenti, la nomina di figure responsabili della sicurezza informatica e l'implementazione di politiche strutturate di gestione del rischio. Inoltre, la direttiva prevede un regime sanzionatorio severo per chi non si conforma ai requisiti, incentivando così comportamenti responsabili e una maggiore attenzione alla protezione dei dati e dei servizi essenziali.

In Italia, la direttiva NIS2 è stata recepita con il Decreto Legislativo 4 settembre 2024, n. 138, entrato in vigore il 16 ottobre 2024, L'Agenzia per la Cybersicurezza Nazionale (ACN) è stata designata come autorità competente per la supervisione e il coordinamento dell'attuazione della direttiva in Italia.

Per supportare concretamente le organizzazioni nell'adeguamento agli obblighi previsti, l'ACN ha pubblicato la Determinazione n. 164179 del 14 aprile 2025, che definisce le misure di sicurezza di base da adottare, nonché i requisiti per la notifica degli incidenti significativi. La determinazione, in vigore dal 30 aprile 2025, stabilisce un quadro dettagliato di misure e requisiti per i soggetti "importanti" ed "essenziali", differenziando così gli obblighi in base alla criticità del settore e alla dimensione del soggetto. Le misure sono sviluppate in linea con il Framework nazionale per la Cybersecurity e la Data Protection e coprono ambiti quali la gestione del rischio, la governance, la sicurezza della supply chain e la continuità operativa. L'adozione di queste misure dovrà essere completata entro ottobre 2026, con un approccio che bilancia rigore e gradualità per garantire un'efficace protezione delle infrastrutture critiche italiane ed europee.

A settembre 2025, ACN ha pubblicato il documento "Linee Guida NIS – Specifiche di base", una guida alla lettura delle specifiche di base, redatta con l'obiettivo di accompagnare il lettore nella comprensione e interpretazione del testo, evidenziandone e discutendone le caratteristiche peculiari.

Per completare la rappresentazione del contesto normativo e regolamentare è opportuno considerare anche il Regolamento di esecuzione (UE) 2024/2690 della Commissione, adottato il 17 ottobre 2024, che stabilisce le modalità di applicazione della Direttiva NIS2 (UE 2022/2555) per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cybersicurezza e la definizione dei criteri per determinare quando un incidente è considerato "significativo".

In conformità al Regolamento di esecuzione (UE) 2024/2690, il 26 giugno 2025 la European Union Agency for Cybersecurity (ENISA) ha pubblicato la Technical Implementation Guidance, un documento pratico e operativo sviluppato che fornisce indicazioni dettagliate per supportare l'implementazione tecnica della Direttiva NIS2, offrendo esempi, mappature dei requisiti di sicurezza e linee guida operative rivolte a operatori digitali e infrastrutture critiche.

Questi ultimi due documenti, pur essendo dedicati ai "soggetti pertinenti" tra i quali non rientrano le università, rappresentano comunque un valido riferimento per tutte le organizzazioni incluse nel perimetro di applicazione della direttiva NIS2, in quanto forniscono una definizione dettagliata e tecnico-metodologica delle misure di sicurezza e della gestione del rischio e stabiliscono concretamente i criteri per la classificazione degli incidenti significativi e le modalità di notifica.

Nel contesto di riferimento descritto, l'Università degli Studi di Catania rientra nell'ambito di applicazione definito dalla direttiva NIS2 e dal D.Lgs. 138/2024. Inoltre, è stata individuata dall'ACN quale soggetto importante, in relazione alla tipologia di soggetti classificati come "Istituti di istruzione che svolgono attività di ricerca".

