AGENZIA REGIONALE PROTEZIONE AMBIENTALE DELLA CAMPANIA

DELIBERAZIONE DEL DIRETTORE GENERALE N. 285 DEL 01/04/2026

IL RUP LA VIA

OGGETTO: AVVISO PUBBLICO N. 08/2024 PER LA PRESENTAZIONE DI PROPOSTE DI INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER DEI GRANDI COMUNI, DEI COMUNI CAPOLUOGO DI REGIONE, DELLE CITTÀ METROPOLITANE, DELLE AGENZIE REGIONALI SANITARIE E DELLE AZIENDE ED ENTI DI SUPPORTO AL SERVIZIO SANITARIO NAZIONALE, DELLE AUTORITÀ DI SISTEMA PORTUALE, DELLE AUTORITÀ DEL BACINO DEL DISTRETTO IDROGRAFICO E DELLE AGENZIE REGIONALI PER LA PROTEZIONE DELL'AMBIENTE A VALERE SUL PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY", CODICE D'INVESTIMENTO M1C1I1.5 – CUP E64F24000280006. PRESA D'ATTO DELLA CONCLUSIONE DEL PROGETTO, APPROVAZIONE DEL QUADRO ECONOMICO FINALE E DELLA RELAZIONE CONCLUSIVA.

L'anno duemilaventisei, il giorno uno del mese di Aprile presso la sede dell'A.R.P.A.C. alla stregua dell'istruttoria compiuta dal RUP e della dichiarazione di completezza e regolarità resa dal medesimo

PREMESSO CHE

- con deliberazione n. 141 del 22/03/2024 l'Agenzia ha approvato la partecipazione all'Avviso Pubblico ACN n. 08/2024 relativo alla Misura PNRR M1C1 Investimento 1.5 "Cybersecurity", con approvazione del progetto preliminare;
- con deliberazione n. 195 del 12/04/2024 è stata rettificata la predetta deliberazione n. 141/2024, con approvazione della nuova versione del progetto preliminare e del relativo quadro finanziario, per un importo complessivo pari ad € 1.262.713,42 IVA inclusa, riferito al progetto contraddistinto dal CUP E64F24000280006;
- con deliberazione n. 512 del 17/10/2024 ARPAC ha preso atto dell'ammissione a finanziamento del progetto per l'intero importo richiesto, pari ad € 1.262.713,42 IVA inclusa, nonché del relativo Atto d'Obbligo disciplinante i rapporti con l'Agenzia per la Cybersicurezza Nazionale;
- il progetto risultava finalizzato al rafforzamento complessivo della postura di cybersicurezza dell'Agenzia, attraverso interventi di natura tecnologica, organizzativa, procedurale e formativa;
- il termine originariamente previsto per la conclusione delle attività progettuali era fissato al 31.12.2025; successivamente, per effetto di formali proroghe concesse da ACN, il termine di conclusione del progetto è stato differito al 31.03.2026 e successivamente al 30.04.2026;
- entro il 28.02.2026 risultano completate tutte le attività previste da progetto, come da documentazione agli atti e da relazione finale predisposta dal Responsabile di Progetto;

CONSIDERATO CHE

- per l'attuazione del progetto l'Agenzia ha proceduto ai seguenti affidamenti:

1 deliberazione n. 566 del 14/11/2024, relativa all'adesione all'Accordo Quadro CONSIP ID 2296 – Lotto 1 "Servizi di Sicurezza da Remoto", per un importo imputato al progetto pari ad € 183.000,00 IVA inclusa;

2 deliberazione n. 584 del 26/11/2024, relativa all'adesione all'Accordo Quadro CONSIP ID 2296 – Lotto 2 "Servizi di Compliance e Controllo", per un importo imputato al progetto pari ad € 984.906,00 IVA inclusa;

3 deliberazione n. 587 del 27/11/2024, relativa all'acquisizione tramite MePA delle licenze Cyber Guru per attività di awareness e simulazione phishing, per un importo imputato al progetto pari ad € 10.540,80 IVA inclusa;

- gli affidamenti sopra richiamati hanno consentito la realizzazione degli interventi previsti nella progettualità finanziata, in coerenza con gli obiettivi di potenziamento della resilienza cyber dell'Ente;
- sulla base degli atti adottati e delle spese imputate al progetto, il Quadro economico finale risulta così determinato:

Voce	Importo finale (IVA inclusa)
Acquisizione di beni e servizi	1.178.446,80 €
Spese generali (7%)	82.491,28 €
Totale finale progetto	1.260.938,08 €

- rispetto all'importo complessivamente ammesso a finanziamento, pari ad € 1.262.713,42 IVA inclusa, si determina una economia finale pari ad € 1.775,34;
- il RUP ha predisposto apposita relazione conclusiva delle attività svolte, da allegare alla presente deliberazione quale parte integrante e sostanziale, nella quale si dà atto dell'avvenuto completamento delle attività progettuali entro il termine prorogato del 31.03.2026, e del conseguimento degli obiettivi previsti;
- occorre, pertanto, procedere alla formale presa d'atto della conclusione del progetto, nonché all'approvazione del Quadro economico finale e della relazione conclusiva;

RITENUTO

- di dover prendere atto che, in attuazione del progetto finanziato, risultano eseguite tutte le attività previste, secondo quanto rappresentato nella relazione conclusiva allegata al presente provvedimento;
- di dover procedere alla formale conclusione del progetto, atteso che le attività previste risultano completate e coerenti con gli obiettivi approvati e con gli affidamenti disposti per la sua attuazione;
- di dover approvare la Relazione conclusiva di progetto, dalla quale si evince l'avvenuta esecuzione delle attività programmate ed il conseguimento dei risultati attesi nell'ambito della progettualità finanziata;

ATTESO CHE tutti gli atti richiamati nella presente deliberazione sono depositati presso l'ufficio proponente;

VISTI

- la Direttiva NIS2 – Direttiva (UE) 2022/2555;
- il D. Lgs. 82/2005;
- il D. Lgs. 36/2023;

- la L.R. 10/98 ed il vigente Regolamento sull'Organizzazione di ARPAC;
- la deliberazione n. 815/2025 di approvazione di Bilancio di previsione esercizio 2026 e pluriennale per il triennio 2026/2028.

Per tutto quanto premesso e considerato si propone di adottare la seguente

DELIBERAZIONE

Per le motivazioni espresse in narrativa che qui si intendono integralmente riportate e trascritte:

- di prendere atto della conclusione del progetto finanziato nell'ambito del PNRR – Missione 1, Componente 1, Investimento 1.5 "Cybersecurity", CUP E64F24000280006, originariamente previsto con termine al 31.12.2025 e successivamente prorogato da ACN, con completamento di tutte le attività entro il 31.03.2026 e successivamente 30.04.2026;
- di dare atto che il progetto è stato realizzato mediante i seguenti affidamenti:
  1.1 deliberazione n. 566 del 14/11/2024 – AQ CONSIP Lotto 1 – € 183.000,00 IVA inclusa;
  1.2 deliberazione n. 584 del 26/11/2024 – AQ CONSIP Lotto 2 – € 984.906,00 IVA inclusa;
  1.3 deliberazione n. 587 del 27/11/2024 – acquisizione licenze Cyber Guru – € 10.540,80 IVA inclusa;
- di approvare il Quadro economico finale del progetto come di seguito riportato:

Voce	Importo finale (IVA inclusa)
Acquisizione di beni e servizi	1.178.446,80 €
Spese generali (7%)	82.491,28 €
Totale finale progetto	1.260.938,08 €

- di dare atto che, rispetto al finanziamento complessivamente assentito pari ad € 1.262.713,42 IVA inclusa, residua una economia finale pari ad € 1.775,34;
- di approvare la Relazione conclusiva di progetto, allegata al presente provvedimento quale parte integrante e sostanziale, nella quale sono illustrate le attività realizzate, gli interventi eseguiti ed i risultati conseguiti nell'ambito della progettualità finanziata;
- di demandare al RUP ed agli uffici competenti tutti gli adempimenti consequenziali in materia di chiusura amministrativa, rendicontazione finale, conservazione documentale e trasmissione agli organismi competenti della documentazione prevista;
- di allegare al presente atto, quale parte integrante e sostanziale, la Relazione finale di progetto recante il dettaglio degli interventi realizzati e delle attività concluse entro il 28/02/2026;
- di dare atto che si procederà con successivo, separato, provvedimento alla quantificazione ed alla liquidazione dei compensi, se previsti e se dovuti, spettanti alle figure coinvolte nell'attuazione del progetto, nei limiti e secondo le modalità previste dalla normativa e dalla disciplina regolamentare vigente, dando altresì atto che la relativa copertura potrà essere assicurata nell'ambito della quota per le 'Spese generali' (7% di cui sopra) prevista dal Quadro finanziario di Progetto.

