AREA A1 - SERVIZI ISTITUZIONALI, PATRIMONIO, INNOVAZIONE E TECNOLOGIA COMUNALE
Servizio: Servizio Segreteria del Sindaco, trasparenza, progetti e finanziamenti speciali, innovazione e tecnologia comunale
Ufficio: Ufficio SITEC e Trasparenza

DELIBERAZIONE
della Giunta comunale

Seduta N. 18 Delibera n. **75** del **17/04/2026**

OGGETTO: **AREA A1 – SITEC E TRASPARENZA – APPROVAZIONE DEL MODELLO DI GOVERNANCE E STRATEGIA DELLA CYBERSECURITY DEL COMUNE DI AOSTA IN ATTUAZIONE DELLA DISCIPLINA NAZIONALE ED EUROPEA (DIRETTIVA UE 2022/2555, L. N. 90/2024 E D.LGS. N. 138/2024) ELABORATO NELL'AMBITO DEL PIANO NAZIONALE DI RIPRESA E RESILIENZA – FINANZIATO DALL'UNIONE EUROPEA – NEXTGENERATIONEU - MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY" M1C1I1.5 – PROGETTO "POTENZIAMENTO DELLA RESILIENZA CYBER PER IL COMUNE DI AOSTA", ED INDIVIDUAZIONE DI UN ULTERIORE SOSTITUTO REFERENTE CSIRT AI SENSI DELLA DETERMINAZIONE N. 379887/2025 DEL DIRETTORE GENERALE DELL'AGENZIA PER LA CYBERSICUREZZA NAZIONALE**

Nome	Presenza
Rocco Raffaele	Presente
Fadda Valeria	Presente
Cometto Corrado	Presente
Gheller Marco	**Assente**
Lazzarotto Cecilia	**Assente**
Sapinet Alina	Presente
Salerno Simonetta	Presente
Tonino Luca	Presente

Presiede la seduta il Sindaco, **Raffaele Rocco**.

Partecipa alla seduta il Segretario Generale , **Stefano Franco**.

LA GIUNTA COMUNALE

Premesso che:

- la crescente digitalizzazione della società e dell'economia ha reso la cybersicurezza una priorità fondamentale per la salvaguardia degli interessi nazionali e la resilienza dei servizi essenziali;
- con il Decreto Legislativo 18 maggio 2018, n. 65, recante "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione", l'Italia ha dato attuazione, recependola nell'ordinamento nazionale, alla Direttiva (UE) 2016/1148, cosiddetta "Direttiva NIS" (Network and Information Security), volta a definire le misure necessarie per conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi;
- le contingenze in ambito nazionale e internazionale, che vanno dalla superata emergenza sanitaria ai più recenti conflitti bellici, ai continui e attuali attacchi informatici nei confronti di istituzioni nazionali pubbliche e private, che assicurano l'erogazione di servizi essenziali o critici (es: energetici, finanziari, informativi), hanno contribuito a catalizzare ulteriormente l'attenzione dei Legislatori nazionali e sovranazionali sulla cybersecurity, nella consapevolezza che la stessa non costituisce solo un fattore di regolamentazione utile allo sviluppo di un mercato digitale unico, ma rappresenta anche un interesse fondamentale per provvedere alla sicurezza degli Stati nazionali;
- in tale contesto, l'Unione Europea ha adottato la Direttiva (UE) 2022/2555, nota come "Direttiva NIS 2", con l'obiettivo di armonizzare le normative nazionali in materia di cybersicurezza e rafforzare la resilienza dei soggetti critici e importanti;
- la Direttiva NIS2, inserendosi nel più ampio quadro delle politiche strategiche della Commissione Europea in materia di cybersicurezza, come il Cybersecurity Act e il Cyber Resilience Act, aggiorna le norme introdotte con la Direttiva del 2016, per tenere il passo con una maggiore digitalizzazione e un panorama in evoluzione per quanto riguarda i rischi derivanti dalle minacce e dagli incidenti, modernizzando la disciplina esistente e riducendo la discrezionalità degli Stati membri;
- in particolare, rispetto alla precedente Direttiva del 2016 (cd. "Direttiva NIS"), la Direttiva NIS2 ha apportato significative revisioni allo scopo di superare carenze intrinseche emerse in fase di attuazione e affrontare le sfide emergenti in materia di sicurezza informatica;
- la "Direttiva NIS2" ha principalmente l'obiettivo:
  - di eliminare le divergenze nell'attuazione della normativa tra gli Stati membri, promuovendo un quadro normativo più uniforme e coordinato;
  - di aumentare la cooperazione tra gli Stati membri;

