REGIONE DEL VENETO
ULSS7 PEDEMONTANA
Via dei Lotti, n. 40
36061 Bassano del Grappa (VI)
Codice fiscale e partita IVA 00913430245

N. 1790 DEL 24/10/2023

DELIBERAZIONE
del

DIRETTORE GENERALE

Nominato con D.P.G.R. n. 26 del 26/02/2021

Coadiuvato dai sigg.:

DIRETTORE AMMINISTRATIVO dott.ssa MICHELA CONTE

DIRETTORE SANITARIO dr. ANTONIO DI CAPRIO

DIRETTORE DEI SERVIZI SOCIO – SANITARI dott. EDDI FREZZA

OGGETTO: PROGETTO COMPUTER EMERGENCY RESPONSE TEAM (CERT) REGIONALE. ADESIONE E APPROVAZIONE SCHEMA DI CONVENZIONE CON REGIONE DEL VENETO.

IL DIRETTORE GENERALE
DELL'AZIENDA ULSS 7 PEDEMONTANA
dott. Carlo Bramezza

Documento informatico firmato digitalmente ai sensi del D. Lgs n. 82/2005, del T.U. n. 445/2000 e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa; il documento informatico è conservato digitalmente negli archivi informatici dell'Azienda.

Proponente: UOC AFFARI GENERALI
Anno Proposta: 2023 Numero Proposta: 1893/23

Il Direttore dell'U.O.C Affari Generali nonché Responsabile del procedimento, attesta che la presente proposta di deliberazione è stata regolarmente istruita nel rispetto della vigente normativa nazionale, regionale e regolamentare: f.to Cristiano Galizian

---

Il Direttore dell'UOC Affari Generali relaziona quanto segue.

Premesso che:

- con D.G.R. n. 1174 del 27.09.2022, la Regione del Veneto ha approvato il progetto del CERT (Computer Emergency Response Team) Regionale;
- 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;

Preso atto che con il medesimo provvedimento è stata demandata alla Direzione regionale ICT e Agenda Digitale la progettazione esecutiva di tale CERT Regionale;

Vista la D.G.R. n. 1024 del 22/08/2023, con la quale la Regione del Veneto ha approvato il progetto esecutivo del CERT regionale insieme allo schema di convenzione per l'adesione dei vari Enti regionali veneti al CERT regionale;

Considerato che la deliberazione n. 1024 citata esplicita che:

- 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 opera 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;
- la Regione Veneto, 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 Regolamento Europeo sul trattamento dei dati (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;

Considerato che questa iniziativa rappresenta una mitigazione dei rischi della sicurezza informatica dell'azienda (dati, procedure, modelli di qualità...) e rilevata la necessità dell'implementazione dei servizi forniti dal progetto regionale a fronte dei sempre maggiori rischi della sicurezza *cyber*;

Vista la nota prot.n. 89336/23 in data 24/10/2023, con la quale il Direttore UOC Sistemi Informativi ha valutato necessario che l'Azienda ULSS 7 Pedemontana aderisca al predetto progetto e ha proposto di sottoscrivere lo schema di convenzione per l'adesione al CERT regionale e gli acclusi allegati, progetto esecutivo (all. 1), allegato tecnico contemplante i servizi richiesti (all. 2), atto di nomina a Responsabile del trattamento dei dati personali (all. 3)

Considerato che – come stabilito dall'art. 8 della convenzione – per gli Enti afferenti all'Area Sanità e Sociale i costi saranno sostenuti da risorse Regionali derivanti dai capitoli di spesa in capo all'Area Sanità e Sociale, così come definito dalla DGR 1024/2023;

Per quanto sopra esposto, il Direttore dell'UOC Affari Generali propone di

- aderire al progetto Computer Emergency Response Team (CERT) regionale;
- approvare, come parte integrante della presente deliberazione, lo schema di convenzione per l'adesione al CERT regionale e gli acclusi allegati progetto esecutivo (all. 1), allegato tecnico contemplante i servizi richiesti (all. 2), atto di nomina a Responsabile del trattamento dei dati personali (all. 3);
- dare atto che i costi saranno sostenuti da risorse Regionali derivanti dai capitoli di spesa in capo all'Area Sanità e Sociale, così come definito dalla DGR 1024/2023.

