REGIONE DEL VENETO

PROCEDURA APERTA TELEMATICA, AI SENSI DELL'ART. 71 DEL D.LGS. N. 36/2023 E SS.MM.II, PER L'ACQUISTO DI SERVIZI DI SICUREZZA PER IL CSIRT REGIONALE DELLA DURATA DI 48 MESI, IN DUE LOTTI.

CODICE GARA APPTEL: **G03944**

Lotto 1 CUI: **S80007580279202600043**

Lotto 2 CUI:

S80007580279202600044 - **S80007580279202400040** - **S80007580279202400043** - **S80007580279202500049**

CONTESTO DEL CSIRT

Indice

Glossario

Acronimo	Significato
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
SOC	Security Operation Center
CTI	Cyber Threat Intelligence
BIA	Business Impact Analysis
SAST	Static Application Security Testing
DAST	Dynamic Application Security Testing

Premessa

Il **CERT-CSIRT Regionale del Veneto** nasce dalla volontà di Regione del Veneto di dotarsi di un presidio strutturato e coordinato a supporto della cybersecurity degli enti del territorio. Il percorso istitutivo ha preso avvio nel **settembre 2022** con la deliberazione della **Giunta regionale n. 1174 del 27 settembre 2022**, che ha sancito formalmente la creazione del CERT-CSIRT regionale. L'avvio operativo è seguito nell'agosto 2023 con l'approvazione del progetto esecutivo (D.G.R. n. 1024/2023), cui ha fatto seguito, nel novembre 2024, l'ammissione a finanziamento nell'ambito dell'Avviso 06/2023. Nel gennaio 2025, con **D.d.r. n. 1025 del 24 gennaio 2025,** è stata approvata la versione 2.1 del progetto esecutivo, che ha consolidato il modello organizzativo e posto le basi per la piena operatività del servizio. Nel marzo 2026 è stata avviata la procedura per il cambio di denominazione in CSIRT Regionale del Veneto, in attesa di formale approvazione da parte della Giunta regionale.

Il modello organizzativo adottato si articola su più livelli di governance: il **Comitato Strategico**, con funzioni di indirizzo e definizione delle priorità evolutive, e il **Comitato Direttivo**, responsabile del governo operativo delle attività. A supporto opera il Team di Governance, con funzioni di raccordo tra gli organi direttivi, i team operativi specialistici — Team Security Strategy e Team di Esperti Cyber — e i referenti degli enti aderenti. L'intero impianto organizzativo è strutturato lungo tre dimensioni fondamentali — persone, processi e tecnologie — al fine di garantire un approccio equilibrato, sostenibile e orientato alla crescita progressiva della maturità di sicurezza degli enti della Constituency.

Nel periodo di riferimento il CERT-CSIRT ha erogato un **portafoglio articolato di servizi**, che include: gestione del rischio, business continuity management, analisi della sicurezza del codice (SAST e DAST), security operations center (SOC) e cyber threat intelligence (CTI), vulnerability management, formazione e sensibilizzazione. A questi si aggiungono servizi a supporto dell'organizzazione, quali la formazione interna del team CERT-CSIRT e il supporto normativo e tecnologico alla Regione del Veneto. L'erogazione di tali servizi ha contribuito a un **progressivo innalzamento del livello di postura di sicurezza degli enti aderenti**, come evidenziato dai risultati del Cyber Maturity Assessment condotto nel periodo, con specifico focus sugli enti sanitari e socio-sanitari, la cui

continuità operativa riveste carattere essenziale per la tutela della salute e del benessere dei cittadini.

Il percorso intrapreso pone le basi per un consolidamento ulteriore del modello operativo, con l'obiettivo di estendere la copertura dei servizi, rafforzare le capacità proattive e reattive degli enti della Constituency e contribuire allo sviluppo di una cultura della cybersecurity diffusa e strutturata nel territorio regionale.

Contesto

Negli ultimi decenni, la crescente diffusione delle tecnologie dell'informazione e della comunicazione ha determinato una profonda trasformazione delle attività sociali, economiche e istituzionali, spostandole in modo sempre più significativo nello spazio cibernetico. Il processo di digitalizzazione dei servizi pubblici ha generato importanti opportunità in termini di efficienza, accessibilità e qualità dei servizi offerti ai cittadini, ma ha al contempo incrementato in maniera rilevante l'esposizione al rischio informatico.

La **progressiva digitalizzazione delle informazioni e dei processi** ha infatti reso le organizzazioni pubbliche maggiormente vulnerabili a eventi di natura cibernetica, con potenziali impatti sulla disponibilità, integrità e riservatezza dei dati trattati. In tale contesto, il crimine informatico rappresenta una delle principali minacce alla sicurezza delle reti e delle informazioni, con effetti economici e operativi sempre più rilevanti.

Negli ultimi anni si è inoltre assistito a **una crescente complessità degli attacchi informatici**, che colpiscono non solo i cittadini ma anche i sistemi e le infrastrutture degli enti pubblici, con particolare riferimento alle strutture sanitarie e sociosanitarie. In questo ambito, l'intensificarsi dei processi di digitalizzazione, se da un lato abilita nuovi modelli organizzativi e operativi, dall'altro espone servizi essenziali per la salute e il benessere della popolazione a rischi cyber sempre più significativi.

Il contrasto e la prevenzione degli attacchi cibernetici, nonché la necessità di garantire adeguati livelli di sicurezza delle reti e delle informazioni, costituiscono pertanto un ambito di primaria attenzione a livello regionale, con l'obiettivo di assicurare la continuità e l'affidabilità dei servizi pubblici, in particolare di quelli critici per la qualità della vita, la salute e la sicurezza del cittadino.

In tale scenario, la crescente consapevolezza del rischio digitale si è tradotta nella definizione di un articolato quadro normativo e strategico a livello regionale, nazionale ed europeo, che richiede agli enti pubblici una gestione strutturata e coordinata del rischio cyber. È all'interno di questo contesto che si **inserisce l'avvio e il progressivo sviluppo del CERT-CSIRT regionale**, quale strumento di supporto, coordinamento e rafforzamento della postura di sicurezza degli enti del territorio.

Origine e obiettivi del CERT-CSIRT

Il CSIRT regionale trae origine dalla volontà di Regione del Veneto di dotarsi di **un modello strutturato e coordinato di supporto alla cybersecurity degli enti del territorio (Constituency)**, in grado di rispondere in maniera organica alle crescenti esigenze di protezione delle reti, dei dati e dei servizi digitali, con particolare riferimento agli ambiti più critici per la collettività.

Il percorso di istituzione del CERT-CSIRT ha preso avvio nel settembre 2022, con l'approvazione del progetto di istituzione di un CERT regionale tramite deliberazione della **Giunta regionale n. 1174 del 27 settembre 2022**. Tale atto ha rappresentato il primo passo formale verso la creazione di un presidio regionale dedicato alla prevenzione, al supporto e al coordinamento in materia di sicurezza informatica.

Successivamente, nell'agosto 2023, con deliberazione della Giunta regionale n. 1024, è stato approvato il progetto esecutivo nella sua prima versione, che ha consentito l'avvio operativo delle attività e la definizione di un modello organizzativo ispirato alle best practice di riferimento in ambito CERT. Il progetto ha quindi proseguito nel proprio percorso evolutivo attraverso ulteriori affinamenti e aggiornamenti, anche grazie all'ammissione a finanziamento della proposta progettuale "Attivazione CERT- CSIRT Regionale" sull'Avviso 06/2023, formalizzata nel novembre 2024.

Nel gennaio 2025, con **Ddr n. 1025 del 24 gennaio 2025**, è stata approvata la **versione 2.1 del progetto esecutivo**, che ha consolidato il modello progettuale e organizzativo del CERT, ponendo le basi per una piena operatività del servizio.

Fin dalla sua origine, il progetto CERT è stato concepito come un'iniziativa di sistema, finalizzata a incrementare il livello di sicurezza dei dati e dei servizi digitali offerti ai cittadini, attraverso il coordinamento del potenziamento della resilienza cyber dei sistemi informativi di numerosi enti regionali. In particolare, il CERT si pone l'obiettivo di favorire una gestione condivisa e strutturata del rischio cyber, promuovendo modelli di governance comuni, la condivisione di informazioni e buone pratiche e la disponibilità di servizi di sicurezza avanzati.

Il progetto è stato strutturato lungo **tre dimensioni fondamentali** – persone, processi e tecnologie – al fine di garantire un approccio equilibrato e sostenibile. Tale impostazione consente di

valorizzare le competenze del personale degli enti aderenti, supportate da adeguati modelli di processo e da soluzioni tecnologiche orientate alla razionalizzazione e alla standardizzazione.

Gli **obiettivi del CERT-CSIRT regionale** si articolano quindi nel fornire supporto alla gestione degli incidenti di sicurezza, nel migliorare la qualità complessiva della sicurezza delle informazioni, nel rafforzare le capacità proattive e reattive degli enti della Constituency e nel contribuire allo sviluppo di una cultura della cybersecurity, con particolare attenzione agli enti sanitari e socio-sanitari, la cui continuità operativa rappresenta un elemento essenziale per la tutela della salute e del benessere dei cittadini.

