Bur n. 122 del 11/10/2022

(Codice interno: 486250)

DELIBERAZIONE DELLA GIUNTA REGIONALE n. 1174 del 27 settembre 2022

CERT (Computer Emergency Response Team) Regionale. Approvazione del relativo progetto. Autorizzazione partecipazione all'avviso pubblico di cui alla Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5. *[Informatica]*

Note per la trasparenza:
Il provvedimento approva il progetto del CERT (Computer Emergency Response Team) Regionale e autorizza la Direzione ICT e Agenda Digitale a partecipare al Bando approvato dall'Agenzia per la Cybersicurezza Nazionale nell'ambito del Piano Nazionale di Ripresa e Resilienza (P.N.R.R.), Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5.

L'Assessore Francesco Calzavara, di concerto con l'Assessore Manuela Lanzarin, riferisce quanto segue.

Negli ultimi venti anni, la diffusione delle nuove tecnologie dell'informazione e delle comunicazioni ha progressivamente focalizzato il centro delle attività umane di carattere sociale, politico ed economico all'interno di una nuova dimensione, denominata cibernetica. Lo straordinario aumento dell'utilizzo di internet ha contribuito allo sviluppo del settore ICT, con un notevole impatto su tutte le funzioni della società moderna. Lo spazio cibernetico ha permesso immense opportunità di sviluppo economico, grazie alle quali le economie dei paesi più avanzati hanno subito una forte accelerazione. Tuttavia, l'incremento delle opportunità è stato accompagnato da un parallelo incremento delle vulnerabilità. Infatti, la digitalizzazione dei servizi e delle informazioni ha inevitabilmente accresciuto l'esposizione al rischio: il pericolo di furto, manomissione e compromissione dei dati nello spazio cibernetico ha evidenziato la necessità di mettere in sicurezza le attività in esso condotte. Il crimine informatico costituisce la piaga maggiore della sicurezza delle reti e delle informazioni, a livello di portata e di danni economici. Il costo del cybercrime è in continua crescita, provocando un ingente trasferimento di risorse al di fuori delle economie nazionali. Inoltre, strutture pubbliche che gestiscono quotidianamente dati ed informazioni digitali riguardanti cittadini si trovano a doverne garantire non solo la disponibilità e l'integrità, ma anche la riservatezza.

Nel febbraio 2013 l'Unione europea ha adottato la propria strategia di cybersicurezza, invitando tutti gli Stati membri a fare altrettanto.

Il Decreto del Presidente del Consiglio dei Ministri (DPCM) del 24 gennaio 2013, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica, ha quindi definito l'architettura istituzionale deputata alla sicurezza nazionale relativamente alle infrastrutture critiche informatizzate. A dicembre 2013, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico ed il relativo Piano nazionale per la protezione cibernetica e la sicurezza informatica hanno stabilito gli indirizzi strategici e quelli operativi per la messa in sicurezza delle attività condotte nel cyber spazio.

Il CERT-PA, in forza del suo mandato istituzionale ed in particolare degli articoli 14bis e 51 del D. Lgs 5 marzo 2005 n. 82 (CAD) ha operato all'interno di AGID dal mese di marzo 2014 fino al 6 maggio 2020 con il compito di supportare le Pubbliche Amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica,

A partire dal 6 maggio 2020, recependo il DPCM 8 agosto 2019, "Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team - CSIRT italiano, il CERT - PA ha terminato tutti i servizi proattivi, reattivi e di risposta agli incidenti, confluendo nel CERT-AGID, passando con gradualità le relative consegne allo CSIRT Italia, il nuovo team per gestire la cyber-difesa nazionale istituito con Decreto del Presidente del Consiglio dei ministri 8 agosto 2019 "Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team - CSIRT italiano, presso la Presidenza del Consiglio dei Ministri - Dipartimento di informazioni per la sicurezza della Repubblica". La decisione rientra nell'ambito del piano di attuazione della Direttiva 2016/1148 NIS, recante le misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione europea, che - tra le altre misure - prevede anche in Italia la costituzione di un Computer Security Incident Response Team unico (cosiddetto CSIRT). Questo Team riceve, da soggetti pubblici e soggetti privati, tutte le segnalazioni in caso di incidente cibernetico e/o di segnalazione di evento.