IL DIRETTORE GENERALE

Vista la relazione e la proposta del Responsabile del procedimento;

Dato atto che il responsabile dell'U.O. competente ha attestato l'avvenuta regolare istruttoria della pratica, in ordine alla compatibilità con la vigente legislazione statale, regionale e regolamentare;

Acquisito il parere favorevole dei Direttori Amministrativo, Sanitario e dei Servizi Socio-Sanitari, per quanto di rispettiva competenza;

DELIBERA

1. di aderire, per le motivazioni esposte in premessa, al progetto Computer Emergency Response Team Regionale – CERT – approvato con la D.G.R. n. 1024 del 22/08/2023 avente l'obiettivo di coordinare, supportare e monitorare le attività di prevenzione, risposta e ripristino degli incidenti critici di tipo *cyber*;

2. di approvare e sottoscrivere lo schema di convenzione tra Regione del Veneto – Direzione ICT e Agenda Digitale e Azienda ULSS 7 Pedemontana e i relativi allegati progetto esecutivo (all. 1), allegato tecnico contemplante i servizi richiesti (all. 2), atto di nomina a Responsabile del trattamento dei dati personali (all. 3) parti integranti della presente deliberazione;

3. di dare atto che la durata della convenzione è di tre anni dalla data della sottoscrizione;

4. di dare atto che la convenzione non comporta costi per l'Azienda;

5. di incaricare l'U.O. proponente di pubblicare la presente deliberazione nella sezione Amministrazione Trasparente del sito istituzionale, ai sensi dell'art. 23 del D. Lgs. 14.3.2013 n. 33;

6. di dare atto che la presente deliberazione viene pubblicata all'albo del sito istituzionale dell'Azienda per 10 gg. continuativi, inviata contestualmente al Collegio Sindacale, e diventa esecutiva il giorno stesso della sua pubblicazione, come da norma regolamentare approvata con deliberazione n. 1386 del 22.7.2022.

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. Idelfo Borgo, domiciliato per la sua carica presso la sede dell'Ente,

E

Azienda ULSS 7 Pedemontana, con sede in Bassano del Grappa, Via dei Lotti, 40, (C.F. 00913430245), rappresentata dal Direttore Generale dott. Carlo Bramezza in qualità di Legale Rappresentante, d'ora in poi "*l'Ente*",

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. 1024 del 22/08/2023, 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;
- con deliberazione n. in data l'Azienda ULSS 7 Pedemontana ha approvato l'adesione al progetto CERT regionale e lo schema della presente convenzione e relativi n. 3 allegati;
- 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
GRUPPO 1	Grande	SI	Avviato	Alto	14	▪ RVE ▪ Azienda Zero ▪ ULSS / AA.OO. / IOV
GRUPPO 2	Grande	SI	Avviato	Medio	3	▪ Arpav ▪ Avepa ▪ Veneto Lavoro
GRUPPO 3	Medio	SI	Avviato	Medio	3	▪ Consiglio Veneto ▪ Infrastrutture Venete/Sistemi Territoriali ▪ Veneto Strade Spa
GRUPPO 4	Medio	SI	Definito	Medio	11	▪ A.T.E.R. PD, TV, VR, VE, BL RO, VI ▪ ESU PD, VE, VR ▪ Veneto Agricoltura
GRUPPO 5	Piccolo	NO	Considerato	Basso	8	▪ 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 ▪ Ente Parco Regionale della Lessinia

Sulla base di quanto sopra, l'Ente fa parte del gruppo n. 1.

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:
    a. presenza di un registro aggiornato degli asset infrastrutturali (FW, Server / Client) in perimetro;
    b. presenza di un registro aggiornato degli asset applicativi in perimetro;
    c. presenza di soluzioni di Backup ad intera copertura dei sistemi e strumenti in uso dalle funzioni organizzative;
    d. presenza di un Active Directory;
    e. presenza di soluzioni di antivirus non deprecati (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 nel Sig. Botter Mirco.

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 (Allegato 1).

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. 1024 del 22/08/2023, allegato alla presente Convenzione (Allegato 1), sono indicati e descritti i servizi a cui l'Ente aderirà e i relativi obblighi di l'implementazione, 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 tre 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 tre 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 (Allegato 2).
Per gli Enti afferenti all'area Sanità e Sociale i costi saranno sostenuti da risorse Regionali derivanti dai capitoli di spesa in capo all'Area Sanità e Sociale come definito con DGR 1024/2023.

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: Ing. Paolo Barichello

• Per l'Ente: Dott. Federico Thiella.