Modello Organizzativo e di Governance

Il CERT-CSIRT Regionale si basa su un **modello organizzativo e di governo** strutturato su più livelli, pensato per garantire un chiaro indirizzo strategico, un'efficace supervisione delle attività e una corretta erogazione dei servizi a favore degli Enti aderenti.

Al vertice del modello si collocano gli organi di indirizzo, rappresentati da due distinti organismi di *governance*. Il **Comitato Strategico**, presieduto dal Presidente del CERT-CSIRT, ha il compito di definire le linee di sviluppo, gli indirizzi strategici e le priorità evolutive del servizio. Il **Comitato Direttivo**, presieduto dal Responsabile del CERT-CSIRT, è invece deputato al governo operativo delle attività e al monitoraggio dell'erogazione dei servizi, assicurando l'attuazione coerente delle decisioni strategiche.

A supporto degli organi direttivi opera il *Team* di *Governance*, che svolge un ruolo centrale di raccordo tra i Comitati, i *team* operativi del CERT-CSIRT e i referenti degli Enti aderenti. Il *Team* di *Governance* definisce i criteri di qualità dei servizi, supervisiona le attività amministrative e il budget, gestisce i rapporti con fornitori e terze parti coinvolte nell'erogazione dei servizi e supporta l'organizzazione e il funzionamento dei Comitati.

L'erogazione dei servizi è affidata ai *team* operativi specialistici, tra cui il *Team Security Strategy* e il *Team* di Esperti *Cyber*, che operano secondo i criteri e le priorità stabilite dal modello di governo del CERT-CSIRT. Tali strutture sono responsabili dell'attuazione dei servizi nei diversi ambiti della *cybersecurity*, avvalendosi, ove necessario, anche del contributo di fornitori esterni.

Il modello si completa con il coinvolgimento dei referenti degli Enti aderenti, organizzati nella **Constituency del CERT-CSIRT**, con i quali è garantito un flusso continuo di coordinamento e condivisione, al fine di assicurare l'efficacia dei servizi e una progressiva crescita della maturità di sicurezza dell'intero ecosistema regionale.

La Constituency del CERT-CSIRT

La Constituency del CERT-CSIRT è formata da **41 Enti** suddivisi tra Regione del Veneto (Giunta), enti sanitari, enti pubblici regionali strumentali, società a partecipazione regionale maggioritaria, altri enti regionali.

Gli enti sono stati individuati con lo scopo di supportare il territorio nella gestione delle minacce di sicurezza ad esso correlate, in attuazione delle "Linee Guida per l'Agenda Digitale del Veneto 2025" (Deliberazione della Giunta Regionale n. 156 del 22 febbraio 2022) ove si sottolineava la necessità di avviare una collaborazione tra Enti Pubblici e Privati per una gestione condivisa del rischio informatico a livello regionale.

Si elencano gli enti appartenenti alla Constituency del CERT, suddivisi in Gruppi da 1 a 5:

Gruppo	Ente
Gruppo 1	Regione del Veneto (Giunta)
Gruppo 1	Azienda Zero
Gruppo 1	ULSS 1 – Dolomiti
Gruppo 1	ULSS 2 – Marca Trevigiana
Gruppo 1	ULSS 3 – Serenissima
Gruppo 1	ULSS 4 – Veneto Orientale
Gruppo 1	ULSS 5 – Polesana
Gruppo 1	ULSS 6 – Euganea
Gruppo 1	ULSS 7 – Pedemontana

Gruppo 1	ULSS 8 – Berica
Gruppo 1	ULSS 9 – Scaligera
Gruppo 1	Azienda Ospedaliera di Padova
Gruppo 1	Azienda Ospedaliera di Verona
Gruppo 1	Istituto Oncologico Veneto
Gruppo 2	Veneto Lavoro
Gruppo 2	Agenzia Veneta per i Pagamenti
Gruppo 2	Agenzia Regionale per la Prevenzione e Protezione Ambientale del Veneto
Gruppo 2	Consorzio Arsenàl.IT
Gruppo 3	Consiglio Regionale del Veneto
Gruppo 3	Veneto Strade Spa
Gruppo 3	Infrastrutture Venete
Gruppo 3	Veneto Innovazione
Gruppo 3	Istituto Zooprofilattico Sperimentale delle Venezie
Gruppo 4	Azienda Regionale per il Diritto allo Studio Universitario di Padova
Gruppo 4	Azienda Regionale per il Diritto allo Studio Universitario di Venezia
Gruppo 4	Azienda Regionale per il Diritto allo Studio Universitario di Verona
Gruppo 4	Veneto Agricoltura
Gruppo 4	Azienda Territoriale Edilizia Residenziale di Belluno

Gruppo 4	Azienda Territoriale Edilizia Residenziale di Padova
Gruppo 4	Azienda Territoriale Edilizia Residenziale di Rovigo
Gruppo 4	Azienda Territoriale Edilizia Residenziale di Treviso
Gruppo 4	Azienda Territoriale Edilizia Residenziale di Venezia
Gruppo 4	Azienda Territoriale Edilizia Residenziale di Verona
Gruppo 4	Azienda Territoriale Edilizia Residenziale di Vicenza
Gruppo 5	Parco Regionale del Fiume Sile
Gruppo 5	Parco Regionale dei Colli Euganei
Gruppo 5	Parco Regionale del Delta del Po
Gruppo 5	Istituto Regionale per le Ville Venete
Gruppo 5	Veneto Acque
Gruppo 5	Veneto Sviluppo
Gruppo 5	Veneto Edifici Monumentali

Servizi e attività del CERT-CSIRT

I servizi del CERT-CSIRT Regionale sono stati definiti e strutturati sulla base dei modelli di riferimento elaborati da **ENISA** (European Union Agency for Cybersecurity) con l'obiettivo di fornire agli Enti aderenti un insieme coerente e integrato di servizi di cybersecurity, in grado di supportare in modo organico il rafforzamento della postura di sicurezza.

Il modello dei servizi è articolato in **quattro ambiti principali**, tra loro complementari, che coprono l'intero ciclo della sicurezza:

1. **servizi di gestione della qualità della sicurezza**, orientati al governo del rischio, alla continuità operativa e alla diffusione della cultura della cybersecurity;
2. **servizi reattivi**, dedicati alla gestione degli incidenti di sicurezza e delle vulnerabilità;
3. **servizi di gestione degli artefatti**, focalizzati sullo sviluppo e sulla verifica della sicurezza di applicazioni;
4. **servizi proattivi**, finalizzati all'anticipazione delle minacce attraverso attività di Threat Intelligence.

Governance del CERT-CSIRT

Nel periodo considerato è stata progressivamente consolidata l'attività di **governance del CERT-CSIRT**, con l'obiettivo di assicurare un governo chiaro, stabile e coerente del servizio. Tale percorso ha riguardato la definizione dei ruoli e delle responsabilità, il rafforzamento del raccordo con i livelli direzionali e strategici e la strutturazione di processi di coordinamento continui con gli enti della constituency.

Il modello di governance si è sviluppato attraverso il coinvolgimento degli organismi di indirizzo e di confronto, consentendo di orientare le decisioni strategiche, monitorare l'evoluzione del progetto CERT-CSIRT e garantire l'allineamento con le priorità regionali e con il quadro normativo nazionale. In particolare, l'adeguamento progressivo alle Linee Guida dell'Agenzia per la Cybersicurezza Nazionale ha rappresentato un elemento qualificante, permettendo al CERT-CSIRT di operare entro un perimetro di riferimento condiviso e riconosciuto.

Nel complesso, l'attività di governance ha accompagnato la trasformazione del CERT-CSIRT da iniziativa progettuale a **servizio strutturato**, dotato di una visione di medio-lungo periodo e di una capacità di indirizzo stabile, creando le condizioni per un ulteriore rafforzamento delle funzioni e per una crescita coerente del sistema regionale di cybersecurity.

Servizio di Gestione del Rischio

CYBER MATURITY ASSESSMENT	
Voce	**Valore**
N. enti aderenti al servizio Gestione del Rischio	**39**
N. enti che hanno effettuato l'assessment nel 2025	**29**
N. controlli identificati	**12.876**
N. controlli soddisfatti	**6.899**
% controlli soddisfatti	**53,6**
N. report prodotti nel 2025	**29**
N. report previsti nel 2026	**39**

Il servizio di gestione del rischio è stato avviato nel biennio 2023–2024 con l'obiettivo di valutare la **postura di cybersicurezza degli Enti appartenenti alla Constituency**.

La gestione del rischio costituisce un **processo continuo e sistematico volto a individuare, valutare e trattare i rischi** che possono compromettere la sicurezza delle informazioni e dei servizi digitali degli Enti. In tale contesto, il modello di Cybersecurity Maturity Assessment adottato è finalizzato a fornire una visione organica e strutturata del livello di maturità delle organizzazioni in ambito di sicurezza informatica.

Attraverso l'analisi dei processi, delle misure organizzative e delle soluzioni tecnologiche in essere, **l'assessment consente di valutare il grado di preparazione degli Enti rispetto alle principali minacce cyber**. L'esecuzione del Maturity Assessment contribuisce ad accrescere la consapevolezza in merito a eventuali carenze, criticità e vulnerabilità, supportando l'individuazione delle azioni di miglioramento prioritarie. In tal modo, il servizio favorisce un rafforzamento

progressivo del livello di resilienza e della maturità complessiva in materia di cybersecurity, promuovendo un approccio strutturato e continuo alla gestione del rischio cyber.

