



Allegato a supporto della deliberazione n.  
62 del 31 ottobre 2023

Data 29/08/2023

Protocollo N° 0460089 ClassC.101.01.1 Fasc.

Allegati N°2 per tot.pag. 15

*Oggetto: DGR n. 1024 del 22/08/2023 - Approvazione del progetto esecutivo del Computer Emergency Response Team (CERT) Regionale*

Al Consiglio regionale del Veneto  
Segretario generale – Roberto Valente  
[protocollo@consiglioveneto.legalmail.it](mailto:protocollo@consiglioveneto.legalmail.it)

Con la presente si comunica l'avvenuta approvazione, con DGR n.1024 del 22/08/2023, del Progetto Esecutivo CERT Regionale (Computer Emergency Response Team) di Regione del Veneto. L'obiettivo è definire un CERT regionale ovvero una struttura istituita e operante sul territorio con il ruolo di coordinare, supportare e monitorare le attività di prevenzione, risposta e ripristino degli incidenti critici di tipo cyber nell'ambito del dominio costituito dalle PAL (Pubbliche Amministrazioni Locali), Società a partecipazione regionale maggioritaria e Enti pubblici regionali strumentali o altri Enti.

Gli obiettivi del CERT sono:

1. Fornire supporto ed assistenza specialistica nell'analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cyber security.
2. Agevolare la diffusione di informazioni tempestive e immediatamente utilizzabili su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cibernetici indirizzati a specifici settori, organizzazioni o territori.
3. Incentivare l'applicazione dei processi di gestione della sicurezza, delle metodologie e delle metriche valutative per il governo della sicurezza cibernetica definite.
4. Facilitare le attività di prevenzione e monitoraggio degli eventi cibernetici sul territorio, agendo come unità capaci di esercitare un controllo più diretto a livello locale.
5. Collaborare e cooperare con le altre organizzazioni nazionali ed internazionali nel potenziamento e miglioramento della capacità difensiva delle organizzazioni in materia di cyber security.
6. Accrescere le competenze specialistiche degli addetti alla sicurezza cibernetica e migliorare le attività di sensibilizzazione su questi temi a livello locale.

Il progetto esecutivo di CERT Regionale è stato declinato al fine ultimo di potenziare il livello di resilienza cyber dei sistemi informativi per la messa in sicurezza dei dati e dei servizi dei cittadini.

Area Risorse Finanziarie, Strumentali, ICT ed Enti Locali

**Direzione ICT e Agenda Digitale**

Centro Vega –Palazzo Lybra -Via Pacinotti n.4 – 30175 Marghera- (Ve) Tel. 041/2792202-2204 – Fax 041/2792218

[ictagendadigitale@regione.veneto.it](mailto:ictagendadigitale@regione.veneto.it)

[ictagendadigitale@pec.regione.veneto.it](mailto:ictagendadigitale@pec.regione.veneto.it)



REGIONE DEL VENETO

giunta regionale

Il CERT regionale rappresenta il punto di raccordo tra gli Enti locali, ovvero le pubbliche amministrazioni locali di riferimento, le società partecipate, gli enti strumentali ed eventuali altri Enti/Società che ne facciano richiesta o che in futuro intratterranno rapporti con Regione del Veneto.

Gli Enti aderiranno ai servizi del CERT sottoscrivendo lo schema di convenzione allegato alla Delibera (Allegato B).

Successivamente alla presente nota, verranno avviati gli incontri con codesto Ente per l'attivazione del progetto.

Cordiali saluti.

**Referente Sicurezza ICT**

UO Sistemi informativi, servizi e tecnologie digitali  
dott. Giuseppe Mendola tel 041.2792242

Direzione ICT e Agenda Digitale

*Il Direttore*

*- dott. Idelfo Borgo -*

copia cartacea composta di 2 pagine, di documento amministrativo informatico firmato digitalmente da BORGIO IDELFO, il cui originale viene conservato nel sistema di gestione informatica dei documenti della Regione del Veneto - art.22.23.23 ter D.Lgs 7/3/2005 n. 82

*Area Risorse Finanziarie, Strumentali, ICT ed Enti Locali*

**Direzione ICT e Agenda Digitale**

*Centro Vega -Palazzo Lybra -Via Pacinotti n.4 - 30175 Marghera- (Ve) Tel. 041/2792202-2204 - Fax 041/2792218*

*ictagendadigitale@regione.veneto.it*

*ictagendadigitale@pec.regione.veneto.it*



Proposta n. 1541 / 2023

**PUNTO 4 DELL'ODG DELLA SEDUTA DEL 22/08/2023**

ESTRATTO DEL VERBALE

**DELIBERAZIONE DELLA GIUNTA REGIONALE n. 1024 / DGR del 22/08/2023**

**OGGETTO:**

Approvazione del progetto esecutivo del Computer Emergency Response Team (CERT) Regionale, in continuità con la D.G.R. n. 1174 del 27/09/2022.



**COMPONENTI DELLA GIUNTA REGIONALE**

Presidente	Luca Zaia	Presente
Vicepresidente	Elisa De Berti	Assente
Assessori	Gianpaolo E. Bottacin	Presente
	Francesco Calzavara	Presente
	Federico Caner	Presente
	Cristiano Corazzari	Presente
	Elena Donazzan	Assente
	Manuela Lanzarin	Presente
Segretario verbalizzante	Roberto Marcato	Presente
	Lorenzo Traina	

**RELATORE ED EVENTUALI CONCERTI**

FRANCESCO CALZAVARA di concerto con MANUELA LANZARIN

**STRUTTURA PROPONENTE**

AREA RISORSE FINANZIARIE, STRUMENTALI, ICT ED ENTI LOCALI

**APPROVAZIONE**

Sottoposto a votazione, il provvedimento è approvato con voti unanimi e palesi.