Articolo 10 – Trattamento dei dati personali

La Regione Veneto, con indicazione quale Delegato ai sensi della Deliberazione della Giunta Regionale del Veneto n. 596 dell'8 maggio 2018, della 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, come disciplinato dall'Allegato 3 che costituisce parte integrante della presente convenzione e sottoscritto dalle parti.

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, salva la diversa competenza attribuita per legge in relazione alla disciplina sulla protezione dei dati personali.

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*

- Per l'Ente: Azienda ULSS 7 Pedemontana, Via dei Lotti, 40 – 36061 Bassano del Grappa (VI) protocollo.aulss7@pecveneto.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

Il Direttore della Direzione ICT e Agenda Digitale

……....

Per Azienda ULSS 7 Pedemontana

Il Direttore Generale
Dott. Carlo Bramezza

……..

REGIONE DEL VENETO

Regione del Veneto

Direzione ICT e Agenda Digitale

<Progetto ESECUTIVO CERT Regionale
(Computer Emergency Response Team)
di Regione del Veneto >

Progetto Esecutivo

Versione **<1.3>**

Modello documento
Progetto ESECUTIVO CERT Regionale di Regione del Veneto 1.3

SOMMARIO

1 PROVAZIONI

Attività	Nominativo	Azienda	Tel.	e-Mail
Redazione				
Verifica				
Approvazione				

2 LISTA DI DISTRIBUZIONE

Nominativo	Azienda	Tel.	e-Mail	Tipo
Idelfo Borgo				
Paolo Barichello				
Giuseppe Mendola				
Francesco Clemente				
Matteo Scarpa				

Tipo: CC=Copia Controllata, PC=Per conoscenza

3 STORIA DELLE MODIFICHE

Versione	Data	Descrizione
0.0	30.03.2023	Prima stesura
1.0	29.05.2023	Prima versione
1.1	07.06.2023	Integrazione della Prima versione
1.2	24.07.2023	Integrazione della Modalità di adesione e partecipazione
1.3	26.07.2023	Semplificazione capitolo 13 sul Trattamento dei dati personali

4 RIFERIMENTI

N.	Titolo	Autore	Versione	Data

5 COPYRIGHT

6 PREMESSA

6.1 Introduzione

Il presente documento ha lo scopo di descrivere il progetto esecutivo CERT Regionale (Computer Emergency Response Team) di Regione del Veneto.
Il progetto è stato definito attraverso una prima attività di analisi che ha permesso l'individuazione dei servizi inclusi nella soluzione di CERT Regionale.
Nella prima parte del documento viene descritto il nuovo contesto in cui le organizzazioni si trovano ad operare, caratterizzato dall'insorgenza di nuovi rischi di cybersicurezza e dalla crescita della complessità tecnico-organizzativa delle misure per fronteggiarli, i quali hanno reso necessaria la valutazione della costituzione del CERT Regionale.
Nella seconda parte del documento sono stati definiti i ruoli, le responsabilità e le modalità di funzionamento del modello organizzativo proposto, dei processi di attivazione e coordinamento per la gestione di eventuali incidenti di sicurezza, nonché le tempistiche di attuazione, le regole ed i costi di gestione annuali, i modelli di adesione e di partecipazione alla spesa.

6.2 Contesto di riferimento e sua evoluzione

> *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.*
> «L'Assessore Francesco Calzavara, di concerto con l'Assessore Manuela Lanzarin»

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.
Negli ultimi tempi si è inoltre assistito a una sempre maggiore sofisticazione e complessità degli attacchi informatici, rivolti sia al cittadino ma anche verso i sistemi e le infrastrutture degli enti locali con particolare attenzione alle strutture sanitarie e ospedaliere, che con l'intensificarsi del processo di digitalizzazione, se da un lato facilita il lavoro del personale, dall'altro espone l'intera rete ad attacchi.
La crescente consapevolezza del rischio digitale si è tradotto in un consistente corpus regolatorio, normativo e di indirizzo strategico prodotto da diversi organismi regionali, nazionali, ed europei che richiedono e indirizzano una corretta gestione del rischio Cyber.