Napoli, 31.03.2026

Il Responsabile di Progetto
dott.ssa Loredana LA VIA

La proposta di deliberazione è accolta.

Napoli, 01/04/2026

Il Direttore Generale
Avv. Luigi Stefano SORVINO

OGGETTO: AVVISO PUBBLICO N. 08/2024 PER LA PRESENTAZIONE DI PROPOSTE DI INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER DEI GRANDI COMUNI, DEI COMUNI CAPOLUOGO DI REGIONE, DELLE CITTÀ METROPOLITANE, DELLE AGENZIE REGIONALI SANITARIE E DELLE AZIENDE ED ENTI DI SUPPORTO AL SERVIZIO SANITARIO NAZIONALE, DELLE AUTORITÀ DI SISTEMA PORTUALE, DELLE AUTORITÀ DEL BACINO DEL DISTRETTO IDROGRAFICO E DELLE AGENZIE REGIONALI PER LA PROTEZIONE DELL'AMBIENTE A VALERE SUL PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY", CODICE D'INVESTIMENTO M1C1I1.5 – CUP E64F24000280006. PRESA D'ATTO DELLA CONCLUSIONE DEL PROGETTO, APPROVAZIONE DEL QUADRO ECONOMICO FINALE E DELLA RELAZIONE CONCLUSIVA.

PARERE DI REGOLARITA' AMMINISTRATIVA

Sulla suesposta proposta, avente ad oggetto "AVVISO PUBBLICO N. 08/2024 PER LA PRESENTAZIONE DI PROPOSTE DI INTERVENTI DI POTENZIAMENTO DELLA RESILIENZA CYBER DEI GRANDI COMUNI, DEI COMUNI CAPOLUOGO DI REGIONE, DELLE CITTÀ METROPOLITANE, DELLE AGENZIE REGIONALI SANITARIE E DELLE AZIENDE ED ENTI DI SUPPORTO AL SERVIZIO SANITARIO NAZIONALE, DELLE AUTORITÀ DI SISTEMA PORTUALE, DELLE AUTORITÀ DEL BACINO DEL DISTRETTO IDROGRAFICO E DELLE AGENZIE REGIONALI PER LA PROTEZIONE DELL'AMBIENTE A VALERE SUL PIANO NAZIONALE DI RIPRESA E RESILIENZA, MISSIONE 1 – COMPONENTE 1 – INVESTIMENTO 1.5 "CYBERSECURITY", CODICE D'INVESTIMENTO M1C1I1.5 – CUP E64F24000280006. PRESA D'ATTO DELLA CONCLUSIONE DEL PROGETTO, APPROVAZIONE DEL QUADRO ECONOMICO FINALE E DELLA RELAZIONE CONCLUSIVA.", in ordine alla regolarità amministrativo-contabile ed alla copertura finanziaria, si esprime parere favorevole.

Data **01/04/2026**

Il Direttore Amministrativo

Luca Antonio Esposito / InfoCert S.p.A.

DELIBERAZIONE N° 285 DEL 01/04/2026

ATTESTAZIONE DI PUBBLICAZIONE

Si dichiara che la presente deliberazione è stata affissa all'Albo di questa Agenzia dal giorno 01/04/2026 e vi resterà per gg 15 (quindici) .

Napoli, **01/04/2026**

Il Funzionario Incaricato
Valeria Torella / InfoCert S.p.A.

DELIBERAZIONE N° 285 DEL 01/04/2026

ATTESTAZIONE DI IMMEDIATA ESEGUIBILITA'

La presente Deliberazione è stata dichiarata immediatamente eseguibile per l'urgenza

Napoli data **01/04/2026**

Il Direttore Generale
Avv. Luigi Stefano SORVINO

Luigi Stefano Sorvino / InfoCert S.p.A.

