ATTO DI INDIRIZZO DEL DIRETTORE GENERALE

Attuazione del D.Lgs. 4 settembre 2024, n. 138 (NIS2)

OGGETTO. Attuazione del D.Lgs. 138/2024: ricognizione documentale, allineamento dei ruoli, verifica degli adempimenti ACN 2026, completamento delle misure di sicurezza di base e costituzione del fascicolo di conformità NIS della Stazione Zoologica Anton Dohrn.

Premesse e quadro istruttorio

VISTA la Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (NIS2);

VISTO il D.Lgs. 4 settembre 2024, n. 138 e, in particolare, gli articoli 7, 23, 24, 25, 30, 31, 35, 38 e 42;

VISTA la Legge 28 giugno 2024, n. 90 e, in particolare, l'articolo 8, relativo alla struttura e al referente per la cybersicurezza nelle pubbliche amministrazioni rientranti nel relativo ambito di applicazione;

VISTI lo Statuto e il vigente Regolamento di Organizzazione e Funzionamento della Stazione Zoologica Anton Dohrn;

VISTO il Decreto del Presidente, Repertorio n. 92/2024, registrato l'8 agosto 2024, con il quale il dott. Francesco Paolo Patti è stato nominato Referente per la Cybersicurezza SZN, con riporto diretto al Direttore Generale per la condivisione delle azioni necessarie all'adempimento degli obblighi di legge;

RICHIAMATA la comunicazione SZN del 15 ottobre 2024 all'Agenzia per la Cybersicurezza Nazionale, con la quale sono stati trasmessi l'atto di nomina del Referente per la Cybersicurezza e la relativa documentazione;

VISTO il Decreto del Presidente, Repertorio n. 117/2024, registrato il 29 ottobre 2024, recante la nomina del Responsabile per la sicurezza delle informazioni (CISO) della SZN e la definizione dei relativi compiti;

VISTA la Dichiarazione NIS DNISA00000077 del 17 febbraio 2025, relativa alla prima registrazione della SZN;

VISTA la comunicazione ACN registrata al Registro Unico n. 136514 del 12 aprile 2025, con la quale - in relazione alla Determinazione del Direttore Generale ACN n. 136430 del 12 aprile 2025 - la SZN è stata inserita nell'elenco dei soggetti NIS quale soggetto importante, con codice identificativo IT7A47VA, per la tipologia "Enti e Istituzioni di ricerca";

RICHIAMATA la nota "Attività CISO SZN", prot. n. 0006699 del 28 luglio 2025, che ricostruisce gli adempimenti svolti, le attività del presidio cyber e alcune criticità tecniche allora rilevate, le quali devono essere oggi riesaminate per verificarne l'eventuale superamento;

VISTA la nota prot. n. 0007264 del 1° settembre 2025, con la quale il dott. Francesco Paolo Patti ha formalizzato la rinuncia agli incarichi di CISO e di Referente per la Cybersicurezza;

VISTA la comunicazione ACN relativa alla Dichiarazione DNISA00041955 e alla Determinazione del Direttore Generale ACN n. 127159 del 10 aprile 2026, con la quale la SZN è stata confermata nell'elenco dei soggetti NIS 2026 quale soggetto importante, mantenendo il codice identificativo IT7A47VA;

RICHIAMATI il Verbale del Tavolo Settoriale Ricerca MUR del 14 aprile 2026 e i materiali ACN e CRUI-CODAU ivi condivisi, con particolare riguardo alla categorizzazione delle attività e dei servizi, ai fornitori rilevanti e alle misure di sicurezza di base;

VISTO il Vademecum NIS ACN, versione 1.0 di settembre 2026, nonché il promemoria ACN trasmesso ai soggetti inseriti nel 2025, che richiamano gli adempimenti annuali, l'obbligo di notifica degli incidenti significativi già operativo

per i soggetti 2025 e il completamento delle misure di sicurezza di base entro il termine di diciotto mesi dalla ricezione della PEC di inserimento;

RICHIAMATO il riscontro dell'Agenzia per la Cybersicurezza Nazionale del 21 settembre 2026, reso su quesito della Stazione Zoologica, con il quale l'Agenzia ha invitato l'Ente a completare e trasmettere l'Aggiornamento delle Informazioni e il Modello di Categorizzazione delle Attività e dei Servizi;