1.2 Oggetto dell'appalto

L'Università degli Studi di Catania intende affidare un servizio di supporto specialistico per l'adeguamento alle prescrizioni derivanti dalla direttiva europea NIS2. Le attività oggetto dell'affidamento saranno suddivise nelle seguenti tre macro-fasi:

1. Adempimenti di cui all'art. 23, c. 2, lett. a) del D.Lgs. 138/2024
2. Valutazione
3. Adeguamento

Le attività di dettaglio sono descritte di seguito al par. 3 "Prestazioni richieste"

1.3 Ammontare dell'appalto

L'importo complessivo stimato massimo dell'appalto, da ribassare, è pari a € 135.000,00 oltre IVA al 22%. Non saranno valutate proposte economiche di importo superiore al valore massimo stimato.

Non sono previsti oneri di sicurezza per rischi da interferenze.

Ai sensi dell'art. 108 c. 9 del D.Lgs 36/2023 non è necessario stimare i costi della manodopera e gli oneri aziendali relativi alla salute e sicurezza sul lavoro trattandosi di un appalto per servizi di natura intellettuale.

La stazione appaltante ai sensi dell'art. 58 c. 2 del D.Lgs. 36/2023 non ha suddiviso l'appalto in lotti, ritenuto che l'importo dell'appalto e i requisiti di capacità tecnica e professionale previsti sono tali da

garantire l'effettiva possibilità di partecipazione da parte delle microimprese, piccole e medie imprese.

L'importo contrattuale risultante dall'esito della procedura sarà da intendersi complessivamente remunerativo di tutte le prestazioni comprese nel presente capitolato.

1.4 Modalità di affidamento

La stazione appaltante procederà con l'affidamento diretto dell'appalto ai sensi dell'art. 50, comma 1, lett. b) del D.Lgs. 36/2023, previa consultazione di più operatori economici in possesso di documentate esperienze pregresse, idonee all'esecuzione delle prestazioni contrattuali ed a seguito della valutazione tecnico-economica delle proposte pervenute da parte del Responsabile Unico di Progetto (RUP).

1.5 Pagamento dei corrispettivi

La liquidazione dei corrispettivi pattuiti avverrà al completamento delle attività, a seguito di presentazione di regolare fattura e previa verifica di conformità della prestazione.

1.6 Subappalto

Specificando che non può essere affidata in subappalto l'integrale esecuzione del contratto, fermo restando quanto indicato al comma 1 art. 119 del D.Lgs. n. 36/2023, il subappalto è ammesso nei limiti previsti dal sopra richiamato articolo ed è regolato come ivi indicato. L'operatore economico indica all'atto dell'offerta le parti delle attività che intende subappaltare o concedere in cottimo. In caso di mancata indicazione delle parti da subappaltare il subappalto è vietato. L'operatore affidatario ed il subappaltatore sono responsabili in solido nei confronti della stazione appaltante dell'esecuzione delle prestazioni oggetto del contratto di subappalto.

1.7 Richieste di chiarimenti

É possibile ottenere chiarimenti in merito alla presente procedura mediante la proposizione di quesiti scritti da inoltrare almeno cinque giorni prima della scadenza del termine fissato per la presentazione delle proposte via PEC all'indirizzo protocollo@pec.unict.it.

Le richieste di chiarimenti devono essere formulate esclusivamente in lingua italiana.

Ai sensi dell'art. 88 c. 3 del D.Lgs. 36/2023, le risposte a tutte le richieste presentate in tempo utile verranno fornite mediante PEC almeno sei giorni prima della scadenza del termine fissato per la presentazione delle proposte.

In ogni caso i predetti chiarimenti, se di interesse generale, verranno resi pubblici in forma anonima.

Non sono ammessi chiarimenti per via telefonica.

1.8 Direttore dell'esecuzione del contrato

Il RUP, ai sensi dell'art. 114 e dell'allegato II.14 – artt. 31 e 32 – del D.Lgs. 36/2023, provvederà alla nomina di un direttore dell'esecuzione del contratto (DEC) che eserciterà il coordinamento, la direzione e il controllo tecnico-contabile dell'esecuzione del contratto stipulato dalla stazione appaltante, in modo da assicurarne la regolare esecuzione nei tempi stabiliti e in conformità alle prescrizioni contenute nei documenti contrattuali e nelle condizioni offerte in sede di affidamento.