Relazione tecnica di fine Progetto PNRR M1C1 – Investimento 1.5 "Cybersecurity"

La presente relazione tecnica sintetizza le attività realizzate nell'ambito del progetto di rafforzamento della postura di Cybersecurity dell'Agenzia, finanziato a valere sul **PNRR – Missione 1, Componente 1, Investimento 1.5 "Cybersecurity"**.

L'intervento si è inserito in un percorso più ampio di consolidamento delle capacità organizzative, procedurali e tecnologiche dell'Ente in materia di sicurezza informatica, con l'obiettivo di incrementare il livello di resilienza cyber, migliorare la capacità di prevenzione e risposta agli incidenti, rafforzare la conformità rispetto ai riferimenti normativi applicabili e promuovere una maggiore diffusione della cultura della sicurezza a tutti i livelli dell'organizzazione.

L'attuazione del progetto è stata accompagnata da un'attività continuativa di **supporto PMO (Project Management Office) e technical advisory**, finalizzata al coordinamento complessivo delle iniziative di sicurezza informatica, al presidio delle attività di governance progettuale ed al monitoraggio dello stato di avanzamento delle diverse linee di intervento. Tale supporto ha consentito di assicurare coerenza tra obiettivi strategici, priorità operative e risultati conseguiti, favorendo una gestione strutturata dell'intera progettualità.

Una prima componente fondamentale del progetto ha riguardato la realizzazione di un articolato percorso di **assessment della postura Cyber** dell'Agenzia: in particolare, è stato condotto un assessment trasversale volto ad analizzare in dettaglio procedure, processi, assetti organizzativi e capacità cyber complessive dell'Ente, con l'obiettivo di consolidare il quadro conoscitivo di partenza e supportare la definizione del piano strategico delle iniziative tattiche di rafforzamento.

A tale attività si è affiancato un assessment verticale sulla **gestione delle identità digitali e degli accessi logici**, finalizzato a rilevare il livello di maturità esistente nelle modalità di gestione delle utenze e dei privilegi di accesso, nonché ulteriori assessment mirati sull'operatività del personale e sulla gestione della sicurezza fisica presso i cinque Dipartimenti provinciali.

Il percorso di assessment è stato inoltre accompagnato da attività di follow up, funzionali a monitorare nel tempo l'evoluzione della postura di sicurezza a seguito degli interventi oggetto dell'intera progettualità.

Sulla base delle evidenze emerse è stata sviluppata una rilevante attività di **definizione e formalizzazione dei processi di sicurezza**, mediante la revisione e redazione di un corpo documentale volto a disciplinare ruoli, responsabilità, regole e modalità operative interne ed esterne all'Ente.

In tale ambito sono state predisposte o aggiornate politiche di alto livello relative, tra l'altro, alla gestione dei backup e del recupero dei dati, degli asset, delle identità digitali, della network security, del vulnerability e patch management, della sicurezza delle informazioni, della classificazione dei dati, della gestione dei log, delle manutenzioni, delle password, degli accessi fisici, dell'hardening e della comunicazione tramite e-mail.

Coerentemente con tali politiche, sono state inoltre redatte procedure operative e linee guida di alto livello riguardanti la gestione degli eventi di sicurezza, il BYOD, il disaster recovery, lo sviluppo sicuro, il change management, la gestione degli accessi logici, anche con riferimento agli amministratori di sistema, nonché la relativa modulistica di supporto per la gestione e la revisione periodica delle utenze.

Un'altra linea di intervento ha riguardato il **potenziamento della consapevolezza (awareness) del personale** attraverso un articolato programma di formazione: le attività formative sono state progettate a partire dalla predisposizione di contenuti verticali, materiali dedicati, test di autovalutazione, attestati di partecipazione e prontuari operativi, calibrati in funzione dei destinatari.

Tale impostazione ha consentito di adattare efficacemente i contenuti formativi ai ruoli ed alle responsabilità dei partecipanti, favorendo una maggiore comprensione dei profili di rischio e delle misure di prevenzione: sono state quindi realizzate sessioni rivolte alla dirigenza, al personale IT, al personale amministrativo coinvolto nelle attività di Business Impact Analysis, al personale dei Dipartimenti Provinciali ed al personale non dirigente della struttura centrale, ampliando di fatto la platea dei destinatari ed offrendo a tutta la popolazione agenziale maggiori opportunità di partecipazione.