RICHIAMATE la nota del Presidente del 25 agosto 2026 e la risposta del Direttore Generale del 4 settembre 2026 in ordine al riassetto del presidio CISO/RTD/cybersicurezza, conclusasi con il conferimento di cui al visto successivo;

VISTO il Decreto del Presidente, Repertorio n. 171/2026, del 21 settembre 2026, con il quale al dott. Francesco Paolo Patti sono stati conferiti gli incarichi di Responsabile per la Transizione Digitale e di CISO/Referente per la Cybersicurezza, unitamente al mandato tecnico-scientifico istruttorio in materia di Intelligenza Artificiale;

Elementi istruttori accertati e punti da chiudere

- **La SZN è soggetto NIS "importante":** La qualificazione risulta da atti ACN 2025 e 2026 ed è già utilizzabile nel fascicolo e in ogni atto interno.
- **Il termine sulle misure di base è imminente:** Per i soggetti inseriti nel 2025 il termine puntuale è pari a diciotto mesi dalla ricezione della PEC di inserimento. È disponibile la data di protocollazione ACN del 12 aprile 2025, ma non risulta ancora agli atti esaminati la ricevuta di avvenuta consegna della PEC, necessaria per fissare il giorno esatto.
- **La notifica degli incidenti è già un obbligo corrente:** Per i soggetti inseriti nel 2025 l'obbligo è operativo dal 2026; occorre quindi verificare senza ritardo l'effettiva operatività di Referente CSIRT, sostituti, utenze, escalation e procedura interna.
- **Il presidio CISO/Referente cyber va riallineato anche verso ACN:** Gli atti 2024 sono disponibili, così come la rinuncia del 1° settembre 2025. La rinuncia non risulta seguita da un atto di presa d'atto né da una dichiarazione di vacanza verso ACN. Le funzioni sono state esercitate in continuità su richiesta della Direzione Generale, come documentato dalla corrispondenza del 24 e 26 febbraio 2026 relativa alla trasmissione della Dichiarazione DNISA00041955. I ruoli NIS registrati sul Portale non hanno pertanto subito variazioni soggette a notifica ai sensi dell'art. 7, comma 7, del D.Lgs. 138/2024. Il Portale non è stato tuttavia oggetto di monitoraggio continuativo nel periodo intermedio. Il conferimento del settembre 2026 ricompone il presidio. Occorre ora verificare puntualmente i dati presenti sul Portale e comunicare ad ACN il Referente per la Cybersicurezza e ad AgID/IPA il RTD. Vanno inoltre aggiornati i ruoli NIS eventualmente interessati. Infine, il fascicolo deve documentare con evidenze come sono state coperte le funzioni nel periodo intermedio.
- **I ruoli NIS non vanno confusi con il CISO:** Punto di contatto NIS, sostituto, Referente CSIRT e sostituti sono ruoli da verificare sul Portale ACN. La loro eventuale coincidenza con CISO, RTD o Referente per la Cybersicurezza deve discendere da atti formali e da un assetto organizzativo coerente.
- **Le evidenze 2026 devono essere ricostruite:** La comunicazione ACN di permanenza 2026 è disponibile, ma non sono emerse, tra i documenti esaminati, copie complete della Dichiarazione DNISA00041955, della trasmissione/aggiornamento informazioni 2026, dell'elenco dei fornitori rilevanti 2026 e della categorizzazione 2026.
- **Due adempimenti annuali risultano scaduti:** l'Aggiornamento delle Informazioni, con termine al 31 maggio 2026, per il quale la sezione Fornitori non risulta compilata, i dati su domini e indirizzi IP sono fermi al 10 luglio 2025 e quelli su utenti e ruoli al 14 luglio 2025; la Categorizzazione delle Attività e dei Servizi, con termine al 30 giugno 2026. Con riscontro del 21 settembre 2026 l'Agenzia ha invitato l'Ente a completare e trasmettere entrambi, confermando che si procede in autonomia.

- **Gli elementi tecnici pregressi non equivalgono a prova di conformità attuale:** La nota CISO del luglio 2025 e la proposta AON 2024 sono utili come base di lavoro, ma lo stato corrente di logging, SIEM, inventari, IP pubblici, rete, vulnerabilità e altre misure deve essere nuovamente attestato con evidenze aggiornate.