A partire dal 2023, sono stati svolti diversi cicli del Cyber Maturity Assessment al fine di consentire il confronto nel tempo e l'analisi delle iniziative intraprese dagli Enti per il miglioramento della propria postura di cybersicurezza.

Il servizio si articola nelle seguenti fasi:

- **Fase 1** – Raccolta delle informazioni e set-up, comprensiva della definizione del perimetro di applicazione, della validazione della checklist dei controlli e della predisposizione del piano di dettaglio per l'esecuzione dell'Assessment.
- **Fase 2** – Assessment, che prevede la pianificazione degli incontri e lo svolgimento delle attività di valutazione.
- **Fase 3** – Analisi dei gap emersi dall'Assessment e definizione del relativo Piano di Rimedio.

  La Fase 3 riveste un ruolo centrale, in quanto consente di indirizzare in modo mirato le principali criticità emerse, supportando gli Enti nel percorso di miglioramento continuo in ambito di cybersecurity.

Si evidenzia che non tutti gli enti della constituency hanno partecipato ai cicli di Cyber Maturity Assessment sin dalla fase di avvio del servizio. In particolare, alcuni enti non hanno svolto il Maturity Assessment nel primo ciclo 2023–2024 (ATER Treviso, ATER Verona e Veneto Sviluppo) mentre ulteriori enti non hanno preso parte al secondo ciclo di valutazione condotto nel periodo 2025–2026 (ULSS2 Marca Trevigiana, ULSS8 Berica, Azienda Ospedaliera di Padova, Azienda Ospedaliera di Verona, ESU Venezia, ESU Verona, ATER Treviso, Parco Regionale del Fiume Sile. Veneto Acque). Per tali realtà è previsto lo svolgimento dell'assessment nel corso del **terzo ciclo del servizio, con avvio nel 2026**.

Servizio di Sensibilizzazione e Formazione

SENSIBILIZZAZIONE E FORMAZIONE	
Voce	**Valore**
N. enti che hanno aderito al servizio di Sensibilizzazione e Formazione	**39**
N. utenti attivi in piattaforma	**74.342**
% partecipazione alla Formazione (utenti in linea + regolari)	**44%**
N. campagne concordate	**372**
N. campagne completate	**286**
% campagne completate	**85%**
N. utenti previsti in piattaforma per il secondo percorso	**75.000**

Nel periodo di riferimento il servizio di **Formazione e Sensibilizzazione** ha registrato un'elevata intensità operativa, accompagnando progressivamente gli Enti della constituency nelle diverse fasi di attivazione, consolidamento ed evoluzione del percorso formativo.

Le attività hanno incluso il **supporto continuo agli Enti** per la raccolta delle informazioni propedeutiche all'avvio del servizio, l'aggiornamento e la gestione delle userlist, nonché il coordinamento delle modalità operative in funzione delle specificità organizzative e delle tempistiche condivise. A questo si è affiancato un **costante supporto** agli utenti e ai referenti degli Enti, tramite incontri di approfondimento e gestione delle richieste pervenute alla casella dedicata, al fine di garantire un utilizzo efficace della piattaforma.

Parallelamente, è proseguita l'implementazione e il monitoraggio delle campagne di phishing simulato, con attività di pianificazione, configurazione, avvio e analisi dei risultati, coinvolgendo un numero crescente di Enti. Tali attività sono state affiancate da incontri tecnici e da supporto specialistico per la corretta configurazione delle componenti infrastrutturali necessarie (SSO, whitelisting, strumenti di segnalazione).

Nel periodo di riferimento è in corso l'attivazione del secondo percorso formativo, che vede attualmente coinvolti **28 Enti,** e sono state condotte attività di supporto dedicate alla migrazione verso la nuova versione della piattaforma, al fine di garantire continuità del servizio e allineamento con l'evoluzione normativa. Le attività hanno incluso sessioni di demo, incontri di pianificazione personalizzata dei rilasci e la condivisione della documentazione aggiornata a supporto degli Enti.

Nel complesso, il servizio di Formazione e Sensibilizzazione evidenzia **uno stato di avanzamento significativo**, con un numero elevato di Enti attivi, un'ampia platea di utenti coinvolti e un percorso in continua evoluzione, caratterizzato da un accompagnamento strutturato e da un'attenta gestione delle diverse esigenze emerse nel contesto della constituency.

Di seguito il dettaglio dei moduli erogati

Primo percorso formativo

1. **Primo modulo - Phishing:**
   Fornisce strumenti per riconoscere e gestire attacchi di phishing, illustrando le tecniche più comuni utilizzate dai criminali informatici via e-mail, messaggistica e social media.
   La durata prevista del modulo è di 40 minuti, circa.

2. **Secondo modulo - Password:**
   Tratta le buone pratiche per la gestione sicura delle credenziali, evidenziando il ruolo centrale delle password nella protezione delle risorse digitali.
   La durata prevista del modulo è di 35 minuti, circa.

3. **Terzo modulo - Social Media:**
   Analizza i rischi legati all'uso dei social network, con focus sulla protezione della privacy e sulla prevenzione di comportamenti che possano compromettere la sicurezza personale e aziendale.
   La durata prevista del modulo è di 40 minuti, circa.

4. **Quarto modulo - Privacy & GDPR:**
   Introduce i principi fondamentali del Regolamento Europeo sulla protezione dei dati, promuovendo un approccio consapevole e conforme alla normativa da parte di tutti i membri dell'organizzazione.
   La durata prevista del modulo è di 40 minuti, circa.

5. **Quinto modulo - Mobile Device:**
   Offre indicazioni pratiche per l'uso sicuro di dispositivi mobili e applicazioni, con attenzione alla separazione tra sfera personale e professionale e alla protezione dei dati.
   La durata prevista del modulo è di 35 minuti, circa.

6. **Sesto modulo – Artificial Intelligence:**
   Fornisce strumenti per riconoscere contenuti falsi o distorti online, evidenziando i rischi di disinformazione e le implicazioni sulla sicurezza informatica.
   La durata prevista del modulo è di 35 minuti, circa.

7. **Settimo modulo - USB Device:**
   Analizza i rischi legati all'uso di dispositivi USB, in particolare quelli di memorizzazione, e promuove buone pratiche per proteggere i dati da sottrazioni o compromissioni.
   La durata prevista del modulo è di 35 minuti, circa.

8. **Ottavo modulo - E-mail Security:**
   Offre indicazioni per la gestione sicura della posta elettronica, con focus sulla protezione delle informazioni sensibili e sulla prevenzione di attacchi veicolati via e-mail.
   La durata prevista del modulo è di 33 minuti, circa.

9. **Nono modulo - Malware & Ransomware:**
   Spiega le principali tipologie di malware, con particolare attenzione al ransomware, e fornisce strategie per ridurre il rischio di infezione e limitare i danni in caso di attacco.
   La durata prevista del modulo è di 35 minuti, circa.

10. **Decimo modulo - Web Browsing:**
    Fornisce conoscenze pratiche per una navigazione sicura, illustrando i rischi associati all'uso dei browser e dei siti web e le misure di protezione da adottare.
    La durata prevista del modulo è di 35 minuti, circa.

11. **Undicesimo modulo – Deep Fake:**
    Esamina il fenomeno del deepfake, offrendo strumenti pratici per identificarlo e difendersi dalla disinformazione digitale.
    La durata prevista del modulo è di 40 minuti, circa.

12. **Dodicesimo modulo - Social Engineering:**
    Approfondisce le tecniche di ingegneria sociale utilizzate dai cyber criminali, evidenziando l'importanza della vigilanza e della protezione delle informazioni personali.
    La durata prevista del modulo è di 38 minuti, circa.

Secondo percorso formativo

1. **Primo modulo - Clean Desk:**
   Promuove buone pratiche per la protezione delle informazioni sensibili nella postazione di lavoro, con focus su privacy, sicurezza fisica e conformità al GDPR.
   La durata prevista del modulo è di 36 minuti, circa.

2. **Secondo modulo - Smart Working:**
   Analizza i rischi legati al lavoro da remoto e fornisce strategie per operare in sicurezza fuori dall'ambiente aziendale, proteggendo dati e sistemi.
   La durata prevista del modulo è di 40 minuti, circa.

3. **Terzo modulo - Social Collaboration & Video-Conferencing:**
   Esamina le minacce associate all'uso di strumenti di collaborazione e videoconferenza, evidenziando l'importanza di un utilizzo consapevole per tutelare privacy e sicurezza.
   La durata prevista del modulo è di 40 minuti, circa.

4. **Quarto modulo - Smishing & Vishing:**
   Approfondisce le tecniche di phishing via messaggistica e telefonate, sensibilizzando sull'uso prudente di canali considerati erroneamente sicuri.
   La durata prevista del modulo è di 36 minuti, circa.

5. **Quinto modulo - Spear Phishing:**
   Fornisce strumenti per riconoscere attacchi mirati di phishing, basati sulla raccolta di informazioni personali e professionali per ingannare specifici individui o gruppi.
   La durata prevista del modulo è di 38 minuti, circa.