Nell'ambito del progetto è stata inoltre realizzata una esercitazione di tipo **Table Top**, basata sulla simulazione di uno scenario di crisi cyber non noto ai partecipanti, con il coinvolgimento dei componenti del Comitato di crisi, al fine di testare dinamiche decisionali, coordinamento operativo e capacità di risposta organizzativa.

Le attività formative sono state accompagnate dal supporto PMO nelle fasi di ingaggio, convocazione e raccolta delle presenze; i risultati sono stati poi raccolti in una specifica relazione dedicata, comprensiva del calendario consuntivo delle sessioni erogate.

Il progetto ha inoltre consentito la **definizione e adozione di una metodologia di analisi del rischio**, accompagnata dal supporto operativo alla concreta esecuzione delle analisi: tale linea di attività ha contribuito a rafforzare l'approccio strutturato dell'Ente all'identificazione, valutazione e trattamento dei rischi cyber, in coerenza con il contesto organizzativo e tecnologico di riferimento.

In stretta connessione con tale ambito è stata sviluppata la componente relativa alla **Business Continuity:** in particolare, è stato definito e formalizzato il framework di Business Continuity Management, con individuazione dello scope, delle metodologie di riferimento e del modello organizzativo.

È stata quindi definita la metodologia di **Business Impact Analysis (BIA)** ed è stata eseguita una BIA su un perimetro selezionato di processi e servizi critici afferenti a un insieme di Unità Operative ritenute strategiche per l'erogazione dei servizi dell'Agenzia; sono state inoltre valutate le

capacità di recupero e di ripristino, con definizione dei principali parametri di riferimento, tra cui RTO e RPO, per i servizi critici considerati.

A completamento del lavoro è stato definito il modello di gestione della crisi ICT, comprensivo di workflow operativo di alto livello, ruoli e responsabilità, nonché delle strategie di continuità ICT e del piano di continuità operativa.

Una specifica linea di intervento ha interessato il rapporto con le **terze parti e la sicurezza della supply chain**, attraverso la predisposizione di linee guida per la definizione dei requisiti di sicurezza applicabili ai fornitori, la redazione di clausole contrattuali di incident response coerenti con il quadro normativo di riferimento, incluse le esigenze connesse alla NIS 2, nonché la definizione di una metodologia di verifica dei fornitori.

Sulla base di tale metodologia sono state svolte attività di audit in modalità self-assessment, integrate, ove necessario, da interviste di approfondimento da remoto, al fine di valutare il livello di presidio dei fornitori rispetto ai requisiti di sicurezza richiesti.

Una componente tecnica particolarmente rilevante del progetto ha riguardato la **valutazione della robustezza dei controlli di sicurezza** a presidio dei sistemi infrastrutturali dell'Ente: a tal fine sono stati eseguiti vulnerability assessment su di un perimetro definito di IP e subnet concordati, attraverso una fase iniziale di identificazione del perimetro, dei servizi e delle applicazioni critiche, seguita dalla definizione delle modalità operative di esecuzione delle analisi. Le attività hanno consentito di individuare le principali vulnerabilità potenzialmente espositive a rischi cyber, con successiva produzione di report contenenti le possibili azioni di rimedio, classificate in funzione della criticità rilevata.

A complemento di tali attività sono stati inoltre effettuati '**penetration test**' ed attività di sfruttamento manuale controllato di vulnerabilità note, secondo framework e metodologie di settore, su un perimetro selezionato di sistemi e applicativi dell'Agenzia. Le attività sono state condotte in modalità grey box, sia in una prima fase di verifica, sia in successivi follow-up e re-test svolti a valle delle attività di patching e remediation; anche in questo caso, le risultanze sono state raccolte in specifici report tecnici recanti le evidenze emerse e le corrispondenti indicazioni di miglioramento.