Ferme restando le competenze del Presidente, del Consiglio di Amministrazione, degli organi di amministrazione e direttivi di cui all'art. 23 del D.Lgs. 138/2024, nonché le attribuzioni previste dallo Statuto e dal ROF,

IL DIRETTORE GENERALE DISPONE QUANTO SEGUE

1. Avvio del fascicolo unico NIS SZN – È istituito presso la Direzione Generale un fascicolo unico di conformità NIS, articolato almeno in: atti ACN e ricevute; ruoli e nomine; adempimenti annuali; categorizzazione di attività e servizi; sistemi informativi e di rete rilevanti; fornitori rilevanti; misure di sicurezza; incidenti e notifiche; formazione; audit, test e piani di rimedio. Ogni adempimento è considerato chiuso solo in presenza di evidenza documentale verificabile.

2. Ricostruzione della decorrenza e delle scadenze – Il Protocollo, con il supporto del Punto di contatto NIS da verificare, acquisisce la PEC ACN di inserimento 2025 completa della ricevuta di avvenuta consegna e attesta la data esatta da cui decorre il termine di diciotto mesi per le misure di sicurezza di base. Fino a tale acquisizione, la programmazione interna assume come termine prudenziale il 12 ottobre 2026, corrispondente a diciotto mesi dalla data di protocollazione ACN del 12 aprile 2025 (data più anticipata possibile di ricezione della PEC), e non può essere differita in attesa della verifica formale.

3. Verifica integrale della posizione sul Portale ACN – È effettuata un'estrazione aggiornata della posizione SZN sul Portale dei Servizi ACN, comprendente almeno: dati dell'organizzazione; qualificazione e codice IT7A47VA; Punto di contatto e sostituto; Referente CSIRT e sostituti; componenti degli organi di amministrazione e direttivi; utenze abilitate; servizi e informazioni dichiarate; IP pubblici statici e domini; accordi di condivisione delle informazioni; fornitori rilevanti. Ogni disallineamento deve essere corretto nei termini normativamente previsti.

4. Separazione e riallineamento dei ruoli cyber/NIS – È predisposta una matrice aggiornata delle funzioni, distinguendo espressamente: a) Referente per la Cybersicurezza ai sensi della L. 90/2024; b) CISO quale presidio organizzativo interno della sicurezza delle informazioni; c) Punto di contatto NIS e relativo sostituto; d) Referente CSIRT e sostituti; e) RTD; f) Responsabile SIST; g) RPD/DPO. La matrice deve indicare atto di conferimento, decorrenza, durata, responsabilità, sostituzioni e canali di escalation.

5. Presidio CISO e Referente per la Cybersicurezza – Il dott. Francesco Paolo Patti, CISO/Referente per la Cybersicurezza e RTD giusta Decreto del Presidente Rep. n. 171/2026, assume senza soluzione di continuità il coordinamento tecnico-organizzativo delle attività disposte dal presente atto, in raccordo con la Direzione Generale, fermo il ruolo operativo del SIST nell'esecuzione tecnica e nella produzione delle evidenze e l'autonomia funzionale del RPD/DPO. Il CISO cura altresì, entro cinque giorni lavorativi, la verifica dei dati registrati sul Portale ACN, le comunicazioni conseguenti al conferimento verso ACN e AgID/IPA e l'eventuale aggiornamento dei ruoli NIS.

6. Verifica degli adempimenti annuali 2026 – Devono essere acquisite e validate le evidenze relative: a) alla registrazione/aggiornamento annuale 2026 e alla Dichiarazione DNISA00041955; b) all'aggiornamento delle informazioni nel periodo 15 aprile-31 maggio 2026 e ad ogni variazione successiva; c) all'elenco dei fornitori rilevanti; d) alla categorizzazione delle attività e dei servizi nel periodo 1° maggio-30 giugno 2026. In assenza di evidenza, l'adempimento è classificato "da verificare/integrare", non "completato". Gli adempimenti di cui alle lettere b) e d) risultano scaduti: la loro trasmissione costituisce priorità assoluta ed è effettuata entro il 30 settembre 2026 per l'aggiornamento delle informazioni ed entro il 7 ottobre 2026 per la categorizzazione delle attività e dei servizi.