6. **Sesto modulo - Ransomware:**
   Esamina la minaccia ransomware, illustrando le conseguenze degli attacchi e le misure preventive per ridurre il rischio e limitare i danni.
   La durata prevista del modulo è di 35 minuti, circa.

7. **Settimo modulo - Multi-Factor Authentication:**
   Promuove l'adozione di sistemi di autenticazione avanzati e analizza le tecniche con cui gli attaccanti cercano di aggirarli, come Sneaky Phishing e Sim Swap.
   La durata prevista del modulo è di 38 minuti, circa.

8. **Ottavo modulo - IoT Device:**
   Tratta i rischi legati ai dispositivi interconnessi, sia in ambito personale che professionale, e propone comportamenti sicuri per gestire l'Internet of Things.
   La durata prevista del modulo è di 40 minuti, circa.

9. **Nono modulo - Bluetooth & Wi-Fi:**
   Fornisce indicazioni per l'uso sicuro delle connessioni wireless, evidenziando i rischi associati alla mobilità e alla connettività continua.
   La durata prevista del modulo è di 35 minuti, circa.

10. **Decimo modulo - Information Classification:**
    Spiega l'importanza della classificazione delle informazioni per la protezione dei dati, con focus sulle Personal Identifiable Information e sulle pratiche organizzative.
    La durata prevista del modulo è di 38 minuti, circa.

11. **Undicesimo modulo - Data Protection:**
    Il modulo approfondisce il tema della protezione dei dati con particolare attenzione alla sicurezza, alla privacy e al rapporto con le normative di qualità e sicurezza delle informazioni, focalizzandosi sul GDPR. È concepito come un aggiornamento avanzato del modulo "Privacy & GDPR", inserito nel percorso di formazione obbligatoria, con contenuti più sofisticati rispetto al primo livello**.**
    La durata prevista del modulo è di 40 minuti, circa.

12. **Dodicesimo modulo - Social Engineering 2:**
    Questo modulo riprende il tema del social engineering, illustrando tecniche di attacco basate sull'inganno e sulla manipolazione psicologica. Attraverso esempi concreti, offre ulteriori elementi di consapevolezza sulle strategie utilizzate dai cybercriminali, fungendo da sintesi dei concetti trattati nei moduli del secondo livello.
    La durata prevista del modulo è di 40 minuti, circa.

Servizio di Security Operation Center

SOC - SECURITY OPERATION CENTER	
Voce	**Valore**
N. enti che hanno aderito al servizio di Incident Detection	**36**
Media EPS Allocati 11 mesi	**85.200**
N. ticket/giorno	**1,9**
Volume di log TB/mese	**~ 190 TB/mese**

Il servizio di **SOC Monitoring** è stato avviato in un contesto complesso e ha inizialmente evidenziato alcune difficoltà nella fase di attivazione, portando quindi a prioritizzare i sistemi più rilevanti come i sistemi di protezione della rete e degli accessi a Internet, delle postazioni di lavoro, dei server di dominio, delle connessioni da remoto e della navigazione web (Firewall Internet/DMZ, Endpoint Protection, Network IDS/IPS, Windows Domain Server, Network VPN e Secure Web Proxy) mentre i sistemi a bassa priorità non sono ancora completamente coperti. Tali sistemi comprendono quelli

dedicati alla gestione degli accessi privilegiati, alla sicurezza della posta elettronica e delle applicazioni web, nonché ulteriori sistemi di protezione, server e infrastrutture di virtualizzazione (PAM, E-mail Security Gateway, Reverse Proxy/WAF, Citrix NetScaler, Cynet/XDR, Windows Server, server Unix/Linux e Hypervisor). Grazie a un lavoro progressivo di coordinamento e consolidamento, il servizio ha oggi raggiunto una piena operatività: 36 enti su 37 firmatari risultano attivi, pari a circa il 95% del totale, a conferma di una copertura ormai quasi completa del perimetro regionale.

Nelle prime fasi, il servizio produceva un numero elevato di segnalazioni, spesso caratterizzate da falsi positivi o ticket ripetitivi, con un impatto significativo sul carico operativo degli enti. Attraverso un'attività strutturata di affinamento del monitoraggio e di miglioramento continuo, si è lavorato per ridurre le segnalazioni ripetitive e prive di effettivo valore operativo.

La principale difficoltà nell'ottimizzazione del monitoraggio è stata rappresentata dalla disponibilità non sempre adeguata di feedback da parte degli enti, necessari per valutare la pertinenza delle segnalazioni e affinare le regole di rilevazione.

SysAid ad oggi rappresenta la piattaforma centrale del servizio, attraverso la quale **gli enti ricevono e gestiscono operativamente i ticket del SOC**, mentre la Regione, in qualità di soggetto di governance, ha visibilità delle segnalazioni degli enti e ne monitora l'andamento nel tempo. Questo consente sia una gestione operativa efficace da parte degli enti, sia un controllo strutturato della qualità del servizio da parte della Regione, permettendo di indirizzare azioni di miglioramento nei confronti dei fornitori e degli enti stessi.

Servizio di Cyber Threat Intelligence

CTI - CYBER THREAT INTELLIGENCE & MISP	
Voce	**Valore**
N. enti che hanno aderito al servizio di CTI	**33**
N. Segnalazioni Alte gestite	**1.004**
N. ticket/giorno	**1,3**
MISP Enti attivi	**2**
MISP Feed attivi	**5**

Il servizio di **Cyber Threat Intelligence (CTI)** è stato avviato in un contesto complesso e ha inizialmente evidenziato alcune difficoltà nella fase di attivazione.

Grazie a un percorso graduale, il servizio ha oggi raggiunto un'elevata operatività: 33 enti su 35 firmatari risultano attivi, pari a circa il 94% del totale, a conferma di una diffusione ormai ampiamente consolidata sul perimetro regionale.

SysAid ad oggi rappresenta la piattaforma centrale per il **servizio CTI**, attraverso la quale **gli enti ricevono e gestiscono le segnalazioni informative**, mentre la Regione, in qualità di soggetto di governance, ha visibilità complessiva dei ticket e ne monitora l'andamento nel tempo. Questo consente una gestione operativa efficace da parte degli enti e, al contempo, un controllo strutturato della qualità del servizio, permettendo di indirizzare azioni di miglioramento nei confronti dei fornitori e degli enti stessi.

Il servizio CTI è ora orientato al consolidamento e all'evoluzione. Sono in corso attività di miglioramento finalizzate ad aumentare ulteriormente il valore informativo delle segnalazioni. In questo quadro, la MISP Regionale, alimentata dai Feed Nazionali (CNAIPIC-Polizia Postale, CSIRT Nazionale di ACN, dalla stessa Constituency e i classici di Threat Intelligence (OSINT \ CLOSINT), rappresenta un elemento già operativo e in progressiva espansione. Oggi la MISP, grazie alla connessione diretta con la MISP di ACN a cui sono stati inviati i perimetri delle aziende sanitarie, è pronta ad una prima evoluzione per istruire i dispositivi degli enti. Oggi il test è stato effettuato su 2 enti (ULSS7 e AOVR). La piattaforma consente la condivisione strutturata di indicatori di compromissione (IoC) e l'integrazione automatica con i sistemi di difesa degli enti (es. FW). L'obiettivo è estendere progressivamente i perimetri monitorati da ACN con il gruppo 2 e forse il gruppo 3, portando di conseguenza l'adozione a questi, aumentando il livello di protezione condivisa e riducendo i tempi di reazione alle minacce.

Servizio di Vulnerability Management

Il servizio di Vulnerability Management si compone di due anime, **Vulnerability Assessment e Penetration Testing**, che sono due tipologie di test di sicurezza complementari e distinte. Inoltre,

dal momento che il CERT-CSIRT si è dotato di due fornitori distinti, uno per tipologia di test, è ragionevole considerarli due servizi altrettanto distinti.

Vulnerability Assessment

VULNERABILITY ASSESSMENT	
Voce	**Valore**
N. enti che aderito al servizio	**34**
N. IP verificati	**6.000**
N. report prodotti (media/massimo)*	**22/34**

*per "media" si intende il numero medio di report prodotto fino a Luglio '26 - per "massimo" si intende il numero di report previsti da contratto

Il servizio di Vulnerability Assessment prevede l'**esecuzione di test di sicurezza automatizzati** che hanno come obiettivo l'individuazione di vulnerabilità su target infrastrutturali e di middleware (es. sistemi operativi) sia sul perimetro interno che pubblico di ogni Ente aderente.

A seguito dell'onboarding attraverso le attività propedeutiche di firma dei documenti di manleva e setup infrastrutturale per rendere raggiungibile la rete dell'Ente su cui sono situati gli asset target, l'erogazione del servizio prevede l'esecuzione di fino a 4 scansioni, a seconda della disponibilità dell'Ente a livello di logistica e pianificazione, al termine di ciascuna delle quali viene condivisa una reportistica utile all'Ente per indirizzare le remediation alle vulnerabilità rilevate.