OGGETTO: Approvazione del progetto esecutivo del Computer Emergency Response Team (CERT) Regionale, in continuità con la D.G.R. n. 1174 del 27/09/2022.

NOTE PER LA TRASPARENZA:

Il provvedimento approva il progetto esecutivo del Computer Emergency Response Team (CERT) Regionale, in continuità con la D.G.R. n. 1174 del 27/09/2022.

---

Il relatore 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. La digitalizzazione dei servizi e delle informazioni ha, infatti, inevitabilmente accresciuto l'esposizione al rischio; il pericolo di furto e la manomissione e compromissione dei dati nello spazio cibernetico hanno 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.

Il contrasto e la prevenzione agli attacchi di natura cibernetica e la necessità di garantire elevati livelli di sicurezza di reti e informazioni rappresentano un ambito di grande attenzione regionale, con l'obiettivo primario di assicurare un corretto svolgimento dei servizi pubblici offerti e per garantire la continuità di quei servizi critici per la qualità di vita, la salute e la sicurezza del cittadino.

Per tale ragione, con D.G.R. n. 1174 del 27/09/2022, la Giunta regionale ha approvato il progetto del CERT (Computer Emergency Response Team) Regionale, avente i seguenti obiettivi:

1. fornire supporto ed assistenza specialistica nell'analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cyber security;
2. agevolare la diffusione di informazioni tempestive e immediatamente utilizzabili su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cibernetici indirizzati a specifici settori, organizzazioni o territori;
3. incentivare l'applicazione dei processi di gestione della sicurezza, delle metodologie e delle metriche valutative per il governo della sicurezza cibernetica definite;
4. facilitare le attività di prevenzione e monitoraggio degli eventi cibernetici sul territorio, agendo come unità capaci di esercitare un controllo più diretto a livello locale;
5. collaborare e cooperare con le altre organizzazioni nazionali ed internazionali nel potenziamento e miglioramento della capacità difensiva delle organizzazioni in materia di cyber security;
6. accrescere le competenze specialistiche degli addetti alla sicurezza cibernetica e migliorare le attività di sensibilizzazione su questi temi a livello locale.

Con il medesimo provvedimento è stata demandata alla Direzione ICT e Agenda Digitale la progettazione esecutiva di tale CERT Regionale.



Il progetto esecutivo di CERT Regionale, elaborato dalla Direzione ICT e Agenda Digitale, di cui segue una breve descrizione, è stato declinato al fine ultimo di potenziare il livello di resilienza cyber dei sistemi informativi per la messa in sicurezza dei dati e dei servizi dei cittadini (**Allegato A**).

Il CERT Regionale rappresenta, infatti, il punto di raccordo tra gli Enti locali, ovvero le pubbliche amministrazioni locali di riferimento, le società partecipate, gli enti strumentali ed eventuali altri Enti/Società che ne facciano richiesta o che in futuro intratterranno rapporti con Regione del Veneto.

I servizi erogati dal CERT Regionale, a favore dei singoli enti, 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: raccolta ed analisi di qualsiasi elemento o evidenza (file, codici malevoli, tracce in memoria) coinvolti in azioni dolose;
- servizi di gestione della qualità della sicurezza: trattasi di servizi e pratiche per migliorare la sicurezza generale di un'organizzazione.

Il CERT Regionale opererà alcuni servizi di sicurezza verso gli Enti aderenti, prevedendo un modello ibrido che garantisca il mantenimento delle responsabilità presso singolo Ente ed una suddivisione dei compiti operativi tra CERT Regionale e singolo Ente, sulla base del gruppo di appartenenza.

Il modello organizzativo del CERT di Regione del Veneto sarà organizzato su tre livelli di Governo che identificano gli attori principali ed i relativi ruoli per lo sviluppo e l'operatività del CERT stesso. Tale modello definisce le relazioni tra il CERT di Regione del Veneto, gli aderenti (enti locali), le Istituzioni nazionali (CSIRT Italiano e altri CERT di settore) e le istituzioni internazionali. In particolare:

1. livello STRATEGICO: composto dal Comitato Strategico del CERT Regionale, è responsabile di fornire un indirizzo strategico sulle politiche di conduzione del CERT Regionale e costituisce un punto decisionale per l'escalation di incidenti gravi verso le autorità competenti; è presieduto da un referente di Regione del Veneto - che ne è il Presidente -, da referenti degli enti aderenti (GRUPPI 1 & 2 e Consiglio Regionale) e dalle istituzioni ed autorità nazionali in termini di sicurezza nazionale cibernetica (i.e. ACN e Polizia Postale).
2. livello DIRETTIVO: composto dal Comitato Direttivo del CERT Regionale, è responsabile di indirizzare la strategia, definendo processi e procedure che garantiscano il raggiungimento degli obiettivi prefissati, avvalendosi di esperti di Cybersecurity ed interloquendo con le istituzioni/organizzazioni nazionali; è presieduto dal Responsabile del CERT Regionale e da rappresentanti con ruoli di Responsabili della Sicurezza Informatica/Responsabili Sistemi Informativi (CISO/CIO) degli enti aderenti (GRUPPI 1 & 2 e Consiglio Regionale), coadiuvato da un team di esperti di cybersecurity.
3. livello OPERATIVO: composto dai referenti di sicurezza degli Enti locali aderenti è responsabile dell'implementazione e della manutenzione dei processi e delle procedure definite a livello direttivo; è presieduto dalle risorse che indirizzano le tematiche di sicurezza all'interno del singolo ente aderente (GRUPPI 1, 2, 3, 4, 5) e di Regione del Veneto.