7. Perimetro di attività, servizi e sistemi rilevanti – Il SIST, con i Direttori di Dipartimento, i responsabili delle infrastrutture e delle sedi e gli owner dei servizi, consolida la mappa delle attività e dei servizi NIS e dei sistemi informativi e di rete rilevanti, includendo le specificità della ricerca: sistemi scientifici, strumentazione connessa, ambienti di calcolo e dati, sistemi gestiti da partner o fornitori, software sviluppato internamente o nell'ambito di progetti, componenti/librerie di terze parti e postazioni individuali che assumano un ruolo rilevante nel servizio.

8. Fornitori rilevanti e catena di approvvigionamento – L'Ufficio competente in materia di appalti e contratti, con RUP/DEC e SIST, ricostruisce e valida l'elenco dei fornitori rilevanti NIS, distinguendo almeno forniture ICT e forniture non fungibili. Per ciascun fornitore devono essere tracciati servizio/prodotto, contratto, dipendenze, accessi a dati/sistemi, criticità, subforniture rilevanti, SLA, obblighi di notifica, clausole cyber, exit strategy e azioni di adeguamento contrattuale.

9. Gap assessment delle misure di sicurezza di base – È completata una matrice unica requisito-evidenza-stato-gap-rischio-azione-owner-termine-costo-prova di chiusura, facendo riferimento alle specifiche di base ACN e utilizzando i materiali MUR/CRUI-CODAU come supporto metodologico. La verifica deve coprire almeno gestione del rischio, ruoli, affidabilità delle risorse umane, audit, supply chain, asset, vulnerabilità, continuità/DR, identità e accessi, sicurezza fisica, formazione, dati/backup, ciclo di vita dei sistemi, reti, monitoraggio e incident response.

10. Incident response e notifica a CSIRT Italia – È verificata con priorità immediata l'operatività della catena di rilevazione, triage, escalation, decisione e notifica. Devono essere disponibili nominativi e sostituti, recapiti e utenze, criteri di significatività, flussi con DG e DPO, registro degli incidenti, modalità di conservazione delle evidenze e un test table-top documentato. Eventuali carenze che possano impedire una notifica tempestiva sono trattate come priorità critica.

11. Piano di rimedio e misure compensative – Per ogni gap non chiudibile entro il termine applicabile è predisposta una misura compensativa motivata, un rischio residuo esplicito e un piano di chiusura con responsabile, costo e data. Gli interventi tecnici, gli acquisti e gli affidamenti necessari sono attivati con separati atti amministrativi, nel rispetto delle competenze e delle disponibilità di bilancio.

12. Formazione e responsabilità degli organi – L'Ufficio Risorse Umane, con il supporto delle funzioni cyber e del SIST, ricostruisce la formazione cyber già svolta e documenta quella programmata nel PIAO 2026. È verificata, inoltre, la formazione richiesta agli organi di amministrazione e direttivi e sono programmati eventuali moduli integrativi per ruoli NIS/cyber, amministratori di sistema, procurement, responsabili di progetto e personale che opera su sistemi rilevanti.

13. Relazione conclusiva alla Direzione Generale – A chiusura della fase urgente è trasmessa al Direttore Generale una relazione firmata dai responsabili delle aree interessate, contenente: stato degli adempimenti ACN; matrice dei ruoli; perimetro di attività/servizi/sistemi; fornitori rilevanti; esito del gap assessment; elenco delle criticità residue; azioni avviate; fabbisogni economici; rischi accettati o da sottoporre alla governance; indice delle evidenze conservate nel fascicolo unico.

Responsabilità operative e tempistica

Le attività sono svolte in forma coordinata, senza duplicare competenze già attribuite da Statuto, ROF, atti di nomina o normativa di settore. Il seguente quadro ha natura di responsabilizzazione istruttoria e operativa.