Penetration Testing

PENETRATION TESTING	
Voce	**Valore**
N. enti che hanno aderito al servizio	**37**
N. report prodotti (media/massimo)*	**23/37**
N.applicativi testati (media/massimo)*	**59/88**

*per "media" si intende il numero medio di report prodotto fino a Luglio '26 - per "massimo" si intende il numero di report previsti da contratto

Il servizio di *Penetration Testing* prevede l'**esecuzione di *test* di sicurezza manuali e puntuali** che hanno come obiettivo l'individuazione di vulnerabilità e misconfigurazioni su *target* applicativi di ogni Ente aderente.

A seguito dell'*onboarding* attraverso la firma dei documenti di manleva, l'erogazione del servizio prevede l'esecuzione di fino a 2 *test*, a seconda della disponibilità dell'Ente a livello di logistica e

pianificazione, al termine di ciascuna delle quali viene condivisa una reportistica utile all'Ente per indirizzare le *remediation* alle vulnerabilità rilevate.

Servizio di SAST e DAST

SAST E DAST	
Voce	**Valore**
N. enti che aderiscono al servizio Secure Code	**17**
N. report prodotti per DAST	**9**
N. report prodotti per SAST	**4**

Nel periodo considerato sono proseguite le attività relative ai **servizi SAST e DAST**, che risultano in progressivo avanzamento secondo le diverse fasi previste. In particolare, la maggior parte degli enti coinvolti ha completato le attività preliminari, con la formalizzazione della documentazione necessaria e la progressiva definizione dei perimetri applicativi.

Parallelamente, per una parte degli enti sono state avviate le attività operative di test, mentre le ulteriori posizioni sono attualmente in fase di completamento delle attività propedeutiche. L'andamento complessivo del servizio evidenzia una crescita graduale e coerente con la pianificazione, tenendo conto delle specificità organizzative dei singoli enti e delle tempistiche di coordinamento necessarie per l'attivazione delle attività.

Servizio di Business Continuity Management & Disaster Recovery

BUSINESS IMPACT ANALYSIS	
Voce	**Valore**
N. BIA svolte	**34**
N. processi analizzati	**36**
N. processi soprasoglia per RTO	**20**
N. processi soprasoglia per RPO	**17**

Il servizio di **Gestione della Continuità Operativa** è stato avviato nel 2025 con l'obiettivo di fornire supporto metodologico e linee guida agli Enti della Constituency. Il **ruolo del CERT-CSIRT è quello di guidare e facilitare le fasi di definizione**, inizializzazione e strutturazione delle attività, mettendo a disposizione competenze specialistiche, mentre la pianificazione, l'attuazione e il mantenimento dei piani di continuità restano in capo ai singoli Enti.

La continuità operativa rappresenta la capacità di un'organizzazione di mantenere o ripristinare le proprie funzioni e i servizi critici entro tempi accettabili, anche in presenza di eventi imprevisti o situazioni di crisi. In ambito di cybersecurity, tale capacità si traduce nella tutela della disponibilità dei servizi essenziali a fronte di attacchi informatici o incidenti, attraverso l'adozione di misure preventive, piani di risposta e strategie di ripristino adeguate.

Un'attività centrale del processo di Continuità Operativa è l'**analisi preliminare dei servizi e dei processi critici dell'organizzazione**, realizzata tramite la **Business Impact Analysis (BIA).** Il servizio di BIA è finalizzato a valutare gli impatti che eventuali interruzioni dei servizi e dei processi operativi possono generare sull'organizzazione nel tempo, consentendo l'individuazione delle priorità di protezione e ripristino.

Attraverso una raccolta strutturata delle informazioni e l'analisi delle interdipendenze organizzative e tecnologiche, la BIA consente di stimare la capacità degli Enti di tollerare periodi di indisponibilità e di definire le azioni di intervento più rilevanti. Il servizio include inoltre la mappatura dei servizi, dei processi critici e degli asset a essi correlati, nonché la definizione degli obiettivi di continuità e ripristino (RTO, RPO e MTPD). Le risultanze della BIA costituiscono la base informativa per la pianificazione delle strategie di continuità operativa e di disaster recovery, orientando le decisioni verso le aree a maggiore impatto potenziale.

Il servizio ha previsto una prima fase nel corso del 2025 e una seconda fase, con avvio a partire da maggio 2026, che ha consentito il confronto tra i due cicli e la valutazione dell'evoluzione del livello di maturità degli Enti in materia di continuità operativa.

Servizio di Reperibilità

REPERIBILITA'

Voce	Valore
Copertura	**H24/365**
Tempo di massimo di risposta	**30 minuti**
Uso del servizio	**0**

Nel corso del periodo di riferimento è stato strutturato e attivato il servizio di **reperibilità del CERT-CSIRT**, nato dall'esigenza di garantire un supporto tempestivo alla constituency in caso di incidenti critici. Il servizio si configura come un presidio operativo dedicato, finalizzato a rafforzare la capacità di risposta degli enti nelle fasi più delicate della gestione di un evento di sicurezza, assicurando un punto di contatto qualificato anche al di fuori delle finestre operative ordinarie.

Il servizio di reperibilità si articola su tre principali componenti. In primo luogo, **la reperibilità H24**, che consente l'intervento del team di *CSIRT Crisis Support* tramite un numero di telefono dedicato in caso di incidenti rilevanti. A questa si affiancano le attività di **analisi dei malware** identificati, volte a supportare gli enti nella comprensione della minaccia e nella valutazione degli impatti potenziali. Infine, il servizio contribuisce al **miglioramento delle risposte del SOC**, attraverso l'analisi e l'affinamento delle segnalazioni provenienti dai sistemi di monitoraggio, favorendo una gestione più efficace e coordinata degli eventi.

Il servizio viene attivato in presenza di incidenti critici che coinvolgono gli enti della constituency e si inserisce in un modello di supporto che mantiene gli enti pienamente autonomi nella gestione dell'incidente, offrendo al contempo un accompagnamento tecnico qualificato. A supporto delle comunicazioni operative, è stata inoltre predisposto un canale di messaggistica istantanea dedicato a consentire scambi informativi diretti e rapidi, anche in modalità unidirezionale, nei momenti di maggiore criticità.

Nel complesso, il servizio di reperibilità rappresenta un elemento chiave nel rafforzamento delle capacità di risposta del CERT-CSIRT e costituisce un primo passo concreto verso un modello di gestione degli incidenti sempre più coerente con gli standard e le aspettative del ruolo CSIRT a livello regionale e nazionale.

Attività di Comunicazione e Formazione

COMUNICAZIONE

Nel 2025 sono state introdotte due importanti novità a beneficio della *Constituency*, rappresentate dalla produzione strutturata di **bollettini e *newsletter***. La gestione di tali comunicazioni è affidata al *Team Governance*, che, attraverso una *mailing list* dedicata, condivide con frequenza bimestrale aggiornamenti relativi a specifiche tematiche di sicurezza con i Referenti di Sicurezza degli Enti.

All'interno della ***newsletter*** viene fornita una panoramica delle attività del CERT-CSIRT, comprensiva dei prossimi eventi in programma, delle principali novità e scadenze, nonché di approfondimenti sugli ultimi *trend* e sulle principali ricerche di settore, e di aggiornamenti normativi di interesse per la *Constituency*.

Il **bollettino**, invece, ha un taglio maggiormente operativo e informativo e ciascuna edizione include le seguenti sezioni:

- *Threat Intelligence Scorecard*, che fornisce una panoramica sulle principali minacce e vulnerabilità, con particolare attenzione ai *trend* emergenti e alle attività malevole osservate;
- *Threat Advisory*, dedicata ad approfondimenti su minacce emergenti, accompagnati da indicazioni operative finalizzate alla prevenzione di rischi specifici;
- *Vulnerability Advisory*, che presenta *report* sulle vulnerabilità critiche riscontrate per i fornitori più rilevanti, includendo *link* di approfondimento e riferimenti utili per supportare le attività di analisi e mitigazione.

Nel medesimo contesto è stato inoltre predisposto un **Piano di comunicazione**, che ad oggi non risulta ancora pubblicato, il quale fornisce una guida pratica per la gestione dei flussi di comunicazione tra il CERT-CSIRT Regionale e gli attori, interni ed esterni, che interagiscono con esso. Il documento è finalizzato a garantire una comunicazione efficace sia in scenari di emergenza (incidenti o *crisi cyber*) sia nello svolgimento delle attività ordinarie di competenza del CERT-CSIRT.

Tale piano è stato oggetto di una significativa revisione con relativo aggiornamento all'inizio del 2026, a seguito dell'attivazione del servizio di reperibilità del CERT-CSIRT, al fine di adeguare i processi comunicativi alle nuove esigenze operative e di risposta.

Ove ritenuto opportuno, sono inoltre previste **comunicazioni di rinforzo**, finalizzate a rafforzare l'attenzione su tematiche di particolare rilevanza. Questa tipologia di comunicazioni comprende, in particolare, le *e-mail* indirizzate ai Referenti di Sicurezza in merito all'identificazione di *Early Warning* con gravità *High* e *Critical*, con l'obiettivo di portare all'attenzione della *Constituency* le azioni suggerite dal CERT-CSIRT Regionale, volte a verificare se i prodotti o sistemi potenzialmente impattati da vulnerabilità siano stati oggetto di opportune verifiche e, ove necessario, dell'applicazione delle misure di contenimento (ad esempio aggiornamenti o mitigazioni).