Dal punto di vista operativo, il CERT Regionale sarà organizzato presso la Direzione ICT e Agenda Digitale e sarà composto da un gruppo di lavoro, che verrà nominato con apposito Decreto dal Direttore della Direzione ICT e Agenda Digitale, in grado di supportare gli Enti nella risposta agli incidenti, nonché fornire risorse specialistiche in grado di erogare supporto su tematiche di sicurezza ad alta specializzazione e nell'utilizzo dei diversi sistemi e strumenti in uso. L'ufficio del CERT Regionale sarà governato da un responsabile al quale afferiranno i diversi team incaricati allo svolgimento delle attività operative. In particolare, all'interno del CERT saranno individuate tre funzioni:

- funzione di Governance: gestione delle attività amministrative dell'ufficio;
- funzione di Security Strategy: gestione del framework di monitoraggio del CERT; erogazione delle attività consulenziali relative alla gestione del rischio, alla business continuity, al disaster recovery, nonché sensibilizzazione, formazione e svolgimento di attività di supporto alla certificazione ISO 27001;



- funzione di esperti Cyber: monitoraggio di vulnerabilità, delle minacce e delle attività di risposta agli incidenti cyber.

Il progetto esecutivo, come sopra descritto, è stato ampiamente condiviso all'interno dell'Unità di Coordinamento - PNRR Sanità e Sociale, istituita con Decreto n. 32 del 4 aprile 2023 del Direttore Generale dell'Area Sanità e Sociale, al fine di garantire che le attività di programmazione e di realizzazione degli interventi e dei connessi investimenti in attuazione delle Missioni del PNRR interessanti l'ambito sanitario, socio sanitario e sociale, si sviluppino secondo un quadro organico, sinergico, integrato e sistemico.

Il progetto esecutivo è stato, inoltre, condiviso con Azienda Zero con nota prot. n. 409345 del 31/07/2023.

Il progetto suddetto risulta, peraltro, coerente con la "Proposta di intervento per la sicurezza ICT della Sanità della Regione del Veneto", trasmessa, con nota in data 01/06/2022, prot. n. 16449, da Azienda Zero all'Area Sanità e sociale per la successiva trasmissione al Crite e da quest'ultimo approvata nella seduta del 5 dicembre 2022, come risulta dalla nota prot. n. 592014 in data 22/12/2022 trasmessa dall'Area Sanità e Sociale ad Azienda Zero.

La Direzione ICT e Agenda Digitale nell'ambito dell'esecuzione delle attività inerenti il CERT Regionale, si qualificherà come **Responsabile del Trattamento**, ai sensi dell'Art. 28 del GDPR, al fine di supportare gli Enti aderenti (**Titolari del trattamento**) nel mettere in atto misure di sicurezza tecniche e organizzative volte ad assicurare l'applicazione del GDPR e garantire livelli di sicurezza adeguati per valutare e ridurre i rischi derivanti dal trattamento dei dati di competenza.

L'adesione al CERT Regionale sarà rivolta agli Enti pubblici regionali strumentali a Regione del Veneto (quali ad es. le varie ATER presenti nel territorio veneto, AVEPA, ARPAV, ecc...), alle società a partecipazione regionale maggioritaria (ad es. Sistemi Territoriali S.p.A., Veneto Innovazione S.p.A., ecc...) ed agli altri Enti regionali (ad es. Consiglio Regionale del Veneto, Azienda Zero, ecc...).

Per poter aderire al CERT i suddetti Enti dovranno possedere i seguenti requisiti:

- nomina di un referente per la sicurezza delle informazioni, il quale dovrà interfacciarsi con i referenti del CERT di Regione del Veneto;
- raggiungimento di un livello minimo di sicurezza;
- personale dedicato alla gestione dei servizi di sicurezza forniti dal CERT Regionale;
- budget dedicato a tematiche di sicurezza.

L'adesione degli Enti interessati al CERT regionale avverrà attraverso la stipula di apposita convenzione della durata massima di tre anni (**Allegato B**), ai sensi dell'art. 15 della Legge n. 241 del 1990.

A seguito dell'adesione al CERT Regionale, gli Enti dovranno raggiungere i seguenti obiettivi:

- adozione dei requisiti di sicurezza AGID - requisiti minimi. Gli enti appartenenti al CERT dovranno soddisfare la lista di requisiti minimi come da linee guida AGID;
- adeguamento alla Direttiva NIS 2 (Direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 sulla sicurezza delle reti e delle informazioni) per gli enti operanti nei settori critici.

Ciò posto, si reputa, quindi, allo stato opportuno, in attuazione del percorso avviato con la citata DGR n. 1174/2022, procedere all'approvazione del progetto esecutivo CERT Regionale e dello Schema di Convenzione di adesione al CERT Regionale da parte degli Enti Regionali, allegati al presente provvedimento quale parte integrante e sostanziale dello stesso, rispettivamente, sotto la lettera **A**) e **B**).