1.9 Definizione delle controversie

Per tutte le controversie relative alla validità, interpretazione ed esecuzione del contratto è competente il Foro di Catania.

1.10 Requisiti per la partecipazione alla procedura

1.10.1 **Requisiti di ordine generale**

Possesso dei seguenti requisiti:

- insussistenza delle cause di esclusione di cui all'art. 94, 95, 96 e 98 del D.Lgs. n. 36/2023;
- insussistenza delle cause di divieto, decadenza o di sospensione di cui all'art. 67 del D.Lgs. 6 settembre 2011, n. 159;
- insussistenza delle condizioni di cui all'art. 53, comma 16-ter, del D.Lgs. del 2001, n. 165 o di cui all'art. 35 del decreto-legge 24 giugno 2014, n. 90 convertito con modificazioni dalla Legge 11 agosto 2014, n. 114 oppure, ai sensi della normativa vigente, insussistenza di ulteriori divieti a contrattare con la pubblica amministrazione.

1.10.2 **Requisiti di idoneità professionale**

Avere iscrizione nel registro della Camera di Commercio, industria, artigianato e agricoltura della Provincia in cui l'impresa ha sede per attività coerenti con quelle oggetto della presente procedura di gara.

Per gli operatori economici non residenti in Italia, la predetta iscrizione dovrà risultare da apposito documento attestante l'iscrizione stessa in analogo registro professionale o commerciale, secondo la legislazione nazionale di appartenenza.

Gli operatori economici non residenti in Italia dovranno provare la predetta iscrizione secondo le modalità di cui all'art. 100 del D.Lgs n. 36/2023.

1.10.3 **Requisiti di capacità tecniche e professionali**

Ai sensi dell'art. 100, c. 11 del D.Lgs. n. 36/2023, possono partecipare alla procedura le imprese che abbiano eseguito con buon esito negli ultimi dieci anni, almeno n. 3 (tre) contratti per servizi analoghi a quelli oggetto della presente procedura, anche a favore di soggetti privati, per un importo complessivo pari almeno al valore stimato dell'appalto. Per servizio analogo si intende aver svolto attività di supporto specialistico per la conformità dei sistemi di gestione per la sicurezza delle informazioni a normative o standard di riferimento.

La comprova del requisito è fornita mediante uno o più dei seguenti documenti:

- certificati rilasciati dall'amministrazione/ente contraente, con l'indicazione dell'oggetto, dell'importo e del periodo di esecuzione;
- contratti stipulati con le amministrazioni pubbliche, completi di copia delle fatture quietanzate ovvero dei documenti bancari attestanti il pagamento delle stesse;
- attestazioni rilasciate dal committente privato, con l'indicazione dell'oggetto, dell'importo e del periodo di esecuzione;
- contratti stipulati con privati, completi di copia delle fatture quietanzate ovvero dei documenti bancari attestanti il pagamento delle stesse.

1.10.4 **Requisiti di capacità economico-finanziaria**

Ai sensi dell'art. 100, comma 11 del D. Lgs. n. 36/2023, possono partecipare alla procedura le imprese che abbiano maturato nei migliori tre anni degli ultimi cinque un fatturato globale pari almeno al doppio del valore stimato dell'appalto.

La comprova del requisito è fornita mediante uno dei seguenti documenti:

- per le società di capitali mediante bilanci, o estratti di essi, approvati alla data di scadenza del termine per la presentazione delle proposte corredati della nota integrativa;
- per gli operatori economici costituiti in forma d'impresa individuale ovvero di società di persone mediante copia del Modello Unico o la Dichiarazione IVA;
- dichiarazione resa, ai sensi e per gli effetti dell'articolo 47 del decreto del Presidente della Repubblica n. 445/2000, dal soggetto o organo preposto al controllo contabile della società ove presente (sia esso il Collegio sindacale, il revisore contabile o la società di revisione), attestante la misura (importo) del fatturato dichiarato in sede di partecipazione.

