



Giunta Regionale della Campania

DECRETO DIRIGENZIALE

DIRETTORE GENERALE/
DIRIGENTE UFFICIO/STRUTTURA
DIRIGENTE SETTORE
DIRIGENTE UOS

Massimo BISOGNO

DECRETO N°	DEL	DIREZ. GENERALE / UFFICIO / STRUTT.	SETTORE	UOS
329	24/09/2026	301	00	00

Oggetto:

Approvazione del “Template Accordo per l’attivazione e la gestione di un collegamento VPN site-to-site” e della relativa “Scheda Tecnica VPN site-to-site”.

IL DIRIGENTE

PREMESSO che

- a. la Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio del 14 dicembre 2022 istituisce il programma strategico per il decennio digitale 2030, nel cui quadro assumono rilievo lo sviluppo di infrastrutture digitali sicure e sostenibili e la digitalizzazione dei servizi pubblici;
- b. il decreto legislativo 7 marzo 2005, n. 82, recante il “Codice dell’amministrazione digitale”, disciplina l’organizzazione e l’impiego delle tecnologie dell’informazione e della comunicazione nelle pubbliche amministrazioni e, in particolare, all’articolo 51 pone specifici obblighi in materia di sicurezza, disponibilità, integrità, riservatezza e continuità dei sistemi, delle infrastrutture e dei dati;
- c. il Regolamento (UE) 2016/679 (“GDPR”) e il decreto legislativo 30 giugno 2003, n. 196, come modificato dal decreto legislativo 10 agosto 2018, n. 101, impongono l’adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio e la protezione dei dati personali fin dalla progettazione e per impostazione predefinita;
- d. il Regolamento (UE) 2019/881 (“Cybersecurity Act”) rafforza il quadro europeo della cybersicurezza e il ruolo dell’ENISA, promuovendo un elevato livello di sicurezza delle tecnologie dell’informazione e della comunicazione;
- e. la Direttiva (UE) 2022/2555 (“NIS2”) ha definito misure volte ad assicurare un livello comune elevato di cybersicurezza nell’Unione europea e ha rafforzato gli obblighi di gestione del rischio, sicurezza delle reti e dei sistemi informativi e gestione degli incidenti;
- f. il Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024 (Cyber Resilience Act), ha definito i requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali, che stabilisce requisiti essenziali di cybersicurezza con riferimento alla progettazione, allo sviluppo e alla produzione dei prodotti con elementi digitali e alla gestione delle relative vulnerabilità durante il ciclo di vita;
- g. il decreto legislativo 4 settembre 2024, n. 138, di recepimento della Direttiva NIS2, disciplina il quadro nazionale per la cybersicurezza, prevedendo, per i soggetti rientranti nel relativo ambito di applicazione, misure tecniche, operative e organizzative adeguate e proporzionate per la gestione dei rischi e degli incidenti;
- h. la legge 28 giugno 2024, n. 90, recante “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici”, ha ulteriormente rafforzato il presidio organizzativo e operativo della cybersicurezza nelle pubbliche amministrazioni;
- i. il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, ha ridefinito l’architettura nazionale di cybersicurezza e istituito l’Agenzia per la cybersicurezza nazionale (ACN);
- j. la Strategia Nazionale di Cybersicurezza 2022-2026 e il relativo Piano di implementazione individuano tra gli obiettivi strategici il rafforzamento della resilienza cyber delle pubbliche amministrazioni, la protezione degli asset digitali e il consolidamento dei processi di prevenzione, gestione e risposta agli incidenti;
- k. il Piano Triennale per l’Informatica nella Pubblica Amministrazione 2024-2026, come da ultimo aggiornato per il 2026, individua sicurezza informatica, infrastrutture e interoperabilità quali

componenti essenziali della trasformazione digitale della PA, secondo principi di sicurezza e protezione dei dati by design e by default;

PREMESSO, altresì, che

- a. la Regione Campania, nell'ambito delle proprie funzioni istituzionali e dei processi di trasformazione digitale, gestisce infrastrutture, reti, sistemi e servizi informativi che richiedono livelli adeguati di sicurezza, affidabilità, tracciabilità e continuità operativa;
- b. l'Ufficio Speciale per l'Amministrazione Digitale assicura, nell'ambito delle competenze attribuite dall'ordinamento regionale, funzioni di governo e presidio delle infrastrutture digitali, delle reti, dei servizi ICT e della sicurezza informatica regionale;
- c. con nota del 22 ottobre 2024, prot. n. 34342, l'Agenzia per la Cybersicurezza Nazionale ha comunicato l'esito positivo dell'analisi preliminare tecnica relativa alle dichiarazioni di conformità rese per il Data Center regionale ai sensi del Decreto direttoriale ACN n. 5489/2023;
- d. l'Ufficio ha adottato e mantiene un Sistema di Gestione Integrato (SGI) conforme agli standard UNI EN ISO 9001:2015 e UNI CEI EN ISO/IEC 27001:2022, con estensioni ISO/IEC 27017 e ISO/IEC 27018, quale presidio organizzativo per la qualità dei servizi e la sicurezza delle informazioni;