Il progetto prevede i costi di funzionamento a capo di Regione del Veneto (Direzione ICT e Agenda Digitale e Area Sanità e Sociale) e dei relativi Enti strumentali. Si precisa che detti costi sono parzialmente diversi da quelli indicati nella D.G.R. n. 1174 del 27/09/2022 in quanto i relativi servizi in sede di progettazione esecutiva sono stati dettagliati e ampliati comportando un aumento dei costi rispetto all'originaria previsione. Si precisa altresì che i servizi relativi agli ambiti di intervento "Altri Servizi" e "Sviluppo sicuro/Analisi del Codice", saranno avviati successivamente al primo anno.

In particolare la spesa sarà così articolata:

- per il primo anno di attività, a partire dal mese di ottobre 2023, Euro 7.771.339,00 iva compresa, che saranno coperti mediante ricorso a:

- risorse del P.N.R.R. Missione 1, per l'importo di Euro 2.000.000,00 iva compresa,



- risorse relative al contratto in corso cig 8863863325 in capo alla Direzione ICT e Agenda Digitale per l'importo di Euro 494.100,00 iva compresa,
- risorse Regionali derivanti dai capitoli di spesa in capo alla Direzione ICT e Agenda Digitale, per l'importo massimo di Euro 668.560,00 iva compresa,
- risorse Regionali derivanti dai capitoli di spesa in capo all'Area Sanità e Sociale per l'importo massimo di Euro 4.608.679,00 iva compresa;

si precisa che il costo del primo anno di attività del CERT Regionale comprende i costi dell'eventuale adesione degli Enti non afferenti all'Area Sanità e Sociale;

- per i successivi 2 anni di attività Euro 8.729.039,00 (iva compresa) annuali, che saranno coperti mediante ricorso:

- risorse relative al contratto in corso cig 8863863325 in capo alla Direzione ICT e Agenda Digitale per l'importo di Euro 494.100,00 iva compresa,
- risorse Regionali derivanti dai capitoli di spesa in capo alla Direzione ICT e Agenda Digitale, per l'importo massimo di Euro 668.560,00 iva compresa,
- risorse Regionali derivanti dai capitoli di spesa in capo all'Area Sanità e Sociale per l'importo massimo di Euro 5.942.620,00 iva compresa;
- risorse relative agli Enti strumentali non afferenti all'Area Sanità e Sociale che aderiranno per l'importo massimo di Euro 1.623.759,00 iva compresa.

Gli importi complessivi in capo alla Direzione ICT e Agenda Digitale, pari ad Euro 2.005.680,00 iva compresa, troveranno copertura sul capitolo di spesa corrente n. 7200 del Bilancio regionale 2023 - 2025. Al riguardo, il Direttore della Direzione ICT e Agenda Digitale attesta che il suddetto capitolo presenta sufficiente capienza.

Per quanto attiene alle risorse regionali derivanti dai capitoli di spesa in capo all'Area Sanità e Sociale saranno messe a disposizione del budget della Direzione ICT e Agenda Digitale secondo la seguente esigibilità:

Risorse	2023 (3 mesi)	2024 (9+3 mesi)	2025 (12 mesi)	2026 (9 mesi)	TOTALE
Sanità e Sociale	€ 1.152.169,75	€ 4.942.164,25	€ 5.942.620,00	€ 4.456.965,00	€ 16.493.919,00

Il trasferimento delle risorse dell'Area Sanità Sociale avverrà nell'ambito di una convenzione da sottoscrivere tra Azienda Zero e Direzione ICT e Agenda Digitale.

Si demanda al Direttore della Direzione ICT e Agenda Digitale il compimento di ogni atto connesso, consequenziale e comunque necessario a dar corso al presente provvedimento.

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 l'art. 15 della Legge n. 241 del 1990;

- VISTO l'art. 7 del D.Lgs. n. 36 del 2023;

- VISTA la DGR n. 1174 del 22/09/2022;