Per le imprese che abbiano iniziato l'attività da meno di tra anni, il requisito di fatturato è rapportato al periodo di attività effettivamente svolto.

1.11 Proposta tecnica

Le imprese partecipanti alla procedura sono tenute a presentare una proposta tecnica dettagliata, che consenta alla stazione appaltante di valutare l'adeguatezza della soluzione proposta rispetto alle prestazioni richieste e la conformità alle specifiche minime definite del presente capitolato.

La proposta tecnica dovrà includere almeno i seguenti elementi:

1. Metodologia

   Descrizione dell'approccio metodologico adottato per le fasi di analisi e adeguamento, strumenti e tecniche utilizzati, modalità di svolgimento delle attività, modalità di coinvolgimento del personale dell'Ateneo.

2. Formazione

   Modalità di erogazione, contenuti formativi, destinatari, calendario indicativo, durata.

3. Deliverable previsti

   Elenco dettagliato dei *deliverable* che saranno prodotti nelle fasi di analisi e adeguamento, descrizione delle modalità con cui si intende organizzare la documentazione richiesta.

4. Contestualizzazione e personalizzazione

   Dovrà essere chiaramente indicata la metodologia che sarà adottata per contestualizzare e personalizzare i documenti che saranno prodotti (procedure, politiche, piani, ecc.) rispetto al *modus operandi* ed alle specificità dell'organizzazione.

5. Supporto operativo

   Modalità di affiancamento all'organizzazione nella definizione del perimetro di intervento, nella raccolta dati, durante la fase di adeguamento ecc.

6. Piano di lavoro e tempistiche

   Cronoprogramma dettagliato delle attività, durata prevista per ciascuna fase, *milestone* e criteri di verifica.

7. Team di progetto

   Composizione del *team* di progetto dedicato, esperienze pregresse e qualifiche professionali, ruoli e responsabilità.

8. Referenze dell'impresa

   Documentate referenze dell'impresa per attività analoghe a quelle previste dal presente capitolato.

1.12 Obblighi ed oneri a carico dell'operatore economico affidatario

1.12.1 **Garanzia definitiva**

Ai sensi dell'art. 53 del D.Lgs. 36/2023, comma 4, l'operatore economico per la sottoscrizione del contratto deve costituire una garanzia, a sua scelta sotto forma di cauzione o fideiussione, con le modalità di cui all'articolo 106 del D.Lgs 36/2023, pari al 5 per cento dell'importo del contratto, da prestarsi secondo quanto previsto dalla normativa vigente.

1.12.2 **Penali**

La penale pecuniaria per ogni giorno solare consecutivo di ritardo sul termine di ultimazione delle prestazioni stabilito dal presente capitolato è fissata nella misura giornaliera compresa tra lo 0,3 per mille e l'1 per mille dell'ammontare netto contrattuale, da determinare in relazione all'entità delle

conseguenze legate al ritardo, e complessivamente non superiori al 10 per cento di detto ammontare netto contrattuale, ai sensi dell'art. 126 del D.Lgs. 36/2023 salvo il risarcimento del maggior danno. In ogni caso, decorsi 30 (trenta) giorni solari consecutivi oltre il termine fissato la stazione appaltante si riserva la facoltà di risolvere il contratto di diritto per inadempimento dell'impresa senza bisogno di pronuncia giudiziale.

L'intenzione di avvalersi della clausola risolutiva viene effettuata mediante PEC. In tal caso la stazione appaltante potrà incamerare la cauzione definitiva e ciò senza pregiudizio per eventuali azioni di risarcimento di danni maggiori.

A giustificazione del ritardo nell'ultimazione dell'opera, l'operatore economico affidatario non potrà mai attribuirne la causa in tutto od in parte alla stazione appaltante o ad altre ditte ed imprese da questa incaricate per altri lavori, forniture o servizi, se lo stesso operatore non avrà tempestivamente denunciato per iscritto alla stazione appaltante il ritardo ascrivibile ad altri, affinché la stazione appaltante possa farne regolare contestazione.