Soggetto/struttura	Compito prioritario	Output	Termine
Direzione Generale	Coordinamento istruttorio; decisioni organizzative; escalation; raccordo con Presidente e organi competenti.	Cruscotto di avanzamento e decisioni	settimanale fino a chiusura
Protocollo / Affari Generali	Acquisizione PEC 2025 con ricevuta; raccolta atti e ricevute; indicizzazione del fascicolo.	Attestazione data PEC + indice atti	entro il 25 settembre 2026
Punto di contatto NIS (da verificare)	Estrazione posizione Portale ACN; verifica aggiornamenti e comunicazioni; supporto alle correzioni.	Export/print ufficiale Portale + ricevute	entro il 28 settembre 2026
SIST	Evidenze tecniche; perimetro sistemi; asset, reti, logging, backup, IAM, vulnerabilità, DR; attuazione tecnica.	Dossier tecnico + evidenze	entro il 2 ottobre 2026
CISO / Referente cyber	Coordinamento tecnico-organizzativo cyber; risk/gap assessment; incident response; reporting.	Matrice misure e piano di rimedio	entro il 7 ottobre 2026
Referente CSIRT e sostituti	Operatività delle notifiche e test del flusso incidenti.	Verbale test / evidenza canali	entro il 30 settembre 2026
Appalti/Contratti + RUP/DEC	Fornitori rilevanti, contratti, clausole e dipendenze.	Registro fornitori rilevanti	entro il 2 ottobre 2026
RU / Formazione	Organi e personale; formazione e affidabilità risorse umane.	Registro e piano formativo	entro il 2 ottobre 2026
Direttori Dipartimento / Sedi / owner servizi	Censimento attività, sistemi e progetti rilevanti, dipendenze e responsabili.	Schede validate di perimetro	entro il 2 ottobre 2026
RPD/DPO	Raccordo privacy/data breach e verifica dei profili di protezione dati, in autonomia funzionale.	Contributo/annotazioni di competenza	entro il 2 ottobre 2026
CISO / Referente per la Cybersicurezza	Trasmissione sul Portale ACN dell'Aggiornamento delle Informazioni 2026 (scaduto il 31/05/2026), previa acquisizione dei dati da SIST e Appalti	Ricevuta di trasmissione	entro il 30 settembre 2026
Direttori di Dipartimento + SIST + CISO	Compilazione e trasmissione del Modello di Categorizzazione Attività e Servizi (scaduto il 30/06/2026)	Modello trasmesso e ricevuta	entro il 7 ottobre 2026

Scadenza interna di consolidamento: il fascicolo urgente, la gap analysis e il piano di rimedio devono essere consolidati entro il 7 ottobre 2026; la relazione conclusiva della fase urgente deve pervenire alla Direzione Generale entro il 9 ottobre 2026, in tempo utile per la sottoposizione agli organi di amministrazione e direttivi ai sensi dell'art. 23 del D.Lgs. 138/2024 prima del 12 ottobre 2026, fermo restando che l'eventuale data successiva risultante dalla ricevuta PEC non comporta il differimento delle attività programmate.

Clausole finali

- Il presente atto non certifica la conformità NIS della SZN; dispone le verifiche, la chiusura delle evidenze e le azioni necessarie affinché la Direzione Generale e gli Organi competenti possano assumere determinazioni basate su un quadro documentale completo.
- Gli incarichi di CISO, Referente per la Cybersicurezza e RTD sono disciplinati dal relativo atto di conferimento, cui il presente atto rinvia. Le funzioni di Punto di contatto NIS e Referente CSIRT sono invece allineate sulla piattaforma ACN secondo la disciplina vigente e gli atti di designazione applicabili.
- Qualsiasi modifica delle informazioni già comunicate ad ACN deve essere aggiornata tempestivamente e, nei casi previsti, entro quattordici giorni dalla modifica.
- La presente disposizione è trasmessa al Presidente, ai componenti degli organi interessati, al SIST, al RPD/DPO, all'Ufficio Risorse Umane, all'Ufficio competente in materia di appalti e contratti, al Protocollo e ai Direttori di Dipartimento e responsabili di sede, per quanto di competenza.

Il Direttore Generale
Ing. Massimo Ferdinando Francesco Cavaliere

MASSIMO FERDINANDO
FRANCESCO CAVALIERE
23.09.2026 16:35:51
GMT+02:00

ALLEGATO A – Ricognizione degli atti disponibili e delle acquisizioni ancora necessarie

L'Allegato A costituisce la checklist documentale iniziale del fascicolo NIS. La classificazione "disponibile" indica che il documento è presente tra gli atti esaminati; non equivale, da sola, ad attestazione di adempimento corrente se il contenuto è riferito ad annualità precedenti.