La normativa che regola il funzionamento del CSIRT prevede un alto livello di cooperazione, sia a livello nazionale che europeo. Il team farà, infatti, affidamento sull'Agenzia per l'Italia digitale (AgID) e in particolare sul CERT-AgID che ha sostituito il CERT-PA, con il compito di definire raccomandazioni e strategie per sensibilizzare e informare le amministrazioni

sui temi della sicurezza informatica. A livello europeo, il CSIRT, attraverso il Dipartimento delle informazioni per la sicurezza della Presidenza del Consiglio dei ministri, di cui all'art. 4, della legge 3 agosto 2007, n. 124, collabora con i suoi omologhi presenti negli altri stati membri, con la Commissione Europea e con l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA). Questa collaborazione permette la creazione di una cornice di sicurezza europea e l'adozione di politiche comuni sulla sicurezza informatica.

Con il Decreto Legge 14 giugno 2021 n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109, è stata istituita l'Agenzia per la Cybersicurezza Nazionale (ACN) che, tra le varie competenze, ha anche quella di predisporre la Strategia nazionale di cybersicurezza che viene poi adottata dal Presidente del Consiglio dei Ministri.

La Strategia Nazionale di Cybersicurezza 2022-2026 in cui si delineano tre obiettivi fondamentali (Protezione, Risposta, Sviluppo) da raggiungere entro il 2026 con il contributo di tutti gli attori a vario titolo coinvolti tra cui anche le Regioni accompagnato da un Piano di implementazione composto da 82 Misure, è stata approvata lo scorso 18 maggio 2022.

In ambito locale, Regione del Veneto, in attuazione delle "Linee Guida per l'Agenda Digitale del Veneto 2025", approvate con Deliberazione della Giunta Regionale n. 156 del 22/02/2022, ove si sottolinea, al fine di implementare i servizi e strumenti di sicurezza per il sistema informatico regionale, la necessità di avviare una collaborazione tra Enti pubblici e privati per una gestione condivisa del rischio informatico a livello regionale, ha partecipato in modo sinergico con le Agenzie Regionali e con Azienda Zero, a percorsi di analisi e studio rispetto alla possibilità di potenziare i presidi di cybersecurity nel contesto regionale, abilitando un ecosistema operativo e sempre più cooperativo che, attraverso la definizione di processi integrati e coordinati, possa rafforzare la capacità di segnalare e di fare intelligence per il settore, ampliare la rete di partnership pubblico-privato e definire un fronte condiviso di risposta al fenomeno cyber, attraverso un dialogo continuo tra gli enti locali.

Dalle valutazioni delle diverse opzioni possibili proposte, alla luce della suddetta esperienza statale, emerge l'importanza di porre particolare attenzione verso l'opportunità di attuare modelli di coordinamento e di servizio tipici di un CERT (Computer Emergency Response Team), inclusivo di un HyperSOC (Security Operation Center) che possa monitorare la sicurezza e gestire gli incidenti a livello regionale, così come descritto nel progetto **Allegato A**.

I servizi che erogherà il CERT regionale possono essere raggruppati in quattro categorie:

- Servizi Reattivi: orientati a gestire gli incidenti quando si verificano, riducendone il danno conseguente;
- Servizi Proattivi: diretti a prevenire l'occorrenza degli incidenti, mediante la condivisione delle informazioni e l'utilizzo di strumenti specifici;
- Gestione degli Artefatti: si prevede la raccolta e l'analisi di qualsiasi elemento o evidenza (file, codici malevoli, tracce in memoria), coinvolti in azioni dolose;
- Servizi di gestione della Qualità della Sicurezza: i servizi che rientrano in questa categoria non sono specifici della gestione degli incidenti o dei CERT in particolare. Si tratta piuttosto di servizi e pratiche per migliorare la sicurezza generale di un'organizzazione.

Il CERT regionale sarà organizzato secondo il modello Campus, avente come Constituency le pubbliche amministrazioni locali di riferimento, le società partecipate, gli enti strumentali, il CSIRT Italiano, il CNAIPIC ed eventuali altri Enti/Società che ne facciano richiesta o che in futuro intratterranno rapporti con Regione del Veneto.

Regione del Veneto avrà un ruolo di coordinamento e direttivo nella fase di implementazione della soluzione, per la formalizzazione del progetto esecutivo (servizi inclusi nella soluzione di CERT Regionale, modello organizzativo e di governance, processi di attivazione e coordinamento per la gestione di eventuali incidenti di sicurezza), nonché nella manutenzione e gestione della soluzione nella fase attuativa. Inoltre, sulla base del proprio ruolo e dei mandati normativi, Regione del Veneto potrà intervenire a supporto delle attività locali in carico a singoli enti aderenti.

Ciascun Ente aderente avrà un ruolo operativo per la definizione dei processi operativi di utilizzo della soluzione ed integrazione con le piattaforme eventualmente sviluppate internamente (ad es. un SOC/CERT sviluppato localmente, che colloquierebbe in maniera permanente con il CERT Regionale ed entrerebbe a far parte del Campus), al fine di garantirne l'autonomia nella definizione ed implementazione delle iniziative di sicurezza e nella gestione di eventi di sicurezza con impatto locale.