- di aggiornare l'elenco dei settori soggetti agli obblighi in materia di cybersicurezza;
- di estendere gli obblighi di sicurezza a un maggior numero di settori e servizi ritenuti vitali per le attività sociali ed economiche, superando la precedente distinzione tra operatori di servizi essenziali e fornitori di servizi essenziali;

- l'Italia ha recepito tale Direttiva attraverso il Decreto Legislativo 4 settembre 2024, n. 138 recante "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la Direttiva (UE) 2016/1148", pubblicato in Gazzetta Ufficiale del 1° ottobre 2024 ed in vigore dal 16 ottobre 2024;
- l'applicazione del summenzionato Decreto Legislativo va inoltre coordinata con la Legge 28 giugno 2024, n. 90 (che definisce il Perimetro di Sicurezza Nazionale Cibernetico), la quale ha introdotto importanti adempimenti per le pubbliche amministrazioni rientranti nel perimetro di applicazione, con lo scopo di rafforzare la sensibilità e la protezione dei predetti soggetti rispetto ai rischi informatici aventi impatto su reti, sistemi informativi e servizi informatici, e ha inserito, tra gli altri, l'obbligo di individuare un «referente per la cybersicurezza»;
- in tal senso, con Deliberazione n. 146 del 5 agosto 2024, la Giunta comunale ha individuato nell'Ufficio e nel Responsabile per la transizione al digitale, ovvero nell'ufficio "SITEC e trasparenza" del Servizio n. 11 dell'Area A1, rispettivamente, la struttura ed il referente per la cybersicurezza del Comune di Aosta, cui sono attribuite le funzioni previste dall'art. 8, comma 1, della Legge 28 giugno 2024, n. 90, stabilendo al contempo che gli stessi si avvarranno, nell'espletamento delle proprie funzioni, di un supporto specialistico esterno fornito dalla società partecipata IN.VA. S.p.A.– C.F. e P.IVA 00521690073, il cui dettaglio è definito nell'ambito dei servizi compresi nella Convenzione in essere ed eventuali aggiornamenti successivi;
- per quel che concerne la suddetta struttura per la cybersicurezza, la citata L. 90/2024, all'art. 8, comma 1, stabilisce che la stessa *"(…) provvede:*

  a) allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni;
  b) alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico;
  c) alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione;
  d) alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione;
  e) alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d);

f) alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale;
g) al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza.";