CONSIDERATO che

- a. nell'esercizio delle attività istituzionali può rendersi necessario attivare collegamenti permanenti e cifrati tra l'infrastruttura regionale e infrastrutture appartenenti a soggetti terzi, pubblici o privati, al fine di consentire, per specifiche finalità e nel rispetto delle rispettive competenze, l'interoperabilità dei sistemi, lo scambio controllato di informazioni e la fruizione di servizi applicativi;
- b. l'attivazione di collegamenti VPN site-to-site determina l'instaurazione di un canale di comunicazione tra domini infrastrutturali distinti e richiede, pertanto, la preventiva definizione e formalizzazione del perimetro dell'interconnessione, dei flussi autorizzati, dei parametri tecnici, delle misure di sicurezza, delle responsabilità, dei referenti, delle modalità di monitoraggio, modifica, sospensione, gestione degli incidenti e dismissione;
- c. la standardizzazione della documentazione relativa a tali collegamenti consente di applicare in modo uniforme i principi di minimo privilegio, segregazione, necessità, tracciabilità, security by design e risk-based approach, assicurando che la disponibilità del collegamento tecnico non si traduca in un'autorizzazione generalizzata all'accesso alle reti, ai sistemi o ai dati;
- d. a tale scopo sono stati predisposti il documento "USAD_LEX_ACVPN_TE_01 - Template Accordo VPN site-to-site", che disciplina gli aspetti giuridici, organizzativi e di sicurezza dell'interconnessione, e il documento "USAD_LEX_ACVPN_AL_01 - Scheda Tecnica VPN site-to-site", destinato a censire e validare gli elementi tecnici e operativi necessari all'attivazione e alla gestione del collegamento;
- e. il Template prevede, tra l'altro, che il collegamento sia limitato ai soli endpoint, subnet, host, protocolli, porte, direzioni e ambienti censiti nella Scheda Tecnica, che le modifiche siano

- preventivamente valutate e autorizzate e che siano disciplinate le attività di collaudo, monitoraggio, manutenzione, gestione degli incidenti e dismissione;
- f. la Scheda Tecnica costituisce lo strumento operativo per la raccolta e la validazione dei contatti tecnici, degli endpoint VPN, dei parametri di negoziazione e cifratura, dei domini di cifratura e delle regole firewall/VPN relative ai soli flussi autorizzati;
 - g. l'adozione di una modulistica uniforme consente di assicurare la preventiva formalizzazione e il censimento delle interconnessioni verso soggetti esterni, rafforzando la governance, la tracciabilità e la gestione del rischio nell'ambito del Sistema di Gestione Integrato;

RILEVATO che

- a. i documenti predisposti risultano coerenti con l'esigenza di disciplinare in modo uniforme, preventivo e tracciabile l'attivazione e la gestione di collegamenti VPN site-to-site con soggetti esterni, definendo un quadro minimo comune di requisiti giuridici, organizzativi, tecnici e di sicurezza;
- b. la documentazione è funzionale al mantenimento e al miglioramento continuo del Sistema di Gestione Integrato, in quanto introduce un presidio documentale specifico per una tipologia di interconnessione suscettibile di incidere sul perimetro di sicurezza delle reti e dei sistemi regionali;
- c. l'approvazione dei documenti non costituisce, di per sé, autorizzazione all'attivazione di singoli collegamenti VPN, che resta subordinata alla compilazione e validazione della Scheda Tecnica, alle verifiche tecniche e di sicurezza, al collaudo e alla sottoscrizione dell'accordo con la specifica controparte;