A livello operativo, sulla base delle mission e del mandato normativo di Azienda Zero e dai SAD, queste entità dovranno coordinare e supportare rispettivamente enti sanitari e comuni nella gestione della propria sicurezza, fungendo anche da collettore e centralizzatore di alcuni servizi di sicurezza che potranno quindi essere integrati con il CERT Regionale.

Sarà inoltre attuata una costante correlazione ed integrazione con altri Enti/Società che ne facciano richiesta o che in futuro intratterranno rapporti con Regione del Veneto, quali CSIRT Italiano, il CNAIPIC, la Polizia di Stato, ecc.

Il modello di Governance del CERT regionale sarà organizzato in tre livelli:

- 1° livello (strategico): composto dal Comitato Strategico CERT Regionale, è responsabile di fornire un indirizzo strategico sulle politiche di conduzione del CERT Regionale e punto decisionale per l'escalation di incidenti gravi verso le autorità competenti Comitato Strategico CERT Regionale.
- 2° livello (direttivo): composto dal Comitato Direttivo CERT Regionale, è responsabile di indirizzare la strategia definita a livello strategico, definendo processi e procedure che garantiscano il raggiungimento degli obiettivi prefissati.
- 3° livello (operativo): composto da CERT Regionale, SOC/CERT ed esperti Cyber degli Enti locali aderenti, è responsabile dell'implementazione e della manutenzione dei processi e delle procedure definite a livello direttivo.

I costi e gli investimenti iniziali necessari all'attivazione del CERT Regionale sono stimati in Euro 7.500.000,00 iva inclusa massimi, dei quali quelli ricadenti in capo alla Direzione ICT e Agenda Digitale sono stimati in euro 2.440.000,00 iva inclusa mentre quelli relativi alla sicurezza ICT della Sanità regionale sono stimati in euro 5.060.000,00 iva inclusa, in capo all'Area Sanità e Sociale.

I costi di gestione per gli anni successivi all'avvio sono stimati in un massimo di € 6.402.000,00 iva inclusa, dei quali € 1.764.300,00 in capo all'Area Risorse Finanziarie, Strumentali, ICT Ed Enti Locali ed € 4.667.400,00 in capo all'Area Sanità e Sociale.

In sede di successiva progettazione esecutiva, che sarà curata dalla Direzione ICT e Agenda Digitale, saranno dettagliati i servizi inclusi nella soluzione di CERT Regionale, precisati i ruoli, tempi di attuazione, responsabilità e modalità di funzionamento del modello organizzativo proposto, i processi di attivazione e coordinamento per la gestione di eventuali incidenti di sicurezza, le regole e i costi di gestione, i modelli di adesione e di partecipazione alla spesa e la dettagliata ripartizione dei costi tra l'Area Risorse Finanziarie, Strumentali, ICT Ed Enti Locali, l'Area Sanità e Sociale e gli altri Enti/Società che aderiranno al CERT Regionale. Tale progetto esecutivo sarà sottoposto all'approvazione della Giunta Regionale.

Gli importi in capo alla Direzione ICT e Agenda Digitale saranno in quota parte a carico dei capitoli di spesa della Direzione stessa e in parte derivanti da fonti di finanziamento di tipo governativo o europeo. In data 02/08/2022 è stato infatti pubblicato l'avviso pubblico per la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5, approvato con Decisione di esecuzione del Consiglio europeo in data 13/07/2021.

L'avviso ha lo scopo di individuare, mediante procedura valutativa selettiva con graduatoria, le proposte progettuali finalizzate al potenziamento del livello di maturità delle capacità cyber dei sistemi informativi delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome.

Il fine ultimo degli interventi è quello di potenziare il livello di resilienza cyber dei sistemi informativi per la messa in sicurezza dei dati e dei servizi dei cittadini. Questi interventi, nonché il complesso degli interventi dell'Investimento 1.5, rappresentano un elemento fondante per la transizione digitale sicura della PA. Pertanto, l'investimento 1.5 rappresenta un'opportunità imprescindibile per la PA, e nel complesso per il Paese, per irrobustire le infrastrutture e i servizi digitali, nonché le competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza per il paese.

La dotazione finanziaria dell'Avviso ammonta complessivamente a Euro 45.000.000,00. L'importo massimo ammissibile a finanziamento è pari a Euro 1.000.000,00 per progetto e comunque Euro 2.000.000,00 per Soggetto proponente. I progetti e quindi i relativi interventi ammessi a finanziamento dovranno concludersi entro 24 mesi dalla data di sottoscrizione dell'Atto d'obbligo, e comunque non oltre la data del 30 novembre 2024, sulla base del cronoprogramma presentato. Le proposte progettuali dovranno essere inviate dai soggetti interessati entro le ore 18:00 del 30/09/2022.