- con Determinazione del Direttore Generale dell'Agenzia per la cybersicurezza nazionale (di seguito anche ACN) n. 379860 del 19 dicembre 2025 il Comune di Aosta (00120680079) è stato individuato quale soggetto importante ai sensi del D.lgs. n. 138/2024;
- con successiva Determinazione del Direttore generale dell'Agenzia per la Cybersicurezza Nazionale n. 379887 del 19 dicembre 2025 *"di cui all'articolo 7, comma 6, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, recante termini, modalità e procedimenti di utilizzo e accesso alla piattaforma digitale nonché ulteriori informazioni che i soggetti devono fornire all'Autorità nazionale competente NIS e termini, modalità e procedimento di designazione dei rappresentanti NIS sul territorio nazionale*" è stata aggiornata la precedente determinazione (n. 333017 del 22 settembre 2025), disciplinando, tra l'altro, le modalità di designazione del punto di contatto e di aggiornamento annuale e continuo delle informazioni, tramite i servizi dedicati NIS/Aggiornamento annuale e NIS/Aggiornamento continuo disponibili sul Portale ACN;
- in data 8 gennaio 2026 è stata approvata la deliberazione della Giunta comunale n. 2/2026 avente ad oggetto "Decreto legislativo 4 settembre 2024, n. 138 e determinazione n. 379887/2025 del direttore generale dell'Agenzia per la cybersicurezza nazionale - individuazione dell'organo amministrativo e direttivo, del punto di contatto per la cybersicurezza e del suo sostituto, e del referente CSIRT e suo sostituto";
- con deliberazione della Giunta comunale n. 22 del 2 febbraio 2026 è stato approvato il Piano Integrato di Attività e Organizzazione (PIAO) 2026-2028, avente come Appendice n. 3 il "Piano triennale per l'informatica del Comune di Aosta 2026-2028", con particolare riferimento al capitolo 7 "Sicurezza informatica" per il miglioramento del governo della cybersecurity, l'adozione di politiche e strategia di sicurezza, di procedure di sicurezza, in tema di governance e gestione del rischio cyber quale obiettivo strategico sia della precedente, sia dell'attuale consiliatura;

Visti:

- la deliberazione della Giunta comunale n. 126 del 23 giugno 2021, avente ad oggetto "Nuovo assetto organizzativo delle aree e dei servizi dell'Ente", così come modificata dalla deliberazione della Giunta comunale n. 124 del 28 luglio 2023;

- il decreto del Sindaco n. 43 del 13 novembre 2023 con il quale il Segretario generale del Comune di Aosta, dr Stefano Franco, dirigente dell'Area A1 "Servizi istituzionali, patrimonio, innovazione e tecnologia comunale", è stato nominato quale Responsabile per la transizione digitale (RTD);
- la deliberazione della Giunta comunale n. 113 del 17 giugno 2024, avente ad oggetto "Area A1 - Segreteria generale - Assetto organizzativo - approvazione definitiva "Disciplina della graduazione, definizione dei criteri e delle modalità di attribuzione degli incarichi di posizioni di particolare responsabilità" e graduazione delle PPR", con la quale sono state approvate le schede descrittive di ciascuna posizione di particolare responsabilità, le quali sostituiscono, con decorrenza 1° luglio 2024, quelle approvate nella suddetta deliberazione della Giunta comunale n. 126/2021;
- la scheda del Servizio n. 11 "Segreteria del Sindaco, progetti e finanziamenti speciali, trasparenza, innovazione e tecnologia comunale", approvata con la suddetta D.G.C. n. 113/2024, all'interno della quale è precisato che tra le competenze attribuite al Servizio vi sono le attività riconducibili al Responsabile della Transizione al Digitale in riferimento all'art. 17 del d.lgs. 82/2005 e s.m.i. (Ufficio della transizione al digitale);
- la deliberazione della Giunta regionale n. 1099 dell'11 agosto 2025 con la quale è stato istituito presso la società in house IN.VA. S.p.A. il Computer Security Incident Response Team della Valle d'Aosta (denominato "CSIRT Valle d'Aosta" o "CSIRT-VDA");

Rilevato che:

- il rafforzamento delle capacità di cybersecurity del sistema comunale è una priorità per il Comune di Aosta quale strumento decisivo per rispondere efficacemente alle crescenti sfide del mondo digitale e dare esecuzione, al contempo, alle strategie nazionali ed europee;
- la citata normativa nazionale in materia di cybersicurezza guarda in modo specifico al miglioramento del governo della cybersecurity da parte delle organizzazioni pubbliche e private e dispone in materia di adozione di politiche e strategia di sicurezza, di procedure di sicurezza; la stessa prevede inoltre un obbligo di notifica degli "incidenti informatici" in un tempo contingentato a pena di sanzioni, nonché obblighi in tema di governance e gestione del rischio cyber;
- in tale contesto, in data 26 febbraio 2024 l'Agenzia per la Cybersicurezza Nazionale (di seguito anche ACN) ha promosso l'avviso pubblico n. 08/2024 in qualità di Soggetto attuatore dell'Investimento 1.5 "Cybersecurity" – Missione 1, Componente 1, del PNRR, a titolarità della Presidenza del Consiglio dei Ministri - Dipartimento per la trasformazione digitale, a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5, finanziato dall'Unione