6.2.1 La strategia italiana per la cybersicurezza

Il fatto che la sicurezza di dati, reti e informazioni sia un obiettivo strategico oramai non più di interesse per una singola azienda, amministrazione o settore, ma di dominio nazionale e

internazionale è ben noto alle Istituzioni di riferimento, come testimoniato dal recente fermento normativo in materia e dalla nascita dell'Agenzia per la Cybersicurezza Nazionale.
Prendendo le mosse dalle iniziative avviate nelle more del quadro strategico nazionale per la protezione dello spazio cibernetico, unitamente alle nuove necessità di segnalazione degli incidenti di sicurezza che provengono dalla regolamentazione di settore, è emersa l'opportunità di valutare nuove modalità cooperative per rafforzare ulteriormente la cultura della cybersecurity in ambito regionale, in termini di maggior consapevolezza dei fenomeni cyber, creazione di una conoscenza condivisa e sviluppo e costruzione di competenze specialistiche.
Il recente documento emanato dall'Agenzia per la Cybersicurezza Nazionale di Strategia Nazionale di Cybersicurezza 2022-2026 delinea tre obiettivi fondamentali (Protezione, Risposta, Sviluppo) da raggiungere entro il 2026 ed è accompagnato da un Piano di implementazione composto da 82 Misure. In particolare: nel Documento di strategia, l'obiettivo "Risposta" definisce, per una risoluzione quanto più tempestiva e risolutiva agli interventi a fronte di incidenti, la nascita della rete dei CERT/CSIRT locali (CERT: Computer Emergency Response Team; CSIRT: Computer Security Incident Response Team) facenti parte della rete Nazionale del CSIRT.
Nel Piano di implementazione delle 82 Misure, 17 sono le Misure in cui le Regioni sono tra i soggetti responsabili dell'attuazione. Di queste si evidenzia la Misura #30, che prevede di "Realizzare un sistema di raccolta e analisi HyperSOC per aggregare, correlare ed analizzare eventi di sicurezza di interesse al fine di individuare precocemente eventuali "pattern" di attacco complessi, nonché abilitare una gestione del rischio cyber in chiave preventiva e integrata tra molteplici sorgenti dati, sfruttando anche infrastrutture di High Performance Computing e tecnologie di Intelligenza Artificiale e il machine learning."

6.2.2 Regolamenti, Direttive, standard e linee guida

Di seguito si riportano le principali iniziative europee, nazionali e regionali finalizzate a definire il quadro normativo e la strategia comunitaria di difesa digitale:

- Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile disciplina il modo in cui aziende e organizzazioni devono trattare i dati personali dei cittadini.
- La direttiva NIS 2 introduce misure più stringenti e specifiche in termini di cyber risk management, di segnalazione e condivisione delle informazioni relative agli incidenti di sicurezza.
- Il regolamento (UE) 2017/745 stabilisce le norme relative i dispositivi medici per uso umano e degli accessori per tali dispositivi nell'Unione. L'obiettivo del regolamento è garantire un elevato livello di protezione della salute dei pazienti e degli utilizzatori. Per conseguire questi obiettivi, il regolamento stabilisce un sistema più solido di valutazione della conformità per garantire la qualità, la sicurezza e le prestazioni dei dispositivi immessi sul mercato dell'UE.
- Con DGR 1184 del 14/08/2019 è stato approvato l'Accordo di collaborazione per la crescita e la cittadinanza Digitale stipulato tra Regione del Veneto, AGID e l'Agenzia per la Coesione Territoriale, che, tra gli interventi da realizzare, prevede lo sviluppo di un CERT Regionale a supporto della PA della Regione del Veneto.
- Con DGR 156 del 22/02/2022 la Regione del Veneto ha adottato la nuova Agenda Digitale che delinea le strategie dei prossimi 3 anni per la trasformazione digitale della Regione del Veneto, tra le quali si individua anche l'obiettivo di "istituire un'agenzia di sicurezza informatica su base regionale a favore della collaborazione tra Enti pubblici e privati per una gestione condivisa del rischio a livello regionale".
- Il Security Incident Management Maturity Model, chiamato anche SIM3 fornisce uno standard e un'indicazione di quanto bene un gruppo governa, documenta, svolge e misura la propria funzione di CSIRT.
- Infine, Agid ha rilasciato nella primavera del 2019, il documento in consultazione "Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT

regionali" che raccoglie il testo delle Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali, disponibile per la consultazione pubblica.

6.3 Obiettivi del progetto esecutivo

Tramite la Deliberazione della Giunta Regionale n. 1174 del 27/09/2022 è stato approvato il progetto del CERT (Computer Emergency Response Team) Regionale ed è stato dato il mandato della sua esecuzione alla **Direzione ICT e Agenda Digitale**. L'obiettivo è di definire un CERT regionale 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 ed 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.