Nell'ambito del rafforzamento delle capacità di gestione degli eventi cyber, è stato predisposto il **Piano di risposta agli incidenti**, articolato nella redazione della procedura di Incident Management, di template per gli incident response report e di playbook operativi relativi a differenti scenari di crisi, tra cui ransomware o malware, phishing e data breach; è stato inoltre costruito un modello di base riutilizzabile per la definizione di ulteriori scenari, in modo da favorire l'evoluzione progressiva e strutturata delle capacità di incident response dell'Ente.

Una componente di particolare rilievo del progetto ha riguardato poi l'attivazione ed il consolidamento di un **presidio operativo continuativo di monitoraggio e gestione della sicurezza**, realizzato nell'ambito del servizio SOC, contesto in cui è stata implementata e configurata una piattaforma **SIEM basata su tecnologia Splunk**, finalizzata alla raccolta centralizzata, all'indicizzazione e alla correlazione dei log provenienti dai sistemi e dalle infrastrutture critiche ricomprese nel perimetro progettuale.

L'attivazione della piattaforma ha consentito di strutturare un servizio di monitoraggio continuo dell'infrastruttura, con analisi in tempo reale degli eventi di sicurezza orientata all'identificazione precoce di anomalie, comportamenti anomali e possibili pattern di attacco. Il servizio ha incluso attività di triage e qualificazione degli alert, finalizzate a distinguere gli eventi effettivamente rilevanti dai falsi positivi, nonché attività di supporto alla gestione degli incidenti mediante la tempestiva predisposizione e trasmissione di azioni di mitigazione e remediation a supporto del ripristino delle condizioni di sicurezza.

A completamento delle funzionalità di monitoraggio è stata integrata una componente **XSOAR basata su tecnologia Cortex di Palo Alto**, a supporto dell'orchestrazione e dell'automazione dei processi di Incident Response; tale componente ha consentito di introdurre playbook automatizzati per l'esecuzione di procedure standardizzate e la riduzione dei tempi di risposta, nonché di gestire in modo più strutturato il ciclo di vita degli incidenti, integrando differenti fonti informative e automatizzando le principali azioni di contenimento.

L'adozione integrata delle soluzioni SIEM e XSOAR ha contribuito a migliorare l'efficacia operativa del presidio SOC, ad aumentare la tracciabilità delle attività e a garantire una visione più organica dello stato della sicurezza.

In parallelo il progetto ha incluso anche l'implementazione e la gestione di una soluzione **Managed EDR H24**, finalizzata al monitoraggio continuo degli endpoint (postazioni di lavoro) ed al rafforzamento delle capacità di rilevazione e gestione degli incidenti di sicurezza sugli asset terminali: in tale ambito sono state adottate piattaforme e strumenti dedicati, tra cui **Trend Micro Vision One**, l'integrazione con piattaforma **RedCarbon** basata su funzionalità di analisi avanzata, un portale di monitoraggio e una piattaforma di Incident Management, oltre all'erogazione del servizio SOC continuativo e al supporto di un Service Manager dedicato.

Le attività principali hanno incluso il monitoraggio costante di alert, anomalie e minacce, l'analisi e classificazione degli incidenti in base alla severità, il supporto alle azioni di remediation, quali patching, isolamento degli endpoint e attivazione di blocchi di sicurezza, nonché la produzione di report tecnici sugli incidenti e sulle attività svolte. Nella fase iniziale sono state completate le attività di setup, configurazione delle piattaforme, verifica del corretto deployment degli agent sugli endpoint e tuning delle policy di sicurezza.

È stato inoltre erogato un servizio di **Service Desk**, con gestione e tracciamento delle richieste tramite sistema di ticketing e classificazione per priorità e tipologia.

A rinforzo del presidio SOC e delle soluzioni implementate, sono state svolte attività di **supporto specialistico evolutivo**, finalizzate all'ottimizzazione continua delle capacità di rilevazione e gestione degli eventi di sicurezza: in particolare, sono state condotte attività di tuning delle regole di correlazione e dei pattern di notifica sulle piattaforme SIEM e XSOAR, con l'obiettivo di ridurre i falsi positivi e incrementare il valore degli alert realmente significativi.