Europea – Next Generation EU, per l'attuazione degli investimenti finalizzati alla realizzazione di interventi di potenziamento della resilienza cyber per la Pubblica Amministrazione, rivolto, tra gli altri, ai Comuni capoluogo di Regione, avente come termine per la conclusione delle attività il 30 aprile 2026 e come termine per la rendicontazione il 30 giugno 2026;

- il Comune di Aosta ha stabilito di aderire al suddetto avviso con deliberazione della Giunta comunale n. 54 del 28 marzo 2024;
- con le nota prot. n. 30781 del 25 settembre 2024, prot. n. 34059 del 21 ottobre 2024 e prot. n. 250 del 3 gennaio 2025, recepite agli atti in pari date al civ. prot. n. 56544/2024, civ. prot. n. 61448/2024 e civ. prot. n. 309/2025, ACN ha trasmesso rispettivamente le Determinazioni prot. n. 30550 del 23 settembre 2024, prot. n. 33707 del 17 ottobre 2024 e prot. n. 43937 del 31 dicembre 2024, recanti l'approvazione della graduatoria finale a valere sull'Avviso n. 8/2024, con relativi allegati, con particolare riferimento all'allegato A riportante la graduatoria definitiva delle proposte progettuali ammesse e totalmente finanziabili, tra le quali risulta quella del Comune di Aosta denominata "Potenziamento della resilienza Cyber per il Comune di Aosta", per un importo finanziabile pari ad euro 671.000,00;
- il suddetto progetto prevede 5 interventi (Governance e programmazione cyber; Gestione del rischio cyber e della continuità operativa; Gestione e risposta agli incidenti di sicurezza; Gestione delle identità digitali e degli accessi logici; Sicurezza delle applicazioni, dei dati e delle reti), per i quali sono previste due tipologie di intervento (Miglioramento dei processi e dell'organizzazione e Progettazione e sviluppo di nuovi sistemi e tecnologie), due categorie di costo (Acquisizione di servizi e Acquisizione di beni), e le attività come di seguito dettagliato:

Intervento	**Tipologia di intervento**	**Attività**
1. Governance e programmazione cyber	B. Miglioramento dei processi e dell'organizzazione	Formalizzare una procedura per la gestione, la revisione e l'aggiornamento periodico dell'inventario degli asset dell'organizzazione che includa processi e procedure da adottare per sistemi client, server, utenze, applicazioni aziendali utilizzate on-premises e cloud e le informazioni minime da censire, durante tutto il loro ciclo di vita.

1. Governance e programmazione cyber	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Implementare soluzioni tecnologiche che permettano il censimento degli asset e delle loro configurazioni all'interno di un inventario e la mappatura dei dati e dei loro flussi tra sistemi (CMDB).
2. Gestione del rischio cyber e della continuità operativa	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare una procedura di Business Impact Analysis (BIA).
3. Gestione e risposta agli incidenti di sicurezza	B. Miglioramento dei processi e dell'organizzazione	Integrare la procedura di gestione e analisi dei log, definita in collaborazione con INVA, prevedendo i processi di raccolta, analisi, conservazione, e protezione per tutti i tipi di log (es: log degli amministratori di sistema, log di accesso ai database, log di sicurezza, etc).
3. Gestione e risposta agli incidenti di sicurezza	B. Miglioramento dei processi e dell'organizzazione	Prevedere l'aggiornamento della procedura già esistente di Disaster Recovery, includendo dei piani di ripristino elaborati specificatamente per l'Ente, e che preveda una fase di aggiornamento degli stessi a seguito di test periodici e/o cambiamenti del contesto dell'organizzazione e/o incidente.
4. Gestione delle identità digitali e degli accessi logici	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare all'interno di uno specifico documento le linee guida relative alla gestione sicura delle utenze. In particolare, il documento dovrà contenere indicazioni circa: le modalità di creazione, modifica, cancellazione e ricertificazione delle utenze; le modalità di assegnazione, modifica, rimozione e ricertificazione dei diritti di accesso. Il documento dovrà anche prevedere la necessità di utilizzare solamente utenze nominative ed univoche e regolare l'accesso da remoto alle risorse.
5. Sicurezza delle applicazioni, dei dati e delle reti	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare una procedura e/o metodologia per la classificazione, gestione e protezione delle informazioni e delle risorse (IT, IoT e Cloud) in base alla loro criticità in termini di