Successivamente, l'ambito delle comunicazioni è stato ampliato includendo ulteriori aree di interesse, quali:

- la *compliance* normativa, con riferimento a scadenze e obblighi previsti dalle normative vigenti o dai relativi aggiornamenti, al fine di evidenziare l'importanza dell'adeguamento nei tempi definiti;
- gli approfondimenti sui servizi erogati, incluse modalità e tempistiche di ingaggio dei fornitori, canali disponibili e documentazione di supporto;
- ulteriori indicazioni operative relative a tematiche di interesse per la Constituency (es. attivazione di nuovi servizi, rischi legati a minacce *cyber* connesse al contesto geopolitico, ecc.).

Alla fine del 2024 era stata avviato un tavolo di lavoro finalizzato alla pubblicazione del **sito del CERT-CSIRT**, che è stato successivamente portato in produzione all'inizio dell'anno successivo. Il sito rappresenta il canale istituzionale attraverso il quale vengono veicolate le principali informazioni relative al CERT-CSIRT.

In una fase iniziale, il sito era strutturato in quattro sezioni principali, attraverso le quali venivano veicolate le informazioni essenziali relative al CERT-CSIRT, quali la missione, i servizi, i contatti e i *link* utili.

Contestualmente, si è proceduto all'**aggiornamento continuo e al caricamento dei contenuti della sezione *news***, contribuendo alla diffusione tempestiva delle principali comunicazioni, iniziative e aggiornamenti rilevanti del CERT-CSIRT.

In un momento successivo, il sito è stato ulteriormente sviluppato con l'introduzione della sezione dedicata agli *alert*, rafforzando il ruolo del portale come canale informativo e di allerta a supporto della *Constituency*.

Nel 2026 è stato inoltre richiesto **supporto nella gestione dei contenuti della *Community Cyber Security***. Tale attività risulta attualmente sospesa, in quanto il portale della *Community* è stato interessato da un processo di migrazione, che ha comportato tempistiche prolungate di assestamento della piattaforma.

In attesa della risoluzione delle criticità attualmente presenti, sono in corso attività di coordinamento e gestione delle comunicazioni con il *team* responsabile della gestione dei portali, in preparazione alla futura ripresa delle attività.

Tutte **le iniziative descritte trovano continuità nel 2026**, con l'obiettivo di rafforzare ulteriormente il modello di comunicazione, il livello di consapevolezza della *Constituency* e l'efficacia complessiva delle attività del CERT-CSIRT.

FORMAZIONE

FORMAZIONE PER LA DIRIGENZA DEGLI ENTI NELLA CONSTITUENCY	
Voce	**Valore**
N. certificazioni ottenute per referenti della cybersicurezza	**13**
N. discenti formati per sanità	**44**
N. discenti formati per enti strumentali	**28**
N. discenti formati per percorso tecnici	**70**

FORMAZIONE PER LA DIRIGENZA DEGLI ENTI NELLA CONSTITUENCY	
Voce	**Valore**
N. certificazioni ottenibili per referenti della cybersicurezza	**18**
N. discenti da formare per sanità	**63**
N. discenti da formare per enti strumentali	**48**
N. medio discenti coinvolti per percorso tecnici	**70**

Il ciclo di eventi formativi promossi dal CERT-CSIRT Regionale si è sviluppato a partire dal 2024 con l'attivazione di un percorso di specializzazione finalizzato al **conseguimento della Certificazione di Referente della *Cybersicurezza***.

Nel dettaglio, il programma si è articolato in:

- **2 moduli** formativi erogati da remoto, dedicati al contesto normativo, agli standard in materia di *cybersecurity* e al ruolo del CERT-CSIRT, nonché alla gestione del rischio *cyber*;
- **3 simulazioni** in presenza, focalizzate sulla gestione di scenari di crisi cyber, tra cui attacchi mediante terza parte, incidenti *ransomware* e data *breach*;
- **2 *workshop*** in presenza, dedicati alla cybersecurity in ambito sanitario e agli impatti organizzativi e operativi della Direttiva NIS 2;
- **2 percorsi** di Certificazione in presenza, comprendenti CSX *Fundamentals* (24 ore) e CCSK – *Certificate of Cloud Security Knowledge* (16 ore).

Il percorso si è concluso nel mese di maggio 2025 con lo svolgimento dell'esame di certificazione, che ha registrato un esito positivo per 13 partecipanti su 16, i quali hanno conseguito la certificazione **di Referente della Cybersicurezza**.

Alla luce dei risultati ottenuti, nel 2026 il percorso è stato riproposto mantenendo la medesima articolazione, a favore di una nuova classe composta da ulteriori 20 partecipanti, con l'obiettivo di garantire continuità e rafforzamento delle competenze in ambito *cybersecurity* all'interno della *Constituency*.

In linea generale, la classe sarà composta da un partecipante per ciascun Ente Sanitario. Fanno eccezione gli Enti che hanno recentemente individuato un nuovo referente CERT-CSIRT: in tali casi è prevista la partecipazione di due referenti, al fine di garantire un adeguato passaggio di competenze e la continuità operativa.

Al percorso si uniranno inoltre i partecipanti chiamati a completare le attività di recupero relative al percorso formativo 2024, per favorire un allineamento complessivo delle competenze all'interno della Constituency.

Il calendario delle attività formative prenderà avvio nel mese di maggio e proseguirà fino a ottobre. Durante questo periodo saranno erogati i diversi appuntamenti secondo la pianificazione condivisa, con l'obiettivo di accompagnare i partecipanti in un percorso strutturato e progressivo.

L'esame finale è previsto nel mese di dicembre e rappresenterà il momento di valutazione e sintesi dell'intero percorso formativo.

Nel corso del 2026 è stato inoltre avviato il **mantenimento della certificazione** conseguita dai referenti nel 2025, la cui validità avrà termine il 15 settembre 2026. Il mantenimento della certificazione prevede complessivamente la partecipazione a 16 ore di formazione in ambito cybersecurity.

A tal fine, il CERT-CSIRT si impegna ad erogare specifiche sessioni di formazione volte a consentire il raggiungimento del monte ore richiesto. Qualora non fosse stato possibile partecipare alle sessioni organizzate dal CERT-CSIRT, è prevista la possibilità di produrre idonea documentazione attestante la partecipazione ad altre attività formative, purché coerenti con l'ambito professionale e con le tematiche della cybersicurezza.

A tal proposito, il CERT-CSIRT ha fornito a ciascun referente certificato un riepilogo delle ore di formazione effettivamente fruite nel corso del 2025.

Un mese prima della data di scadenza del certificato (15/09/2026), l'Ente Certificatore provvederà a trasmettere una comunicazione finalizzata alla richiesta delle evidenze documentali necessarie ai fini del rinnovo della CERT-CSIRTificazione.

Nel 2025, le attività formative sono state ulteriormente ampliate con **l'avvio di iniziative dedicate alle Figure Apicali e Tecniche**, con l'obiettivo di rafforzare la postura di sicurezza della *Constituency* e approfondire argomentazioni rilevanti (obblighi e aggiornamenti normativi, gestione dei servizi, argomentazioni in materia di sicurezza informatica, tecnologie d'interesse, minacce e rischi).

Le sessioni formative rivolte alle **Figure Apicali degli Enti aderenti al CERT-CSIRT** sono state progettate per rafforzare la consapevolezza delle minacce cyber e per supportare il ruolo di responsabilità che tali figure svolgono nella gestione della sicurezza informatica delle proprie organizzazioni.

Per quanto riguarda gli Enti Sanitari, i partecipanti hanno incluso le figure di Direttore Generale, Direttore Amministrativo, Direttore Sanitario e Direttore dei Servizi Socio-Sanitari. Per gli Enti Strumentali, invece, è stato previsto il coinvolgimento delle figure di Direttore Generale e Direttore Amministrativo, ove presenti all'interno dell'Ente, nonché dei Direttori della Regione del Veneto individuati in qualità di Organo Direttivo ai sensi della DGR n. 841 del 29 luglio 2025.

Tra tutti gli Enti coinvolti, solo l'Ente Veneto Strade ha comunicato la propria rinuncia alla partecipazione alle attività formative, avendo già provveduto autonomamente alla formazione delle **Figure Apicali in ambito NIS2**.

Nel dettaglio, il programma si è articolato in:

- **2 *workshop*** in presenza, di cui uno dedicato agli Enti Sanitari, focalizzati sulle responsabilità dirette e indirette delle Figure Apicali e del loro impatto sulla *governance* e l'organizzazione aziendale;
- **2 simulazioni** in presenza, di cui una dedicata agli Enti Sanitari, realizzate mediante l'utilizzo della piattaforma "*ImmersiveLab*", e incentrate sulla gestione di un caso reale di attacco *cyber*. Le attività che hanno previsto il coinvolgimento attivo dei partecipanti nell'analisi delle cause e delle conseguenze dell'incidente, nell'identificazione delle responsabilità e nella definizione delle azioni da correttive e di mitigazione da intraprendere;
- **2 *webinar*** erogati da remoto, di cui uno dedicato agli Enti Sanitari, dedicati all'approfondimento sull'importanza di costruire un approccio capace di integrare non solo gli aspetti tecnologici, ma anche quelli umani, organizzativi, legali ed etici, per riflettere su come prepararsi alle trasformazioni future.