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

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





DELIBERA

1. di approvare le premesse quale parte integrante e sostanziale del presente provvedimento;
2. di approvare, quale **Allegato A)** al presente provvedimento, nonché parte integrante/sostanziale dello stesso, il progetto esecutivo CERT (Computer Emergency Response Team) Regionale, che sarà organizzato presso la Direzione ICT e Agenda Digitale, attribuendo al Direttore della Direzione ICT e Agenda Digitale la facoltà di apportarvi delle modifiche a fronte di cambiamenti e/o nuove opportunità tecnologiche che intervenissero e a fronte di variazione dei costi;
3. di individuare il Presidente del Comitato Strategico del CERT Regionale nel Direttore della Direzione ICT e Agenda Digitale;
4. di approvare, quale **Allegato B)** al presente provvedimento, nonché parte integrante/sostanziale dello stesso, lo Schema di convenzione di adesione al CERT Regionale da parte degli Enti regionali, incaricando il Direttore della Direzione ICT e Agenda Digitale della sua sottoscrizione con facoltà di introdurre nell'interesse dell'Amministrazione Regionale eventuali modifiche/integrazioni non sostanziali;
5. di incaricare il Direttore della Direzione ICT e Agenda Digitale del compimento di ogni atto connesso, consequenziale e comunque necessario a dar corso al presente provvedimento, compresa la facoltà, con propri decreti, di organizzare il funzionamento del CERT Regionale, sulla base delle indicazioni contenute nel progetto esecutivo, di cui all'**Allegato A)**, compresa la costituzione dei relativi Comitati;
6. di dare atto che i costi e gli investimenti necessari per la realizzazione del CERT Regionale sono stimati, per il primo anno di attività (indicativamente da ottobre 2023 a settembre 2024), in Euro 7.771.339,00 iva compresa, che saranno coperti mediante ricorso a:
  - risorse del P.N.R.R. Missione 1 per l'importo di Euro 2.000.000,00 iva compresa;
  - risorse relative al contratto in corso cig 8863863325 in capo alla Direzione ICT e Agenda Digitale per l'importo di Euro 494.100,00 iva compresa;
  - risorse Regionali derivanti dai capitoli di spesa in capo alla Direzione ICT e Agenda Digitale, per l'importo massimo di Euro 668.560,00 iva compresa;
  - risorse Regionali derivanti dai capitoli di spesa in capo all'Area Sanità Sociale per l'importo massimo di Euro 4.608.679,00 iva compresa;
  - si precisa che il costo del primo anno di attività del CERT Regionale comprende i costi dell'eventuale adesione degli Enti non afferenti all'Area Sanità e Sociale;
7. di dare atto che i costi e gli investimenti necessari per la realizzazione del CERT Regionale sono stimati, per i successivi 2 anni di attività (indicativamente da ottobre 2024 a settembre 2026) Euro 8.729.039,00 (iva compresa) annuali, che saranno coperti mediante ricorso:
  - risorse relative al contratto in corso cig 8863863325 in capo alla Direzione ICT e Agenda Digitale per l'importo di Euro 494.100,00 iva compresa;
  - risorse Regionali derivanti dai capitoli di spesa in capo alla Direzione ICT e Agenda Digitale, per l'importo massimo di Euro 668.560,00 iva compresa;
  - risorse Regionali derivanti dai capitoli di spesa in capo all'Area Sanità e Sociale per l'importo massimo di Euro 5.942.620,00 iva compresa;
  - risorse relative agli Enti strumentali non afferenti all'Area Sanità e Sociale che aderiranno per l'importo massimo di Euro 1.623.759,00 iva compresa.
8. di dare atto che gli importi complessivi in capo alla Direzione ICT e Agenda Digitale, pari ad Euro 2.005.680,00 iva compresa, troveranno copertura sul capitolo di spesa corrente n. 7200 del Bilancio regionale 2023 - 2025, annualità 2023, 2024, 2025 e 2026;
9. di dare atto che la Direzione ICT e Agenda Digitale, a cui è stato assegnato il capitolo di spesa n. 7200, ha attestato che il medesimo capitolo presenta sufficiente capienza;
10. di dare atto che le risorse regionali derivanti dai capitoli di spesa in capo all'Area Sanità e Sociale, pari ad Euro 16.493.919,00, iva compresa, saranno messe a disposizione del budget della Direzione ICT e Agenda Digitale secondo la seguente esigibilità: Euro 1.152.169,75 nel 2023, Euro



- 4.942.164,25 nel 2024, Euro 5.942.620,00 nel 2025 ed Euro 4.456.965 nel 2026. Il trasferimento delle risorse dell'Area Sanità Sociale avverrà nell'ambito di una convenzione da sottoscrivere tra Azienda Zero e Direzione ICT e Agenda Digitale;
- 11.di dare atto che il presente provvedimento è soggetto a pubblicazione ai sensi dell'art. 23 del D.Lgs. n. 33 del 14/03/2013;
- 12.di pubblicare la presente deliberazione nel Bollettino Ufficiale della Regione, omettendo gli allegati.

IL VERBALIZZANTE  
Segretario della Giunta Regionale  
Dott. Lorenzo Traina



**SCHEMA DI CONVENZIONE PER L'ADESIONE AL CERT (Computer Emergency Response Team) REGIONALE**

Regione del Veneto (di seguito denominata “*Regione*”), con sede legale in Venezia, Palazzo Balbi – Dorsoduro 3901, codice fiscale 02392630279, rappresentata dal Direttore della Direzione ICT e Agenda Digitale, dott. ...., domiciliato per la sua carica presso la sede dell’Ente,

E

....., con sede in ....., Via ....., (C.F. ....), rappresentata da....., in qualità di Legale Rappresentante,

**PREMESSO CHE**

- la Direttiva 2016/1148 NIS, recante le misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell’Unione europea, prevede– tra le altre misure – anche in Italia la costituzione di un Computer Security Incident Response Team unico (cosiddetto CSIRT);
- 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 CSIRT Italia è stato 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”;
- 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;
- con D.G.R. n. 1174 del 27/09/2022, la Giunta regionale ha approvato il progetto del CERT (Computer Emergency Response Team) Regionale, volto ad attuare modelli di coordinamento e di servizio tipici di un CERT (Computer Emergency Response Team), inclusivo di un HyperSOC (Security Operation Center) e monitorare la sicurezza e gestire gli incidenti a livello regionale;
- con D.G.R. n..... del..... la Giunta regionale ha approvato il progetto esecutivo del CERT regionale;
- con la suddetta Deliberazione è stato, altresì, approvato lo schema di convenzione per l’adesione dei vari Enti regionali veneti al CERT regionale;
- vista l’art. 15 della Legge n. 241 del 1990 e l’art. 7 del D.Lgs. n. 36 del 2023;

Tutto ciò premesso,

SI CONVIENE E SI STIPULA QUANTO SEGUE

**Articolo 1 – Condizioni generali**

Le premesse formano parte integrante e sostanziale della presente convenzione.



**Articolo 2 – Definizione CERT e requisiti di ammissione**

Il CERT regionale è una struttura istituita e operante sul territorio con il ruolo di coordinare, supportare e monitorare le attività di prevenzione, risposta e ripristino degli incidenti critici di tipo cyber nell’ambito del dominio costituito dalle PAL (Pubbliche amministrazioni locali), Società a partecipazione regionale maggioritaria, Enti pubblici regionali strumentali o altri Enti.