Alla riscossione della penale si procederà mediante riduzione dell'importo netto dei pagamenti da liquidare.

2 Modalità di esecuzione

2.1 Termini per il completamento dell'appalto

Le prestazioni oggetto del presente appalto devono essere completate entro 12 (dodici) mesi consecutivi a far data dalla stipula del contratto ovvero nel tempo minore proposto dall'operatore economico affidatario.

Limitatamente alle prestazioni relative agli adempimenti degli obblighi di cui all'art. 25 del D.Lgs. 138/2024, il termine di completamento è fissato in 60 (sessanta) giorni consecutivi a far data dalla stipula del contratto.

2.2 Ultimazione della attività

Le attività si considereranno ultimate a seguito di verifica di conformità con esito positivo.

2.3 Verifiche di conformità

Ai sensi dell'art. 116 del D.Lgs. 36/2023, l'appalto è soggetto a verifica di conformità per certificare il rispetto delle caratteristiche tecniche, economiche e qualitative delle prestazioni, nonché degli obiettivi e dei tempi, in conformità delle previsioni e pattuizioni contrattuali.

3 Prestazioni richieste

L'Università degli Studi di Catania intende affidare un servizio di supporto specialistico per l'adeguamento alle prescrizioni derivanti dalla direttiva europea NIS2. Le attività oggetto dell'affidamento saranno suddivise nelle seguenti tre macro-fasi:

1. Adempimenti di cui all'art. 23, c. 2, lett. a) del D.Lgs. 138/2024
2. Analisi
3. Adeguamento

Le prestazioni richieste nell'ambito del presente appalto non includono la fornitura di soluzioni tecnologiche né attività operative sui sistemi informatici dell'organizzazione.

3.1 Adempimenti di cui all'art. 23, c. 2, lett. a) del D.Lgs. 138/2024

Dovranno essere previste attività finalizzate all'adempimento della previsione di cui all'art. 23, c. 2, lett. a) del D.Lgs. 138/2024 in tema di formazione in materia di sicurezza informatica, per gli organi di amministrazione e gli organi direttivi dell'Ateneo.

Dovranno essere proposti percorsi formativi dedicati e personalizzati per i vertici dell'organizzazione, focalizzati sulle responsabilità strategiche e di governance in ambito cybersecurity, la gestione del rischio informatico, la normativa NIS2, le strategie di prevenzione e risposta agli incidenti, le implicazioni legali e operative della sicurezza digitale.

L'attività formativa dovrà prevedere almeno due azioni distinte: la prima dedicata agli argomenti sopra elencati e la seconda, successiva alla macro-fase di analisi, per la presentazione dei risultati e del piano di adeguamento.

La formazione potrà essere erogata tramite moduli in presenza, sessioni online sincrone o asincrone, o una combinazione di tali modalità, per garantire flessibilità e massima partecipazione e potrà essere integrata con workshop pratici, materiale informativo, ecc.

3.2 Analisi

Dovrà essere condotto un *assessment* strutturato del sistema informativo dell'organizzazione al fine di:

- individuare il perimetro tecnico e organizzativo di applicazione della Direttiva NIS2;
- verificare la conformità ai requisiti previsti dalla Direttiva NIS2 e dal D.Lgs. 138/2024 nell'ambito del perimetro individuato;
- valutare l'adozione delle misure di base di sicurezza indicate dalla Determinazione n. 164179 ACN per i soggetti importanti, nell'ambito del perimetro individuato;
- individuare i *gap* di conformità e definire un piano di adeguamento.