Gli importi relativi alla sicurezza ICT della sanità regionale troveranno copertura all'interno della Gestione Sanitaria Accentrata dell'anno 2023 per l'importo massimo di € 5.060.000,00 e, per gli anni successivi, per l'importo massimo di € 4.667.400,00.

La Direzione ICT e Agenda Digitale e l'Area Sanità e Sociale, ciascuna per l'ambito di propria competenza, vengono incaricate dell'esecuzione del presente provvedimento con riferimento all'adozione di ogni atto connesso, consequenziale e comunque necessario a dar corso alle iniziative sopra descritte, senza oneri finanziari e patrimoniali a carico del bilancio regionale.

Il relatore conclude la propria relazione e propone all'approvazione della Giunta regionale il seguente provvedimento.

LA GIUNTA REGIONALE

UDITO il relatore, il quale dà atto che la struttura competente ha attestato, con i visti rilasciati a corredo del presente atto, l'avvenuta regolare istruttoria della pratica, anche in ordine alla compatibilità con la vigente legislazione statale e regionale, e che successivamente alla definizione di detta istruttoria non sono pervenute osservazioni in grado di pregiudicare l'approvazione del presente atto;

- VISTO il P.N.R.R. approvato con Decisione di esecuzione del Consiglio europeo in data 13/07/2021;

- VISTO il Decreto Legge 14 giugno 2021 n. 82, convertito con modificazioni dalla L. 4 agosto 2021, n. 109;

- VISTA la Strategia Nazionale di Cybersicurezza 2022-2026 approvata il 18 maggio 2022;

- VISTO il D.Lgs. n. 33 del 14/03/2013;

- VISTO l'art. 2 comma 2 della legge regionale n. 54 del 31 dicembre 2012;

- VISTA la Deliberazione della Giunta Regionale n. 156 del 22/02/2022;

delibera

1. le premesse costituiscono parte integrante e sostanziale del presente provvedimento;
2. di approvare il "Progetto CERT Regionale (Computer Emergency Response Team)" di Regione del Veneto (allegato A), demandando il dettaglio e la precisazione dei servizi inclusi nella soluzione di CERT Regionale, dei ruoli, tempistiche di attuazione, responsabilità e modalità di funzionamento del modello organizzativo proposto, dei processi di attivazione e coordinamento per la gestione di eventuali incidenti di sicurezza, delle regola e dei costi di gestione annuali, dei modelli di adesione e di partecipazione alla spesa, la dettagliata ripartizione dei costi tra l'Area Risorse Finanziarie, Strumentali, ICT Ed Enti Locali, l'Area Sanità e Sociale e gli altri Enti/Società che aderiranno al CERT Regionale, ad una successiva progettazione esecutiva, affidata alla Direzione ICT e Agenda Digitale, che sarà sottoposta all'approvazione della Giunta Regionale;
3. di dare atto che i costi e gli investimenti necessari per la realizzazione del CERT Regionale sono stimati in Euro 7.500.000,00 iva compresa, che saranno coperti mediante ricorso a risorse del P.N.R.R. Missione 1 e da risorse Regionali derivanti dai capitoli di spesa in capo alla Direzione ICT e Agenda Digitale, per l'importo massimo di Euro 2.440.000 iva compresa e dall'Area Sanità Sociale per l'importo massimo di Euro 5.060.000 iva compresa, come meglio sarà precisato in sede di approvazione da parte della Giunta Regionale della progettazione esecutiva di cui al Punto 2) del presente provvedimento ;
4. di autorizzare la Direzione ICT e Agenda Digitale a partecipare all'avviso pubblicato in data 02/08/2022 per la presentazione di due proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome a valere sul PIANO NAZIONALE DI RIPRESA E RESILIENZA, Missione 1 - Componente 1 - Investimento 1.5 "Cybersecurity" M1C1I1.5;
5. di incaricare la Direzione ICT e Agenda Digitale e l'Area Sanità e Sociale, ciascuna per l'ambito di propria competenza, dell'esecuzione del presente provvedimento con riferimento all'adozione di ogni atto connesso, consequenziale e comunque necessario a dar corso alle iniziative sopra descritte, senza oneri finanziari e patrimoniali a carico del bilancio regionale;
6. di pubblicare integralmente la presente deliberazione nel Bollettino Ufficiale della Regione.

Allegato *(omissis)*