CONSIGLIO REGIONALE DEL PIEMONTE - Determinazioni dirigenziali

DETERMINAZIONE DIRIGENZIALE

Codice Direzione A0300F Codice Settore A0304C

Rep. N. A0304C/88/2026 del 08/10/2026

NIS 2 - Adozione delle misure di sicurezza di base di cui all'allegato 1 alla determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale (ACN) n. 379907 del 19 dicembre 2025.

PREMESSA

Vista la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (nel seguito denominata "direttiva NIS 2");

Visti gli articoli 23, comma 1, 24 e 31, comma 4 del decreto legislativo 4 settembre 2024, n. 138, recante "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148." (nel seguito denominato "decreto NIS");

Vista la determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale (ACN) n. 379907 del 19 dicembre 2025 e, in particolare, l'art. 3 - che stabilisce il termine per l'adozione delle specifiche di base, con scadenza, per il Consiglio regionale del Piemonte, al 12 ottobre 2026 - nonché gli allegati 1 e 3 alla stessa, che stabiliscono, rispettivamente, le misure di sicurezza di base e gli incidenti significativi di base per i soggetti importanti;

Vista l'Appendice C alle "Linee guida NIS - Specifiche di base - Guida alla lettura", versione 2.1 di aprile 2026 emanate dall'ACN;

Considerato che tra le misure di sicurezza di base previste dal summenzionato allegato 1 rientra l'approvazione, da parte degli organi di amministrazione e direttivi, dei seguenti undici documenti: "Organizzazione per la sicurezza informatica", "Piano per la gestione degli incidenti di sicurezza informatica", "Politiche di sicurezza informatica", "Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete", "Piano di trattamento del rischio", "Piano di gestione delle vulnerabilità", "Piano di adeguamento", "Piano di continuità operativa", "Piano di ripristino in caso di disastro", "Piano di gestione delle crisi", "Piano di formazione";

Considerato che i documenti "Organizzazione per la sicurezza informatica" e "Piano per la gestione degli incidenti di sicurezza informatica" hanno già trovato approvazione con la determinazione dirigenziale rep. n. A0304B/396/2025 del 29/12/2025 e che il requisito concernente il Piano di formazione deve intendersi soddisfatto mediante la programmazione formativa del Consiglio regionale contenuta nel PIAO vigente, allegato alla deliberazione dell’Ufficio di Presidenza n. 23 del 29 gennaio 2026, e sarà assicurato anche per le annualità successive attraverso il relativo aggiornamento periodico nell'ambito dei futuri PIAO;

Considerata, altresì, l'opportunità di adottare anche un ulteriore documento a fini di raccordo organico in materia di continuità operativa e gestione delle crisi, denominato "Modello metodologico per la continuità operativa e la gestione delle crisi";

Vista la deliberazione dell’Ufficio di Presidenza n. 318 del 18 dicembre 2025 "PIANO GENERALE DI ATTUAZIONE DELLA DIRETTIVA (UE) 2022/2555 "NIS 2" E DEL D.LGS. 138/2024 IN CONSIGLIO REGIONALE DEL PIEMONTE. APPROVAZIONE." (nel seguito denominata "DUP n. 318");

Considerato che nel succitato "Piano generale di attuazione della direttiva (UE) 2022/2555 "NIS 2" e del D.lgs. 138/2024 in Consiglio regionale del Piemonte", al paragrafo 9, sono elencati i documenti di cui il Consiglio regionale deve dotarsi al fine di adempiere gli obblighi imposti dal decreto NIS;
Vista la deliberazione dell’Ufficio di Presidenza n. 198 del 30 luglio 2025, così come modificata dalla DUP n. 318, la quale ha confermato esclusivamente i direttori del Consiglio regionale quali "organi amministrativi e direttivi dell'Ente";

Considerato che l’attuazione delle misure di sicurezza di base previste dalla disciplina NIS richiede altresì la predisposizione e il progressivo aggiornamento di ulteriori documenti attuativi e operativi, tra cui procedure operative, inventari, registri, matrici, istruzioni tecniche e ulteriori strumenti di supporto, la cui redazione e manutenzione saranno curate dal Settore Sistemi Informativi e Archivistici, con il coinvolgimento delle strutture e dei soggetti competenti, in una fase successiva all’approvazione dei documenti allegati al presente provvedimento;

Tutto cio' premesso,

IL DIRETTORE

a. Visti gli artt. 4 e 16 del D.lgs. n. 165/2001;
b. vista la l.r. 7/2001;
c. visto il D. lgs n. 118/2011 come modificato dal D. lgs n. 126/2014;
d. vista la l.r. 23/2008;
e. vista la D.U.P. n. 117/2011;
f. vista la D.U.P. n. 122/2011;
g. vista la D.U.P. n. 62/2013;
h. Vista la DCR 136-27423 del 16.12.2025;
i. Vista la D.C.R. 167-17646 del 28.07.2026;
j. vista la D.U.P. 136/2026;

Nell'ambito delle risorse assegnate con D.U.P. n.ro 266 del 30 luglio 2026

D E T E R M I N A

1. di approvare il documento "Politiche di sicurezza informatica", allegato alla presente determinazione per farne parte integrante e sostanziale (Allegato A);
2. di approvare il documento "Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete", allegato alla presente determinazione per farne parte integrante e sostanziale (Allegato B);
3. di approvare il documento "Piano di trattamento del rischio", allegato alla presente determinazione per farne parte integrante e sostanziale (Allegato C);
4. di approvare il documento "Piano di gestione delle vulnerabilità", allegato alla presente determinazione per farne parte integrante e sostanziale (Allegato D);
5. di approvare il documento "Piano di adeguamento", allegato alla presente determinazione per farne parte integrante e sostanziale (Allegato E);
6. di approvare il documento "Modello metodologico per la continuità operativa e la gestione delle crisi", allegato alla presente determinazione per farne parte integrante e sostanziale (Allegato F);

7. di approvare il documento "Piano di continuità operativa", allegato alla presente determinazione per farne parte integrante e sostanziale (Allegato G);
8. di approvare il documento "Piano di ripristino in caso di disastro", allegato alla presente determinazione per farne parte integrante e sostanziale (Allegato H);
9. di approvare il documento "Piano di gestione delle crisi", allegato alla presente determinazione per farne parte integrante e sostanziale (Allegato I);
10. di demandare al Settore Sistemi Informativi e Archivistici la predisposizione, il progressivo aggiornamento e il coordinamento degli ulteriori documenti attuativi e operativi necessari all'attuazione delle misure di sicurezza NIS, tra cui procedure operative, inventari, registri, matrici e istruzioni tecniche, assicurando, ove necessario, il coinvolgimento delle strutture organizzative competenti e dei soggetti gestori dei sistemi e dei servizi.

Il Direttore

Michele Pantè