Dovranno essere prodotti almeno i seguenti *deliverable*:

- *Gap analisys*: rappresenta il risultato di un'attività di valutazione sistematica volta a identificare le discrepanze tra lo stato attuale dell'organizzazione e i requisiti tecnici e organizzativi previsti dalla normativa. Fornisce una visione chiara dei punti di non conformità e delle aree prioritarie di intervento.
  - Contenuti principali:
    - Mappatura dei requisiti: elenco strutturato dei requisiti organizzativi, procedurali e tecnici applicabili.
    - Valutazione dello stato attuale: descrizione delle misure esistenti, processi e controlli implementati.
    - Identificazione dei *gap*: evidenza delle non conformità, delle carenze tecniche e organizzative, e delle aree di rischio.
    - Classificazione e prioritizzazione dei *gap*: categorizzazione per ambito (es. governance, accessi, rete, incidenti) e per livello di criticità (alto, medio, basso).
    - Analisi del rischio associato.
  - Obiettivo: fornire una base oggettiva e strutturata per definire le priorità di intervento e pianificare le azioni correttive.
- Piano di *remediation*: documento operativo che definisce le azioni correttive e migliorative necessarie per colmare i *gap* identificati nella fase di analisi e per orientare l'organizzazione nel percorso di adeguamento normativo e rafforzamento della postura di sicurezza.
  - Contenuti principali:
    - Elenco delle azioni correttive: per ciascun *gap*, viene proposta una o più misure di *remediation* (tecniche, organizzative o procedurali).
    - Priorità e tempistiche: classificazione delle azioni in base all'urgenza e alla complessità, con indicazione delle scadenze previste.
    - Responsabilità: assegnazione dei task ai soggetti interni o esterni coinvolti (es. IT, compliance, fornitori).
    - Risorse necessarie: stima *budgettaria* dei costi di adeguamento, di strumenti, competenze e supporti richiesti per l'implementazione.
    - Metriche di verifica: criteri per valutare l'efficacia delle azioni intraprese e il raggiungimento della conformità.
  - Obiettivo: trasformare l'analisi dei *gap* in un piano d'azione concreto, misurabile e sostenibile, allineato con le priorità strategiche dell'organizzazione. Le misure di *remediation* dovranno essere verticalizzate nello specifico contesto tecnico-organizzativo dell'Ateneo, così come individuato nel perimetro di riferimento.

Si precisa che la *gap analisys* e il piano di *remediation* dovranno estendersi all'intera organizzazione dell'Ateneo, con particolare riguardo alle strutture che godono di autonomia gestionale, quali i dipartimenti, pur mantenendo un approccio olistico, integrato e centralizzato al governo della sicurezza informatica, alla definizione delle misure tecniche e organizzative ed al processo di adeguamento alla direttiva NIS2.

Per una migliore comprensione dell'organizzazione dell'Ateneo e delle strutture didattiche, di ricerca e di servizio che la compongono, utile ai fini di una corretta e consapevole determinazione dell'*effort* necessario allo svolgimento delle prestazioni richieste, si rimanda ai seguenti riferimenti:

https://www.unict.it/it/ateneo/strutture

https://www.unict.it/it/ateneo/amministrazione

https://www.unict.it/it/ateneo/statuto-di-ateneo

https://www.unict.it/it/ateneo/organi-dellateneo

3.3 Adeguamento

Nella fase di "Adeguamento" l'impresa affidataria dovrà supportare e affiancare l'Organizzazione nell'implementazione delle misure di sicurezza di base per i soggetti importanti di cui alla determinazione ACN n. 164179 con particolare riferimento ai requisiti organizzativi[1], alla luce delle risultanze emerse nella precedente fase di analisi.

Nell'implementazione dei requisiti organizzativi necessari per colmare i *gap* individuati nella fase di analisi, si terrà conto oltre che delle prescrizioni contenute nella normativa NIS2 e nelle determinazioni dell'ACN, anche delle indicazioni operative contenute nel Regolamento di esecuzione (UE) 2024/2690 e nella Technical Implementation Guidance di ENISA, nonché delle "Linee Guida NIS – Specifiche di base – Guida alla lettura" pubblicate da ACN a settembre 2025.