A.1 – Atti già disponibili e utilizzabili

Atto/documento	Esito	Utilizzo nel fascicolo/atto	Nota istruttoria
Decreto Presidente Rep. 92/2024 – Referente per la Cybersicurezza	**DISPONIBILE**	Prova del precedente assetto L. 90/2024	Da leggere insieme alla rinuncia 2025; non prova l'attuale titolarità.
Comunicazione SZN ad ACN del 15/10/2024	**DISPONIBILE**	Evidenza della trasmissione della nomina del Referente	Utile come antecedente; verificare eventuali comunicazioni successive.
Decreto Presidente Rep. 117/2024 – nomina CISO	**DISPONIBILE**	Compiti e precedente presidio CISO	Da leggere insieme alla rinuncia 2025; non prova l'attuale titolarità.
Dichiarazione NIS DNISA00000077 del 17/02/2025	**DISPONIBILE**	Storico prima registrazione	Conteneva autovalutazione "essenziale", superata dalla decisione ACN.
Comunicazione ACN / Det. DG ACN n. 136430 del 12/04/2025; prot. ACN 136514	**DISPONIBILE**	Prova inserimento 2025, status e codice IT7A47VA	Status ufficiale: soggetto importante.
Notifiche Portale ACN del 26/05/2025 e 10/07/2025	**DISPONIBILI**	Evidenze puntuali di aggiornamenti organizzativi/ruoli 2025	Non sostituiscono export completo 2026.
Nota attività CISO prot. 0006699 del 28/07/2025	**DISPONIBILE**	Storico adempimenti/criticità e base per verifiche tecniche	Le criticità 2025 vanno riesaminate e non possono essere date per attuali.
Rinuncia CISO/Referente cyber prot. 0007264 del 01/09/2025	**DISPONIBILE**	Prova della rinuncia ai due incarichi	Impone verifica del successivo assetto e di eventuale presa d'atto/sostituzione.
Comunicazione ACN 2026 relativa a DNISA00041955 / Det. 127159 del 10/04/2026	**DISPONIBILE**	Prova permanenza 2026	Conferma status soggetto importante e codice IT7A47VA.
Verbale Tavolo Settoriale Ricerca MUR 14/04/2026 + presentazioni ACN/CRUI-CODAU	**DISPONIBILI**	Supporto metodologico su categorizzazione, fornitori, requisiti	Materiale di indirizzo/supporto; non sostituisce specifiche ACN.
Vademecum NIS ACN settembre 2026 + promemoria soggetti 2025	**DISPONIBILI**	Calendario e regole operative	Fonte primaria di riferimento per tempistiche e aggiornamenti.

Atto/documento	Esito	Utilizzo nel fascicolo/atto	Nota istruttoria
Nota Presidente 25/08/2026 e riscontro DG 04/09/2026 su CISO/RTD/IA	**DISPONIBILI**	Antecedenti istruttori del conferimento 2026	Il conferimento è disposto con Decreto Rep. n. 171/2026, da inserire nel fascicolo.
PIAO SZN 2026 – formazione "Cybersicurezza: sviluppare la consapevolezza nella PA"	**DISPONIBILE**	Base del piano formativo 2026	Va integrato con evidenze di effettiva erogazione/partecipazione.
Proposta AON dicembre 2024 – NIS2 Gap Analysis/Compliance	**DISPONIBILE**	Documento di pianificazione/supporto	Non è prova di gap analysis svolta; acquisire eventuale deliverable finale.

A.2 – Documenti/evidenze da acquisire o verificare prima della chiusura del fascicolo