		riservatezza, integrità e disponibilità, prevendendo l'aggiornamento a cadenza periodica.
5. Sicurezza delle applicazioni, dei dati e delle reti	B. Miglioramento dei processi e dell'organizzazione	Definire e formalizzare, all'interno di uno specifico documento, il processo di gestione delle vulnerabilità. Tale processo deve comprendere una fase di identificazione delle vulnerabilità (in modalità continua o periodica), analisi, valutazione e classificazione e, infine, risoluzione.
5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Implementare soluzioni di firewall
5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Potenziare la sicurezza delle reti locali interne all'Ente (Sostituzione apparati LAN obsoleti delle 7 sedi dell'Ente e attivazione NAC)
5. Sicurezza delle applicazioni, dei dati e delle reti	D. Progettazione e sviluppo di nuovi sistemi e tecnologie	Potenziare la sicurezza delle postazioni di lavoro (Attivazione EDR centralizzato)

- nell'ambito del suddetto intervento denominato "Sicurezza delle applicazioni, dei dati e delle reti" – tipologia di intervento "Progettazione e sviluppo di nuovi sistemi e tecnologie" – categoria di costo "Acquisizione di beni", sono state previste le attività di implementazione delle soluzioni di firewall e attivazione NAC, per le quali il Comune di Aosta con determinazione dirigenziale n. 168/2025 ha stabilito di aderire dell'Accordo Quadro (AQ) – ID 2367 denominato "Cybersecurity 2 – Prodotti e servizi connessi – LOTTO 2, stipulato da CONSIP S.p.A. ai sensi dell'art. 54, comma 3 del D. Lgs n. 50/2016, e Telecom Italia S.p.A., con sede legale in Milano, Via Gaetano Negri n. 1, P. IVA 00488410010 in qualità di impresa mandataria capogruppo del Raggruppamento Temporaneo di Imprese composto, oltre alla stessa, dal-le mandanti Maticmind S.p.A. con sede legale in Milano, Via Roberto Bracco n.6, P. IVA 05032840968, DGS S.p.A., con sede legale in Roma, Via Paolo Di Dono n. 73, P. IVA 03318271214, e SCAI Solution Group S.p.A., con sede legale in Milano, Viale Monte Nero n.73, P. IVA 05348521005; e con successiva determinazione dirigenziale n. 170/2025 ha approvato il relativo ordine di acquisto per un importo pari ad euro 165.765,95 (Iva inclusa);
- per quel che concerne tutte le altre attività previste nei suddetti interventi progettuali, con deliberazione della Giunta comunale n. 63/2025 è stato stabilito di avvalersi del supporto della società partecipata IN.VA. S.p.A., per un importo massimo pari ad euro 503.982,00 (Iva inclusa), nell'ambito del finanziamento progettuale ammesso, e con

determinazione dirigenziale n. 533 del 29 luglio 2025 è stato affidato il servizio in argomento alla società IN.VA. S.p.A. per un importo pari ad euro 413.100,00 (Iva esclusa), e quindi in complessivi 503.982,00 (Iva inclusa), il cui contratto è stato sottoscritto nella forma dell'atto pubblico in data 25 settembre 2025 – numero 14777/2025;