RITENUTO

- a. di dover approvare il documento "USAD_LEX_ACVPN_TE_01 - Template Accordo VPN site-to-site", allegato al presente provvedimento quale Allegato A, a costituirne parte integrante e sostanziale;
- b. di dover approvare il documento "USAD_LEX_ACVPN_AL_01 - Scheda Tecnica VPN site-to-site", allegato al presente provvedimento quale Allegato B, a costituirne parte integrante e sostanziale;
- c. di dover stabilire che i documenti di cui alle lettere precedenti costituiscono documentazione del Sistema di Gestione Integrato dell'Ufficio Speciale per l'Amministrazione Digitale e che, conseguentemente, gli stessi saranno recepiti nel documento "USAD_SGI_MSGI_AL_02 - Elenco Documentale del SGI" in occasione del successivo aggiornamento dell'Elenco Documentale, assicurandone la classificazione, il controllo delle versioni e la gestione secondo le regole del SGI;
- d. di dover stabilire che il Template e la Scheda Tecnica costituiscono il modello di riferimento da utilizzare, fatte salve le necessarie personalizzazioni connesse allo specifico servizio e alla specifica controparte, per l'attivazione e la gestione di collegamenti VPN site-to-site tra l'infrastruttura regionale e infrastrutture di soggetti esterni;

VISTI

- il D.Lgs. 7 marzo 2005, n. 82 e ss.mm.ii.;
- il D.L. 14 giugno 2021, n. 82, convertito dalla L. 4 agosto 2021, n. 109;
- la L. 28 giugno 2024, n. 90;
- il D.Lgs. 4 settembre 2024, n. 138;
- il Regolamento (UE) 2016/679;
- la L.R. 15 maggio 2024, n. 6;
- la L.R. 28 luglio 2017, n. 23;
- la D.G.R. n. 408 del 31 luglio 2024;
- la D.G.R. n. 315 del 4 giugno 2025 e il D.P.G.R.C. n. 63 del 27 giugno 2025;
- tutti gli atti richiamati in premessa;

alla stregua dell'istruttoria compiuta dall'Ufficio Speciale per l'Amministrazione Digitale, nonché dell'espressa dichiarazione di regolarità formale del presente atto resa dal Direttore dell'Ufficio Speciale per l'Amministrazione Digitale.

DECRETA

per i motivi esposti in narrativa che qui si intendono integralmente riportati e trascritti:

1. di approvare il documento “USAD_LEX_ACVPN_TE_01 - Template Accordo VPN site-to-site” (Allegato A), che forma parte integrante e sostanziale del presente provvedimento;
2. di approvare il documento “USAD_LEX_ACVPN_AL_01 - Scheda Tecnica VPN site-to-site” (Allegato B), che forma parte integrante e sostanziale del presente provvedimento;
3. di stabilire che i documenti approvati con il presente provvedimento entrano a far parte della documentazione del Sistema di Gestione Integrato dell'Ufficio Speciale per l'Amministrazione Digitale e saranno inseriti nel documento “USAD_SGI_MGSGI_AL_02 - Elenco Documentale del SGI” in occasione del successivo aggiornamento dello stesso, con la relativa classificazione, revisione e gestione documentale secondo le procedure del SGI;
4. di stabilire che il Template e la Scheda Tecnica costituiscono il modello di riferimento per la formalizzazione, la valutazione, l'attivazione, il collaudo, l'esercizio, il monitoraggio, la modifica, la sospensione e la dismissione dei collegamenti VPN site-to-site tra l'infrastruttura regionale e infrastrutture appartenenti a soggetti esterni, ferme restando le verifiche tecniche, organizzative, di sicurezza e di protezione dei dati richieste in relazione al singolo collegamento;
5. di precisare che l'approvazione dei modelli non determina l'automatica autorizzazione di alcuna interconnessione e che ogni singolo collegamento dovrà essere previamente istruito, censito e validato, con individuazione delle finalità, del perimetro, dei flussi autorizzati, dei referenti e delle misure di sicurezza applicabili, nonché sottoposto a collaudo prima dell'esercizio;
6. di demandare alle competenti funzioni dell'Ufficio Speciale per l'Amministrazione Digitale gli adempimenti necessari alla diffusione, applicazione, manutenzione e aggiornamento dei documenti approvati, secondo le rispettive attribuzioni e le procedure del Sistema di Gestione Integrato;

7. di trasmettere il presente provvedimento, per gli adempimenti di rispettiva competenza, alle strutture dell'Ufficio Speciale per l'Amministrazione Digitale interessate;
8. di disporre la pubblicazione del presente provvedimento nella Sezione relativa agli adempimenti previsti dalla L.R. n. 23 del 28/07/2017 “Regione Campania Casa di Vetro”.

Massimo BISOGNO

Firmato digitalmente ai sensi del CAD e normativa connessa