Parallelamente sono state sviluppate nuove logiche di detection ed ulteriori use case di monitoraggio, orientati all'individuazione di tecniche di attacco avanzate e modellati anche sulla base dei framework di settore, in modo da adattare il presidio alle caratteristiche dell'infrastruttura e dei

servizi dell'Agenzia. Sono state altresì eseguite attività periodiche di **proactive threat hunting**, volte alla ricerca attiva di minacce latenti o compromissioni non ancora rilevate dagli strumenti automatici, mediante analisi di log storici e indicatori di compromissione. Il servizio ha compreso anche il supporto all'aggiornamento, al consolidamento e all'integrazione di nuove sorgenti dati nell'ecosistema di monitoraggio, così da garantirne la continuità operativa, l'evoluzione nel tempo e la coerenza con gli obiettivi di compliance.

Particolare attenzione è stata inoltre dedicata agli aspetti di **reporting, governance e controllo del servizio**, attraverso la produzione di report periodici e SAL finalizzati ad assicurare piena visibilità sull'andamento operativo delle attività di sicurezza: sono stati predisposti executive report contenenti analisi relative agli alert di sicurezza, agli incidenti gestiti, alle notifiche ed ai principali trend rilevati, nonché reportistica di dettaglio sullo stato dei ticket, sulla tracciabilità delle attività e sui tempi di lavorazione.

I SAL periodici hanno consentito di monitorare l'andamento del servizio, verificare KPI e SLA, individuare eventuali criticità o rischi e definire le opportune azioni correttive, mantenendo costante l'allineamento rispetto agli obiettivi progettuali ed ai requisiti di conformità. Il servizio ha incluso inoltre attività di **Light Incident Response (MDR)**, comprendenti interventi remoti sugli endpoint, supporto al team IT nelle azioni di contenimento e gestione degli incidenti critici con comunicazioni tempestive.

Nel complesso, il presidio realizzato ha garantito un modello di gestione della sicurezza continuativo, proattivo e orientato al miglioramento costante della postura Cyber dell'Ente.

Il progetto ha incluso anche una rilevante linea di attività in ambito **compliance GDPR,** ambito in cui si è proceduto all'aggiornamento del registro dei trattamenti ed alla revisione o predisposizione di processi, procedure e template documentali in materia di privacy by design, requisiti privacy per lo sviluppo, nomina degli amministratori di sistema, gestione del data breach, gestione delle richieste degli interessati, nomina dei responsabili del trattamento, definizione di una baseline di misure di sicurezza, clausole standard di protezione dei dati e linee guida BYOD.

È stato inoltre eseguito un pre-assessment di DPIA sui trattamenti considerati, in un'ottica di rafforzamento dell'approccio preventivo e strutturato alla protezione dei dati personali.

Infine, a completamento del percorso di crescita della cultura della sicurezza informatica, è stato attivato ed erogato un **programma continuativo di security awareness** tramite il modulo **Cyber Guru Phishing**, fondato su campagne di simulazione di attacchi e-mail calibrate sul livello di preparazione degli utenti, sul monitoraggio dei comportamenti e sulla produzione di specifica reportistica di analisi: tale attività ha contribuito a rafforzare la consapevolezza del personale rispetto ai principali vettori di attacco connessi al fattore umano e a misurare nel tempo l'efficacia delle azioni di sensibilizzazione intraprese. Ed i risultati sono stati estremamente positivi: nel periodo rendicontato risultano concluse dieci campagne, per un totale di **5.740 attacchi simulati inviati**, **357 click**

effettuati ed un **click rate medio del 6,2%** (di molto inferiore a quello di partenza, rilevato con la prima campagna).

Nel suo complesso, il Progetto ha consentito di sviluppare un percorso organico e strutturato di rafforzamento della Cybersecurity dell'Agenzia, intervenendo in modo integrato sugli aspetti di governance, processi, organizzazione, monitoraggio, gestione degli incidenti, continuità operativa, analisi del rischio, compliance normativa e formazione del personale.

Le attività svolte hanno contribuito ad accrescere il livello di maturità dell'Ente, a migliorare la capacità di prevenzione, rilevazione e risposta agli eventi di sicurezza ed a consolidare le basi per il proseguimento del percorso di adeguamento ai requisiti normativi e strategici in materia di Cyber-sicurezza.

Il Responsabile Progetto
dott.ssa Loredana **LA VIA**