Gli obiettivi del CERT sono:

1. Fornire supporto ed assistenza specialistica nell’analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cyber security.
2. Agevolare la diffusione di informazioni tempestive e immediatamente utilizzabili su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cibernetici indirizzati a specifici settori, organizzazioni o territori.
3. Incentivare l’applicazione dei processi di gestione della sicurezza, delle metodologie e delle metriche valutative per il governo della sicurezza cibernetica definite.
4. Facilitare le attività di prevenzione e monitoraggio degli eventi cibernetici sul territorio, agendo come unità capaci di esercitare un controllo più diretto a livello locale.
5. Collaborare e cooperare con le altre organizzazioni nazionali ed internazionali nel potenziamento e miglioramento della capacità difensiva delle organizzazioni in materia di cyber security.
6. Accrescere le competenze specialistiche degli addetti alla sicurezza cibernetica e migliorare le attività di sensibilizzazione su questi temi a livello locale.

Ai fini dell’adesione al CERT, gli Enti regionali sono stati suddivisi nei seguenti gruppi:

	Tipo di Ente	Risorse Interne IT	Livello di Maturità	Livello di Rischio	N° Enti	Enti
<b>GRUPPO 1</b>	Grande	SI	Avviato	Alto	1	▪ Azienda Zero
<b>GRUPPO 2</b>	Grande	SI	Avviato	Medio	3	▪ Arpav ▪ Avepa ▪ Veneto Lavoro
<b>GRUPPO 3</b>	Medio	SI	Avviato	Medio	3	▪ Consiglio Veneto ▪ Infrastrutture Venete/Sistemi Territoriali ▪ Veneto Strade Spa
<b>GRUPPO 4</b>	Medio	SI	Definito	Medio	12	▪ A.T.E.R. PD, TV, VR, VE, BL, RO, VI ▪ ESU PD, VE, VR ▪ Veneto Agricoltura
<b>GRUPPO 5</b>	Piccolo	NO	Considerato	Basso	7	▪ Veneto Acque ▪ Veneto Innovazione, ▪ Veneto edifici monumentali ▪ Ente Parco Regionale Del Fiume Sile, ▪ Ente Parco Regionale Dei Colli Euganei, ▪ Ente Parco Regionale Del Delta Del Po ▪ Istituto Regionale per le ville Venete

Sulla base di quanto sopra, l’Ente ..... fa parte del gruppo n.....

Ai fini dell’adesione, l’Ente .....dichiara di possedere i seguenti requisiti di ammissione:

1. nomina di un Referente per la sicurezza delle informazioni. Gli enti appartenenti ad ogni GRUPPO (1,2,3,4,5) dovranno identificare una figura responsabile dei servizi di sicurezza che si interfacci con i referenti del CERT di Regione del Veneto;
2. raggiungimento di un livello minimo di sicurezza. Gli enti appartenenti ad ogni GRUPPO (1,2,3,4,5) dovranno soddisfare alcuni requisiti di Sicurezza considerati il livello minimo per l’adesione al CERT Regionale. Tali requisiti sono stati identificati come di seguito:
  - presenza di un registro aggiornato degli asset infrastrutturali (FW, Server / Client) in perimetro;
  - presenza di un registro aggiornato degli asset applicativi in perimetro;
  - presenza di soluzioni di Backup ad intera copertura dei sistemi e strumenti in uso dalle funzioni organizzative;



- presenza di un Active Directory;
- presenza di soluzioni di antivirus non deprecate (e.g. Kaspersky);
- 3. dotazione di personale dedicato alla gestione della sicurezza. Gli enti appartenenti ai GRUPPI (1,2) dovranno garantire la presenza di risorse dedicate alla gestione dei servizi di sicurezza forniti dal CERT Regionale;
- 4. dotazione di personale parzialmente dedicato alla gestione della sicurezza. Gli enti appartenenti ai GRUPPI (3,4,5) dovranno garantire la presenza parziale di risorse dedicate alla gestione dei servizi di sicurezza forniti dal CERT Regionale;
- 5. disponibilità di budget dedicato a tematiche di sicurezza per i GRUPPI (1,2,3,4,5).

Il Referente per la sicurezza delle informazioni dell'Ente è individuato in.....

**Articolo 3 – Servizi erogati dal CERT regionale**

Il CERT regionale eroga i servizi di gestione della qualità della sicurezza, servizi reattivi, servizi proattivi e servizi di gestione degli artefatti, così come descritti nell'allegato Progetto esecutivo, parte integrante e sostanziale della presente Convenzione.

**Articolo 4 – Modello operativo**

Il modello operativo del CERT Regionale di Regione del Veneto è basato su un approccio a fasi per consentire che tutti i servizi siano implementati e gestiti in modo efficace ed efficiente.

In particolare, il modello prevede le seguenti fasi:

- Attivazione: tale fase prevede l'ingaggio dei singoli Enti, la valutazione del gruppo di appartenenza per ciascuno di essi, tenuto conto anche di eventuali specificità che rendano indispensabile una deroga al modello standard, le attività preliminari necessarie alla definizione del perimetro di intervento e dei servizi da erogare.
- Configurazione: una volta definito il perimetro di intervento, tale fase prevede l'esecuzione di tutte le attività tecniche necessarie all'attivazione del servizio (ingaggio fornitori, configurazioni tecniche e fine tuning, verifiche e test pre-avvio del servizio, avvio del servizio).
- Erogazione: infine, una volta terminate le attività di configurazione l'ultima fase è relativa all'erogazione del servizio, inclusiva delle attività di manutenzione ed evoluzione dello stesso, al fine di garantire un servizio in linea alle esigenze del singolo Ente e di Regione del Veneto.