Le **Figure Tecniche**, allo stesso tempo, hanno preso parte a *webinar* e iniziative tematiche, affiancate da sessioni specifiche di approfondimento sui servizi del CERT-CSIRT.

In particolare, il programma si è articolato in:

- **5 *webinar* di approfondimento** sui principali temi *cyber* e sui servizi offerti e sui risultati delle analisi del CERT-CSIRT, di cui una sessione dedicata agli Enti Sanitari con il coinvolgimento del reparto di Ingegneria Clinica presente presso l'Ente. Nello specifico, si illustrano i temi affrontati:

- NIS 2 (D.Lgs.138) e Legge 90/2024;
- I principali attacchi alla Pubblica Amministrazione;
- La *digital security* in Sanità: Dalla *Compliance* NIS 2 alla Gestione Innovativa della Supply Chain;
- Un SOC efficace: processi operativi e benefici per una miglior difesa;
- *Cyber Threat Intelligence*: servizio e caso d'uso.

- **2 iniziative verticali** di approfondimento sull'evoluzione del contesto normativo e tecnologico. Nello specifico, si illustrano i temi affrontati:
  - Governare l'innovazione: Impatto dell'AI nella trasformazione digitale;
  - Governare la complessità normativa: Proposta per un approccio integrato.

A seguito del completamento dei percorsi formativi, rivolti sia alle Figure Apicali sia alle Figure Tecniche, il CERT-CSIRT ha provveduto a predisporre e trasmettere gli attestati di partecipazione con gli Uffici di Formazione di ciascun Ente. Gli attestati, riferiti ai singoli appuntamenti formativi, sono stati successivamente condivisi dall'ufficio competente, a conferma dell'effettiva partecipazione.

Anche per l'anno 2026, i **percorsi formativi dedicati alle Figure Apicali e alle Figure Tecniche sono riproposti mantenendo la medesima impostazione**, con l'aggiunta di due eventi promossi dal CERT-CSIRT, di cui uno realizzato in collaborazione con altri CERT-CSIRT regionali, rafforzando così il confronto e la condivisione di esperienze a livello interregionale.

A partire dall'anno in corso, al termine di ciascuna sessione formativa dedicata alle Figure tecniche è previsto il completamento di un test di gradimento, volto a raccogliere il *feedback* sulla qualità della sessione, e lo svolgimento di un *test* di valutazione, finalizzato a verificare l'apprendimento dei contenuti trattati durante le attività erogate, da svolgersi sulla piattaforma *E-Learning* "*VEle*" della Regione del Veneto.

Ad oggi, risultano già erogate le seguenti sessioni:

- *Iniziativa Obblighi NIS 2:* Prossime scadenze e indicazioni operative: iniziativa dedicata agli Enti della Constituency rientranti nell'ambito della Direttiva NIS 2;
- Webinar Resilienza Operativa in Sanità: rischio cibernetico e telemedicina: webinar dedicato ai referenti tecnici degli Enti Sanitari e al reparto di Ingegneria Clinica;
- Webinar Il Valore del *Cloud*: controlli, governance e casi d'uso;
- Webinar La sicurezza del dato: classificazione, protezione e minacce emergenti;
- Webinar Dalla crittografia tradizionale al *Post-Quantum*: rischi, impatti e strategie;
- Webinar Anthropic Mythos: impatti sui programmi di cybersecurity.

Attivazione del MISP Regionale

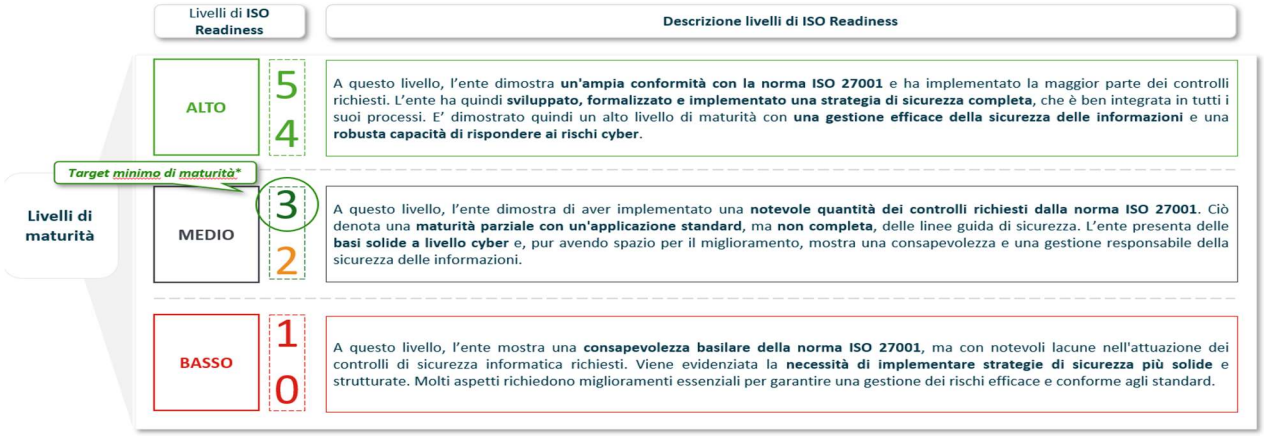
La **piattaforma MISP Regionale**, realizzata dal CERT-CSIRT regionale, rappresenta uno strumento centrale per il rafforzamento della collaborazione in materia di sicurezza all'interno della Constituency, consentendo una condivisione sicura e strutturata delle informazioni sulle minacce informatiche. Ad oggi sono stati raggiunti gli obiettivi operativi definiti, attraverso **l'integrazione nella piattaforma dei flussi informativi provenienti dall'Agenzia per la Cybersicurezza Nazionale e dalla Polizia Postale (CNAIPIC**), inclusi gli indicatori trasmessi tramite comunicazioni ufficiali. Tali indicatori vengono centralizzati e normalizzati all'interno di MISP e possono essere integrati nei sistemi di sicurezza, consentendo integrazioni automatizzate con i sistemi di difesa degli Enti, permettendo l'attivazione diretta di contromisure, ad esempio il blocco e sblocco automatico degli indirizzi IP.

Questo approccio abilita tempi di reazione più rapidi, favorisce la diffusione tempestiva di informazioni utili alla Constituency e determina una significativa riduzione del carico operativo sugli Enti, semplificando la gestione degli alert e migliorando l'efficacia complessiva della risposta alle minacce informatiche.

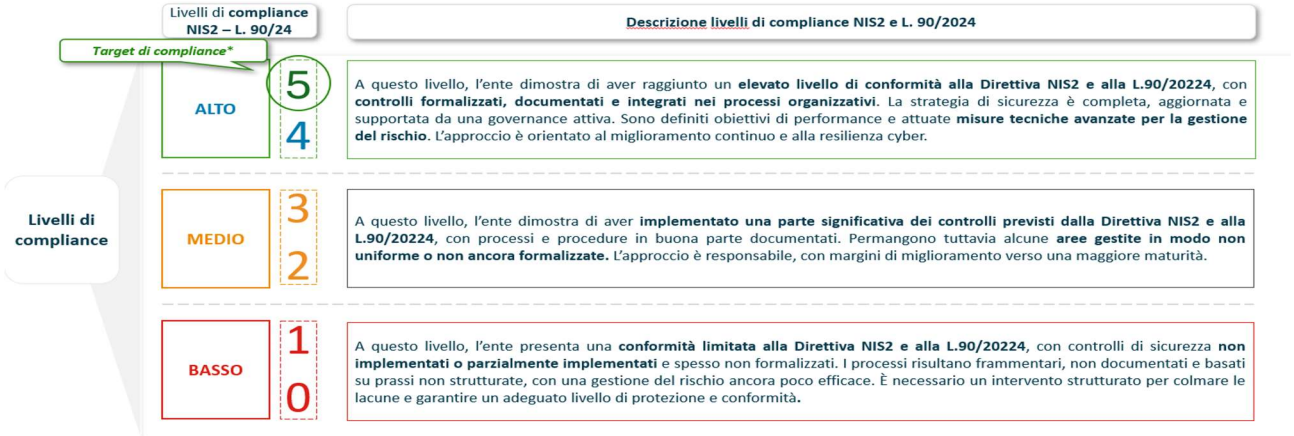
Approccio per il calcolo dei livelli di Maturità, ISO Readiness e Compliance

Nel definire le soglie di maturità da attribuire, è stato tenuto conto dei sei livelli già stabiliti dal **Framework Nazionale per la Cybersecurity e la Data Protection dell'Agenzia per la Cybersicurezza Nazionale (ACN)**, ricondotti a tre livelli di maturità aggregati (Alto, Medio, Basso). Questo calcolo rappresenta la valutazione complessiva su tutti i controlli della checklist diagnostica RV.