Con particolare riferimento alle misure di sicurezza di base per i soggetti importanti individuate da ACN con la Determinazione n. 164179 del 14 aprile 2025, al termine della fase di "Adeguamento", dovranno essere prodotti almeno i seguenti *deliverable* (tra parentesi è indicato il codice identificativo del requisito di riferimento definito da ACN):

- Elenco dei sistemi informativi e di rete rilevanti (GV.OC-04.1).
- Inventario degli apparati fisici (hardware) che compongono i sistemi informativi e di rete, ivi inclusi i dispositivi IT, IoT, OT e mobili (ID.AM-01.1).
- Inventario dei servizi, dei sistemi e delle applicazioni software che compongono i sistemi informativi e di rete, ivi incluse le applicazioni commerciali, open-source e custom, anche accessibili tramite API (ID.AM-02.1).
- Inventario dei servizi informatici erogati dai fornitori, ivi inclusi i servizi cloud. (ID.AM-04.1).
- Registro recante l'elenco dei dipendenti che hanno ricevuto la formazione (PR.AT-01.3).
- Documentazione dell'organizzazione per la sicurezza informatica (GV.RR-02.1).
- Elenco degli amministratori dei sistemi informativi e di rete rilevanti (GV.RR-04.1).
- Documentazione delle attività consentite da remoto per i sistemi informativi e di rete rilevanti (PR.IR-01.1).
- Elenco dei sistemi informativi e di rete ai quali è possibile accedere da remoto con la descrizione delle relative modalità di accesso (PR.IR-01.2).
- Documentazione dei livelli di servizio attesi (SL) dei servizi e delle attività anche ai fini di rilevare tempestivamente gli incidenti significativi (DE.CM-01.2)

[1] Si veda il par. 2.4 delle "Linee Guida NIS" di ACN

- Procedure per l'autenticazione delle utenze (PR.AA-03.3).
- Procedure per l'assegnazione dei permessi alle utenze (PR.AA-05.3).
- Procedure per la protezione dell'accesso fisico ai sistemi informativi e di rete rilevanti (PR.AA-06.2).
- Piano di gestione dei rischi per la sicurezza informatica (GV.RM-03.1).
- Piano di trattamento del rischio (ID.RA-06.1).
- Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete (ID.RA-05.1)
- Piano di continuità operativa (ID.IM-04.1).
- Piano di ripristino in caso di disastro (ID.IM-04.2).
- Piano per la gestione delle crisi per i sistemi informativi e di rete rilevanti (ID.IM-04.3).
- Piano di gestione delle vulnerabilità (ID.RA-08.3).
- Piano di formazione in sicurezza informatica (PR.AT-01.1).
- Piano di adeguamento che identifichi gli interventi necessari ad assicurare l'attuazione delle politiche di sicurezza, di cui alla misura (ID.IM-01.1).
- Procedure per la gestione degli incidenti di sicurezza informatica e la notifica al CSIRT Italia (RS.MA-01.1).
- Procedure per la comunicazione ai destinatari dei servizi di incidenti o minacce significativi (RS.CO-02.1 e RS.CO-02.2).
- Procedure per il ripristino del normale funzionamento dei sistemi informativi e di rete coinvolti da incidenti di sicurezza informatica (RC.RP-01.1)
- Procedure per il monitoraggio dei canali di comunicazione del CSIRT Italia (ID.RA-08.1)
- Documentazione delle pratiche di sviluppo sicuro del codice nello sviluppo del software (PR.PS-06.1)
- Tutte le politiche di sicurezza informatica non esplicitamente indicate ma comunque previste dal requisito GV.PO-01.1
- Tutte le procedure previste per misure tecnologiche, là dove nella determinazione di ACN è indicato "Sono adottate e documentate procedure".

Per i *deliverable* che prevedono la predisposizione di elenchi, inventari o registri, la produzione dei dati è a carico della stazione appaltante. L'impresa affidataria dovrà produrre modelli, indicare metodologie e fornire supporto per la raccolta dei dati e la definizione del perimetro di intervento, in conformità con la normativa.