**Articolo 5 - Modello di governo**

Il modello organizzativo del CERT di Regione del Veneto sarà organizzato su tre livelli di Governo che identificano gli attori principali ed i relativi ruoli per lo sviluppo e l'operatività del CERT stesso. Tale modello definisce le relazioni tra Il CERT di Regione del Veneto, gli aderenti (enti locali), le Istituzioni nazionali (CSIRT Italiano e altri CERT di settore) e le istituzioni internazionali. In particolare:

- livello STRATEGICO: composto dal Comitato Strategico del CERT Regionale, è responsabile di fornire un indirizzo strategico sulle politiche di conduzione del CERT Regionale e costituisce un punto decisionale per l'escalation di incidenti gravi verso le autorità competenti; è presieduto da un referente di Regione del Veneto - che ne è il Presidente -, da referenti degli enti aderenti (GRUPPI 1 & 2 e Consiglio Regionale) e dalle istituzioni ed autorità nazionali in termini di sicurezza nazionale cibernetica (i.e. ACN e Polizia Postale).
- livello DIRETTIVO: composto dal Comitato Direttivo del CERT Regionale, è responsabile di indirizzare la strategia, definendo processi e procedure che garantiscano il raggiungimento degli obiettivi prefissati, avvalendosi di esperti di Cybersecurity ed interloquendo con le istituzioni/organizzazioni nazionali; è presieduto dal Responsabile del CERT Regionale e da rappresentanti con ruoli di Responsabili della Sicurezza Informatica/Responsabili Sistemi Informativi (CISO/CIO) degli enti aderenti (GRUPPI 1 & 2 e Consiglio Regionale), coadiuvato da un team di esperti di cybersecurity.



- livello OPERATIVO: composto dai referenti di sicurezza degli Enti locali aderenti è responsabile dell'implementazione e della manutenzione dei processi e delle procedure definite a livello direttivo; è presieduto dalle risorse che indirizzano le tematiche di sicurezza all'interno del singolo ente aderente (GRUPPI 1, 2, 3, 4, 5) e di Regione del Veneto.

Regione del Veneto, con Decreti del Direttore della Direzione ICT e Agenda Digitale, provvederà alla costituzione dei due Comitati.

#### Articolo 6 – Obblighi in capo alle parti

La realizzazione concreta del CERT regionale si informa al principio di “leale collaborazione”.

Gli Enti aderenti si obbligano a rispettare i requisiti di ammissione di cui al precedente art. 2 ed a svolgere le attività di cui all'art. 3.

Nel progetto esecutivo approvato con D.G.R. n....., allegato alla presente Convenzione, sono indicati e descritti i servizi a cui l'Ente aderirà e i relativi obblighi di implementazione e, tenendo in considerazione gli obiettivi minimi che gli enti dovranno raggiungere a seguito della costituzione del CERT Regionale, come da linee guida AGID e Direttiva NIS 2.

#### Articolo 7 – Durata della convenzione

La durata della presente Convenzione è fissata in anni (max 3 anni) a decorrere dalla data di sottoscrizione, con possibilità di rinnovo al termine attraverso accordo scritto fra le Parti.

#### Articolo 8 – Spese ed oneri

Con la presente Convenzione l'Ente..... aderisce al CERT di Regione Veneto per ... anni.

Qualora l'adesione avvenga coincidentemente con il primo anno di attività del CERT l'Ente non afferente l'Area Sanità e Sociale non sosterrà i costi per i primi 12 mesi.

Per gli anni successivi i costi per l'Ente ..... sono quelli indicati nel progetto esecutivo in funzione dei servizi selezionati nell'allegato tecnico.

#### Art. 9 - Referenti

Per il necessario rapporto tra la Regione del Veneto - Direzione ICT e Agenda Digitale e la Controparte, richiesto ai fini dell'applicazione della presente Convenzione, sono nominati i seguenti 2 referenti:

- Per la Regione del Veneto - Direzione ICT e Agenda Digitale: .....
- Per l'Ente .....

#### Articolo 10 - Trattamento dei dati personali

La Direzione ICT e Agenda Digitale nell'ambito dell'esecuzione delle attività inerenti il CERT regionale, si qualifica come **Responsabile del Trattamento**, ai sensi dell'Art. 28 del GDPR, al fine di supportare gli Enti aderenti (**Titolari del trattamento**) nel mettere in atto misure di sicurezza tecniche e organizzative volte ad assicurare l'applicazione del GDPR e per garantire livelli di sicurezza adeguati a valutare e ridurre i rischi derivanti dal trattamento dei dati di competenza.

Nel contesto del CERT Regionale, a titolo esemplificativo ma non esaustivo, gli **Interessati al Trattamento** dei dati personali saranno dunque:



- I destinatari dei servizi erogati agli Enti.
- Gli incaricati al trattamento, ossia i dipendenti degli Enti.

Il trattamento dei dati risponde alla seguente finalità:

- Svolgere un compito di interesse pubblico in quanto collegato all'esercizio di pubblici poteri. In questo caso si fa riferimento alla costituzione del CERT Regionale e all'**erogazione dei servizi di interesse per gli Enti aderenti**.