Nel definire i livelli di ISO Readiness, è stato stabilito un approccio metodologico in linea con lo **standard ISO 27001** e con i livelli di maturità complessiva definiti dalla checklist RVE, **ricondotti a tre livelli di maturità aggregate** (Alto, Medio, Basso). La ISO Readiness è quindi calcolata considerando il **sottoinsieme** di controlli della **checklist diagnostica RV** che rientrano nello standard **ISO 27001.**



Nel definire i livelli di compliance normativa, è stata effettuata un'analisi di un **sottoinsieme di controlli** diagnostici mappati sulla **Direttiva 2555/2022 (NIS2), decreto di recepimento (D.lgs. n. 138/2024) e relative determine nonché la L. 90/2024**. I risultati sono aggregati in tre livelli di compliance (Alto, Medio e Basso). Per soddisfare gli obblighi normativi è richiesto il raggiungimento del **livello 5** di maturità, corrispondente all'**adempimento** di tutti i requisiti previsti.



Evoluzione del CERT-CSIRT nel tempo

Il **12 marzo 2026** si è riunito il **Comitato Strategico Straordinario**, che ha deliberato e approvato formalmente il **cambio di denominazione del CERT in CSIRT**, riconoscendo il percorso di maturazione organizzativa e operativa raggiunto dal servizio e sancendo il passaggio a un modello pienamente coerente con gli standard nazionali di riferimento.

L'evoluzione del CERT regionale verso il modello CSIRT rappresenta il naturale consolidamento di un percorso progettuale e organizzativo avviato negli anni precedenti, volto a rafforzare le capacità del sistema regionale di prevenire e allertare in maniera più efficace gli enti riguardo agli incidenti di sicurezza informatica che li coinvolgono.

Nel corso del tempo, il CERT ha progressivamente ampliato il proprio perimetro di azione, passando da una logica prevalentemente orientata al supporto e al coordinamento a un modello allineato alle Linee Guida emanate dall'Agenzia per la *Cybersicurezza* Nazionale (ACN) per la realizzazione dei CSIRT. Tale evoluzione ha comportato la definizione di un assetto organizzativo e di governo formalizzato, l'adozione di processi strutturati per la gestione degli incidenti, l'attivazione di canali di comunicazione sicuri e dedicati e il rafforzamento delle capacità di coordinamento.

Un passaggio fondamentale di questo percorso è rappresentato dall'ammissione a finanziamento della proposta progettuale "**Attivazione CERT Regionale" nell'ambito dell'Avviso 06/2023**, che ha consentito di rafforzare ulteriormente il modello operativo e di allinearlo agli standard nazionali. Il successivo aggiornamento del progetto esecutivo, culminato con l'approvazione della versione 2.1 nel gennaio 2025, ha consolidato funzioni, processi e responsabilità del servizio.

In tale contesto, **l'ACN ha attestato la piena operatività del CSIRT regionale**, riconoscendo un livello di maturità **SIM3 "basic**", in coerenza con le Linee Guida CSIRT versione 2.0. Questo riconoscimento certifica la capacità del CSIRT di operare come punto di riferimento unico per la gestione degli incidenti cyber, di cooperare in modo strutturato con il livello nazionale e di garantire un supporto coordinato e tempestivo agli enti della propria constituency, inclusa l'attivazione della reperibilità in caso di crisi.

Il passaggio da CERT a CSIRT non rappresenta quindi un mero cambio di denominazione, ma l'esito di un percorso di crescita progressiva e consapevole, che ha portato il servizio a configurarsi come

struttura organizzativa matura e riconosciuta, in grado di contribuire in modo concreto al rafforzamento della resilienza cyber del sistema pubblico regionale e alla tutela della continuità dei servizi essenziali.

Criticità affrontate e lezioni apprese

Nel corso dei primi anni di operatività del CERT-CSIRT, il percorso di crescita e consolidamento del servizio si è sviluppato in un contesto caratterizzato da una forte eterogeneità degli enti coinvolti, sia in termini di dimensioni sia di maturità organizzativa e tecnologica. L'erogazione dei servizi di cybersecurity, così come l'attuazione delle azioni di miglioramento emerse dalle attività di assessment e di supporto, ha quindi evidenziato alcune criticità strutturali e operative, che hanno richiesto un progressivo adattamento dell'approccio del CERT-CSIRT.

L'esperienza maturata ha tuttavia consentito di trarre importanti lezioni apprese, utili a orientare l'evoluzione del servizio, rafforzare il modello di supporto agli enti e definire priorità più aderenti alle effettive capacità operative del sistema regionale.

1. **Limitata capacità organizzativa e operativa di molti enti**, in particolare di quelli di dimensioni più ridotte, dovuta alla **carenza di personale dedicato**. In diversi casi poche risorse sono chiamate a coprire contemporaneamente ambiti diversi (ICT, sicurezza, amministrazione), rendendo complesso garantire continuità e maturità nell'erogazione dei servizi di cybersecurity.

2. **Richieste di adattamento dei servizi alle specifiche peculiarità dei singoli enti**, che hanno introdotto elementi di complessità non inizialmente previsti nel modello di erogazione del CERT-CSIRT. Tali richieste, pur rispondendo a esigenze concrete e legate all'eterogeneità della constituency, hanno comportato un maggiore impegno organizzativo e operativo, incidendo sulla pianificazione delle attività. Le modifiche e personalizzazioni richieste non risultavano originariamente incluse nella progettazione del servizio né coperte dal budget iniziale, evidenziando la necessità di un maggiore equilibrio tra standardizzazione dei servizi e adattabilità ai contesti specifici, al fine di garantirne la sostenibilità nel medio-lungo periodo.

3. L'esperienza maturata nel corso dell'operatività del CERT-CSIRT ha evidenziato come, oltre agli impegni contrattuali inizialmente previsti, fosse emersa in modo crescente da parte degli enti **la necessità di disporre di un servizio di supporto continuativo**, in grado di garantire un punto di riferimento anche al di fuori delle finestre operative ordinarie. Tale esigenza si è manifestata in particolare in relazione alla gestione di crisi per le quali,

tempestività e supporto qualificato risultano elementi determinanti. In questo contesto, è stato finalizzato il servizio di reperibilità tecnica "hands on", concepito per fornire supporto H24 in caso di incidente, mantenendo al contempo gli enti pienamente autonomi nella gestione e nella responsabilità dell'evento. Questa soluzione rappresenta una prima risposta strutturata alle esigenze emerse e si colloca in piena coerenza con il modello CSIRT, rafforzando il ruolo del servizio come punto di riferimento operativo e di coordinamento. Inoltre, l'attivazione della reperibilità tecnica costituisce un primo passo concreto verso azioni di miglioramento coerenti con il livello di maturità SIM3 riconosciuto dall'Agenzia per la Cybersicurezza Nazionale, ponendo le basi per un ulteriore rafforzamento delle capacità di risposta e resilienza del sistema regionale nel medio-lungo periodo.

Annex A – Indicatori, Strumenti e Tecnologie del CERT

I seguenti indicatori sono aggiornati a luglio 2026.

STATISTICHE DEL CERT	
Voce	**Valore**
SENSIBILIZZAZIONE E FORMAZIONE	
N. enti che hanno aderito al servizio di Sensibilizzazione e Formazione	**39**
N. utenti attivi in piattaforma nel primo percorso	**74.342**
N. enti attivi in piattaforma nel primo percorso	**39**
% partecipazione alla Formazione (utenti in linea + regolari)	**44%**
N. utenti previsti in piattaforma per il secondo percorso	**75.000**
SOC - SECURITY OPERATION CENTER	
N. enti che hanno aderito al servizio di Incident Detection	**35**
Media EPS Allocati 11 mesi	**85.200**
N. ticket/giorno	**1,9**
Volume di log TB/mese	**~ 8TB/mese**
CTI - CYBER THREAT INTELLIGENCE & MISP	
N. enti che hanno aderito al servizio di CTI	**33**
N. Segnalazioni Alte gestite	**1004**
N. ticket/giorno	**1,3**
MISP Enti attivi	**2**
MISP Feed attivi	**5**
PENETRATION TEST	
N. enti che hanno aderito al servizio di Penetration Test	**37**
N. report prodotti (media/massimo)	**24/37**
N. applicativi testati all'anno (media/massimo)	**59/94**
VULNERABILITY ASSESSMENT	
N. enti che hanno aderito al servizio di Vulnerability Assessment	**34**
N. IP verificati	**6000**
N. report prodotti	**22/34**
SAST E DAST	
N. enti che aderiscono al servizio Secure Code	**17**
N. report prodotti per DAST	**9**
N. report prodotti per SAST	**4**

REGIONE DEL VENETO

CYBER MATURITY ASSESSMENT	
N. enti aderenti al servizio Gestione del Rischio	**39**
N. enti che hanno effettuato l'assessment nel 2025	**29**
BUSINESS IMPACT ANALYSIS	
N. processi analizzati per la BIA/anno	**36**
FORMAZIONE PER LA DIRIGENZA DEGLI ENTI NELLA CONSTITUENCY	
N. discenti formati per enti sanitari nel 2025	**44**
N. discenti formati per altri enti nel 2025	**28**
N. discenti da formare per enti sanitari nel 2026	**63**
N. discenti da formare per altri enti nel 2026	**48**
N. medio discenti tecnici coinvolti per percorso specializzato 2025 e 2026	**70**
REPERIBILITA'	
Copertura	**H24/365**
Tempo di massimo di risposta	**30 minuti**
DOCUMENTAZIONE DEL CERT	
N. Linee Guida/Prontuari previsti ad anno	**4**
Procedura sulla Gestione della Crisi	**1**
Piano di Gestione degli Incidenti	**1**