Documento/evidenza	Perché serve	Responsabile acquisizione	Priorità
PEC ACN di inserimento 2025 completa della ricevuta di avvenuta consegna	Fissa il giorno esatto del termine di 18 mesi. Il solo protocollo ACN del 12/04/2025 non prova la ricezione PEC.	Protocollo + PDC NIS	**CRITICA**
Copia/esportazione della Dichiarazione DNISA00041955 e relativa ricevuta 2026	Prova il contenuto effettivamente dichiarato nel 2026.	PDC NIS	**ALTA**
Ricevuta/estrazione dell'aggiornamento informazioni 15/04-31/05/2026	Prova l'adempimento annuale 2026 e lo stato attuale delle informazioni.	PDC NIS	**CRITICA**
Elenco dei fornitori rilevanti NIS comunicato nel 2026	È parte delle informazioni da mantenere aggiornate e supporta supply-chain risk.	PDC + Appalti/Contratti + SIST	**CRITICA**
Ricevuta ed export della categorizzazione attività/servizi 2026	Prova l'adempimento ex art. 30 e definisce il perimetro operativo.	PDC + SIST + owner servizi	**CRITICA**
Snapshot/export corrente dei ruoli Portale ACN: PDC, sostituto, CSIRT, sostituti, organi, utenze	Verifica che ruoli e associazioni siano attuali e operativi.	PDC NIS	**CRITICA**
Copia dell'atto di conferimento 2026 (CISO/Referente cyber/RTD); ricostruzione documentata della copertura delle funzioni dal 1° settembre 2025 alla data di conferimento; ricevute delle comunicazioni ad ACN e AgID/IPA	Documenta il presidio organizzativo, il periodo intermedio non comunicato sul Portale ACN e il riallineamento dei ruoli verso ACN e AgID.	DG + Protocollo + CISO	**CRITICA**

Documento/evidenza	Perché serve	Responsabile acquisizione	Priorità
Eventuali Delibere CdA n. 158 del 15/10/2024 e n. 177 del 28/11/2024 in copia firmata	Sono richiamate in documenti di lavoro successivi come atti collegati alle nomine 92/117; occorre verificarne contenuto e natura prima di citarle come presupposti formali.	Segreteria CdA / Protocollo	MEDIA
Eventuale deliverable finale AON: gap analysis, report, piano di adeguamento, evidenze di esecuzione	Distingue una proposta commerciale/progettuale da attività effettivamente svolta.	SIST/DG/RUP se presente	ALTA
Evidenze aggiornate di chiusura delle criticità tecniche segnalate nel luglio 2025	Serve a sapere se logging amministratori, SIEM, IP pubblici, rete e altre criticità siano ancora aperte.	SIST + funzione cyber	CRITICA
Registro incidenti 2026 e prove di operatività della notifica CSIRT	Dimostra readiness su un obbligo già vigente.	CSIRT referent + SIST + funzione cyber	CRITICA
Inventario corrente di sistemi/asset/servizi rilevanti, diagrammi rete, accessi remoti, backup/restore, vulnerability/patch evidence	Costituisce base tecnica per le misure di sicurezza e per il gap assessment.	SIST + Dipartimenti/Sedi	CRITICA
Registro formazione cyber 2025-2026 e formazione organi ex art. 23	Dimostra attuazione, non solo programmazione.	RU / Formazione	ALTA
Quesito SZN ad ACN e riscontro dell'Agenzia del 21 settembre 2026	Documenta la ricognizione e l'indicazione dell'Agenzia sui due adempimenti scaduti.	CISO	CRITICA
Ricevuta di trasmissione dell'Aggiornamento delle Informazioni 2026	Chiude un adempimento scaduto il 31/05/2026.	CISO + Protocollo	CRITICA
Ricevuta di trasmissione della Categorizzazione Attività e Servizi 2026	Chiude un adempimento scaduto il 30/06/2026.	CISO + Protocollo	CRITICA

A.3 – Atti di contesto utili, ma non indispensabili per l'adozione del presente atto

- la Delibera CdA n. 16 del 16 novembre 2018 relativa al precedente assetto RTD/SIST, utile soprattutto se l'istruttoria CISO dovesse evolvere verso un conferimento unitario con il ruolo RTD;
- la Delibera CdA n. 134 del 4 agosto 2022 di nomina del RPD/DPO e la Delibera CdA n. 28 del 12 marzo 2020 sul data breach, già richiamate nel Decreto CISO 117/2024, utili per completare la matrice di governance;
- le presentazioni e i materiali formativi GARR/SZN del 2025, utili quale evidenza di awareness ma non sostitutivi del registro di formazione individuale;
- il dossier istruttorio CISO/RTD/IA 2026 e le bozze di avviso interno, da tenere separati dagli atti effettivamente adottati e da utilizzare soltanto come supporto alla distinta istruttoria organizzativa.