Si specifica che:

- I dati personali oggetto dei trattamenti saranno trattati limitatamente al tempo necessario per perseguire le finalità dei trattamenti, fermo restando il periodo di tempo eventualmente previsto dalle relative normative di settore.
- I dati personali saranno trattati nel territorio Europeo: in nessun caso è previsto il trasferimento degli stessi fuori dai confini dell'Unione europea.

Tra le parti (Titolare del trattamento e Responsabile del trattamento) sarà formalizzato un contratto o altro atto giuridico (nomina Responsabile del trattamento) che vincoli il Responsabile del trattamento al Titolare del trattamento. Sarà inoltre formalizzato un contratto tra il CERT di Regione del Veneto (Responsabile del trattamento) e i fornitori (Sub-responsabili del Trattamento) dei servizi che saranno coinvolti negli ambiti di intervento del CERT.

Si riportano di seguito, a titolo esemplificativo ma non esaustivo, le attività che le parti in gioco dovranno eseguire per assicurare il rispetto dei regolamenti sulla privacy.

#### **Azioni di adeguamento in carico al CERT (Responsabile del Trattamento):**

1. Considerato l'oggetto, il contesto e le finalità dei trattamenti, può collaborare con il titolare dei dati alla valutazione d'impatto sulla protezione dei dati al fine di valutare eventuali rischi per i diritti e le libertà delle persone fisiche interessate nel rispetto dell'Art. 35 del GDPR.
2. In caso di utilizzo di Fornitori Esterni (Sub-responsabili) ha la responsabilità della scelta in termini di idoneità delle misure di sicurezza.
3. Aggiorna il proprio registro dei trattamenti in qualità di Responsabile del trattamento.
4. Adotta adeguati standard di sicurezza in termini di protezione dei dati, ai sensi dell'Articolo 32 del GDPR.
5. Nomina e istruisce adeguatamente tutti gli incaricati che agiscono per suo conto.
6. Stipula un idoneo atto giuridico che lo vincoli ai sub-responsabili in termini di protezione dei dati, ai sensi dell'articolo 28 del GDPR.

#### **Azioni di adeguamento per l'Ente partecipante al CERT (Titolare del trattamento):**

1. Con l'atto di sottoscrizione della Convenzione ivi prevista, esprime atto di accettazione alla nomina della Direzione ICT e Agenda Digitale, nell'ambito delle funzioni gestite dal servizio CERT regionale, a Responsabile del trattamento, ai sensi dell'Art. 28 del GDPR.
2. Aggiorna i registri delle attività di trattamento per il rispetto dell'Art. 30 del GDPR.
3. Predisporre una eventuale valutazione d'impatto se prevista ai sensi dell'Art. 35 del GDPR.
4. Nomina e istruisce adeguatamente tutti gli incaricati che agiscono per suo conto.

#### **Articolo 11 – Norme regolatrici**



Per quanto non espressamente disciplinato nella presente convenzione si applicano le norme del codice civile e le ulteriori eventuali disposizioni di settore compatibili.

**Articolo 12- Divieto di cessione della convenzione**

È fatto espresso divieto alle Parti di trasferire a terzi (in tutto o in parte) i diritti contemplati nella presente Convenzione operativa, a pena di risoluzione della medesima.

**Articolo 13 – Registrazione**

Le Parti convengono che la presente Convenzione sia oggetto di registrazione solo ed esclusivamente in caso d’uso, con tutte le spese a carico del richiedente, ai sensi dell’art. 5, 2° comma, del D.P.R. n. 131/1986. Le spese di bollo della presente Convenzione sono a carico della Controparte.

**Articolo 14- Foro competente**

Le Parti s’impegnano a risolvere tutte le controversie che dovessero comunque insorgere tra loro in dipendenza della presente Convenzione innanzi al Tribunale Amministrativo Regionale per il Veneto con sede a Venezia.

**Articolo 15 - Comunicazioni**

Ogni comunicazione connessa all’esecuzione della presente convenzione dovrà essere inviata rispettivamente ai seguenti indirizzi:

- Per la Regione: Direzione ICT e Agenda Digitale: Via Pacinotti n. 4– 30172 Marghera Venezia [ictagendadigitale@pec.regione.veneto.it](mailto:ictagendadigitale@pec.regione.veneto.it)
- ....

Le parti, previa lettura del presente atto, lo confermano in ogni sua parte e lo sottoscrivono a tutti gli effetti.

Per Regione del Veneto

Per ....

Il Direttore della Direzione ICT e  
Agenda Digitale

Il Legale Rappresentante

.....

.....

Allegato

Tecnico

ENTE:.....

GRUPPO ENTE:

SERVIZI RICHIESTI:





Ambiti di Intervento	Breve descrizione	Adesione (SI/NO)
<b>Gestione del Rischio</b>	Linee Guida + Assessment + Report	
<b>BC/DR</b>	Linea Guida + Predisposizione Template + Assessment + Report	
<b>Sensibilizzazione e formazione</b>	Piattaforma + (Custom x G1)	
<b>Altri servizi</b>	Vari	
<b>SOC/ Incident management</b>	HyperSOC per G1 e G2 - SOC G3,4,5	
<b>Vulnerability management</b>	Gestione Continua delle Vulnerabilità	
	Penetration Testing	
<b>Threat intelligence</b>	Piattaforma	
<b>Sviluppo sicuro / Analisi del codice</b>	Linea Guida + SAST DAST	
<b>Governo dell'erogazione dei Servizi</b>		

data e firma