- con la suddetta determinazione dirigenziale n. 533/2025 è stato assunto a favore di IN.VA. S.p.A. di Brissogne (C.F. e Partita IVA 00521690073) l'impegno n. 2061/2025 per l'importo di euro 503.982,00, esigibilità 2025, e l'accertamento n. 726/2025 di pari importo;
- con determinazioni dirigenziali n. 720 del 16 ottobre 2025 (successivamente rettificata con n. 62 del 3 febbraio 2026) e n. 933 del 16 dicembre 2025 sono stati approvati il Certificato di Regolare Esecuzione e il Rapporto di fine intervento, attestanti la corretta fornitura e installazione degli apparati di sicurezza di cui al suddetto Accordo Quadro (AQ) – ID 2367, con conseguente autorizzazione alla fatturazione;
- con determinazione dirigenziale n. 934 del 16 dicembre 2025, tra le altre, è stato approvato lo Stato Avanzamento Lavori (SAL) in relazione al quinto bimestre dell'anno 2025 delle attività svolte da IN.VA. S.p.A. di Brissogne (C.F. e Partita IVA 00521690073) nell'ambito dell'affidamento di cui alla determinazione dirigenziale n. 533/2025 e contratto rep. n. 14777/2025, trasmesso con nota civ. prot. n. 72964 dell'11 dicembre 2025 e controfirmato per accettazione dal sottoscritto RUP e dai Responsabili dell'istruttoria (civ. prot. n. 73256/2025);
- con determinazione dirigenziale n. 197 del 3 aprile 2026, tra le altre è stato approvato lo Stato Avanzamento Lavori (SAL) conclusivo delle attività svolte da IN.VA. S.p.A. di Brissogne (C.F. e Partita IVA 00521690073) nell'ambito dell'affidamento di cui alla determinazione dirigenziale n. 533/2025 e contratto rep. n. 14777/2025, trasmesso con nota civ. prot. n. 15721 del 20 marzo 2026 e controfirmato per accettazione dal sottoscritto RUP e dai Responsabili dell'istruttoria (civ. prot. n. 16327/2026);
- allegati al suddetto SAL (civ. prot. n. 15721/2026), IN.VA. S.p.A. ha inviato, tra gli altri, i seguenti documenti prodotti nell'ambito dei Servizi di supporto per il miglioramento dei processi e dell'organizzazione per il Comune di Aosta in ambito Cybersecurity:
  - Classificazione e protezione delle informazioni.pdf
  - Comunicazione di Chiusura della Crisi.pdf
  - Dichiarazione Stato di Crisi.pdf
  - Gestione Analisi dei Log.pdf
  - Linee Guida gestione sicura delle Utenze e degli Accessi.pdf
  - Piano di Continuità Operativa.pdf

- Procedura di Business Impact Analysis.pdf
- Procedura di Gestione degli Asset.pdf
- Procedura Gestione delle Vulnerabilità.pdf;

Rilevato che le attività svolte nell'ambito del progetto PNRR "Potenziamento della resilienza Cyber per il Comune di Aosta", nonché il percorso progressivo di rafforzamento della capacità comunale in materia di cybersicurezza illustrato nelle premesse, hanno portato alla definizione di un modello strategico ed organizzativo di cybersecurity;

Ritenuto quindi di approvare:

- il modello di governance della cybersicurezza del Comune di Aosta - Allegato A al presente provvedimento;
- il modello strategico della cybersicurezza del Comune di Aosta - Allegato B al presente provvedimento – costituito dai seguenti documenti:
  - Classificazione e protezione delle informazioni.pdf
  - Comunicazione di Chiusura della Crisi.pdf
  - Dichiarazione Stato di Crisi.pdf
  - Gestione Analisi dei Log.pdf
  - Linee Guida gestione sicura delle Utenze e degli Accessi.pdf
  - Piano di Continuità Operativa.pdf
  - Procedura di Business Impact Analysis.pdf
  - Procedura di Gestione degli Asset.pdf
  - Procedura Gestione delle Vulnerabilità.pdf;

  facenti parte del deliverable trasmesso da IN.VA. S.p.A. (civ. prot. n. 15721/2026), in considerazione altresì del ruolo che la stessa società svolge quale fornitore strategico di servizi operativi di cybersecurity nei confronti del Comune di Aosta;

dando atto che entrambi costituiscono il Modello di governance e strategia di cybersecurity del Comune di Aosta;

Vista inoltre la nota civ. prot. n. 13098 del 9 marzo 2026 con la quale IN.VA. S.p.A. ha individuato un ulteriore sostituto referente CSIRT, ai sensi dell'art. 7, della Determinazione n. 379887/2025 del Direttore generale dell'Agenzia per la Cybersicurezza Nazionale, in aggiunta al nominativo indicato nella nota civ. prot. n. 562/2026, sempre dipendente del

SOC - Security Operation Center - Area Cybersecurity della stessa società, e ritenuto di procedere con l'aggiunta di questo nominativo nel "Portale NIS" di ACN;

Richiamati infine:

- la deliberazione del Consiglio comunale n. 141 del 29 dicembre 2025 con la quale è stato approvato il Bilancio di previsione per il triennio 2026-2028 e i suoi allegati;
- la deliberazione del Consiglio comunale n. 142 del 29 dicembre 2025 con la quale è stata approvata la Nota di aggiornamento al Documento unico di Programmazione (DUP) 2026-2028 (sezione strategica 2026-2030);
- la deliberazione del Consiglio comunale n. 24 del 25 febbraio 2026 con la quale è stata approvata l'integrazione alla Nota di aggiornamento al Documento unico di Programmazione (DUP) 2026-2028 (sezione strategica 2026-2030 e sezione operativa 2026-2028);
- la deliberazione della Giunta comunale n. 9 del 16 gennaio 2026 avente ad oggetto: "Area A2 - Servizio bilancio. Approvazione del Piano esecutivo di gestione 2026-2028";
- il decreto del Sindaco n. 71 del 18 novembre 2025 di attribuzione delle funzioni di gestione dell'Area A1 – Servizi Istituzionali, Patrimonio, Innovazione e Tecnologia comunale attribuite al Segretario Generale del Comune di Aosta;

Visti il parere favorevole di legittimità ed il parere favorevole di regolarità contabile attestante la copertura finanziaria rilasciati, ai sensi dell'art. 49bis della L.R. 54/1998 e successive modifiche ed integrazioni e dell'art. 5 del regolamento di contabilità, dai dirigenti competenti;

Considerato che l'adozione del presente provvedimento è di competenza della Giunta Comunale ai sensi dell'art. 23 dello Statuto Comunale e per il combinato della L.R. 22/2010 e della L.R. 54/1998 e successive modifiche ed integrazioni;

Con voti favorevoli unanimi, resi nei modi di legge, dando atto che alla votazione hanno partecipato il Sindaco e 5 Assessori;

D E L I B E R A

1. di approvare il Modello di governance e strategia di cybersecurity del Comune di Aosta – Allegati A e B al presente provvedimento;

2. di trasmettere il presente provvedimento, a cura dell'ufficio proponente, per gli eventuali adempimenti consequenziali, a tutti i soggetti interessati, con particolare

riferimento ai soggetti individuati nella deliberazione della Giunta comunale n. 2/2026 e all'Agenzia per la Cybersicurezza Nazionale (ACN);

3. di individuare quale ulteriore sostituto referente CSIRT, ai sensi dell'art. 7, della Determinazione n. 379887/2025 del Direttore generale dell'Agenzia per la Cybersicurezza Nazionale, il dipendente indicato da IN.VA. S.p.A. con la nota civ. prot. n. 13098/2026 e di incaricare il Dirigente dell'Area A1 al caricamento del nominativo sul "Portale NIS" di ACN;

4. di dare atto che il presente provvedimento non comporta spesa.

IL SINDACO: ***Raffaele Rocco***
IL SEGRETARIO GENERALE : ***Stefano Franco***
(Documento firmato digitalmente)