6.4 Metodologia di lavoro

Il progetto ha previsto un **approccio progressivo** costituito da due fasi principali, quella di **analisi** del livello di maturità di sicurezza degli enti coinvolti e del grado di interesse degli enti rispetto ai possibili servizi offerti dal CERT e quella di **elaborazione** del progetto esecutivo.
Attraverso tale approccio si è cercato di avere un quadro chiaro e consolidato del contesto di partenza per poter definire un modello organizzativo ed operativo in linea con le esigenze e stilare una lista di servizi da includere nel CERT per stabilire una roadmap implementativa che preveda di **erogare rapidamente i primi servizi** ad alcuni Enti e successivamente **estendere il perimetro** di Enti coinvolti ed i servizi disponibili.
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 sottolinea la necessità di avviare una collaborazione tra Enti Pubblici e Privati per una gestione condivisa del rischio informatico a livello regionale.
Per la prima fase di analisi e definizione del progetto esecutivo sono stati individuati 26 Enti, in particolare:

- **Enti pubblici regionali strumentali (Quota Regione del Veneto 100%)**:
    1. A.T.E.R. Bl
    2. A.T.E.R. Pd

3. A.T.E.R. Ro
4. A.T.E.R. Tv
5. A.T.E.R. Ve
6. A.T.E.R. Vi
7. A.T.E.R. Vr
8. Agenzia Veneta Per L'innovazione Del Settore Primario "Veneto Agricoltura"
9. Arpav
10. Avepa
11. Ente Parco Naturale Regionale Del Fiume Sile
12. Ente Parco Regionale Dei Colli Euganei
13. Ente Parco Regionale Del Delta Del Po
14. Ente Regionale Veneto Lavoro
15. Azienda Regionale Per Il Diritto Allo Studio Universitario Di Padova - Esu Pd
16. Azienda Regionale Per Il Diritto Allo Studio Universitario Di Venezia - Esu Ve
17. Azienda Regionale Per Il Diritto Allo Studio Universitario Di Verona - Esu Vr
18. Istituto Regionale Per Le Ville Venete

- **Società a partecipazione regionale maggioritaria (Quota Regione del Veneto maggioritaria)**
  19. Veneto edifici monumentali (ex. Immobiliare Marco Polo Srl)
  20. Sistemi Territoriali Spa
  21. Infrastrutture Venete Srl
  22. Veneto Acque Spa
  23. Veneto Innovazione Spa
  24. Veneto Strade Spa

- **Altri Enti Regionali**
  25. Consiglio Veneto
  26. Azienda Zero.
      - AULSS 1 Dolomiti
      - AULSS 2 Marca Trevigiana
      - AULSS 3 Serenissima
      - AULSS 4 Veneto Orientale
      - AULSS 5 Polesana
      - AULSS 6 Euganea
      - AULSS 7 Pedemontana
      - AULSS 8 Berica
      - AULSS 9 Scaligera
      - AOPD (Azienda Ospedaliera Università Padova)
      - AOVR (Azienda Ospedaliera Universitaria Integrata Verona)
      - IOV (Istituto oncologico Veneto)

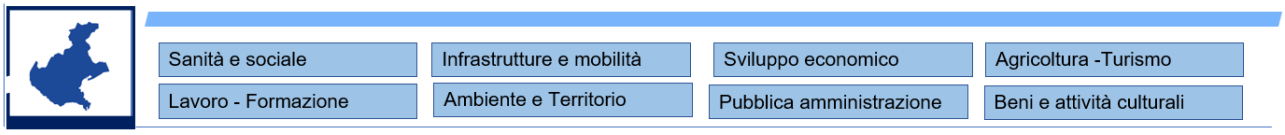


Figura 1 – Gli ecosistemi della Regione del Veneto coinvolti nel progetto di CERT Regionale

7 ANALISI PRELIMINARE E RELATIVI RISULTATI

Per poter definire gli ambiti di intervento prioritari per la definizione del CERT Regionale, sono state considerate ed analizzate le evidenze raccolte durante la fase di analisi relativamente all'organizzazione della cybersecurity, ai processi e servizi, ai sistemi e strumenti in uso nonché ai bisogni degli enti emersi dalle attività di analisi svolte.
Dalle attività di verifica sono emerse le seguenti considerazioni e punti di attenzione di carattere generale:

- Un numero piuttosto limitato di risorse atte a gestire le tematiche di Sicurezza ed in generale facenti parte della Struttura ICT.
- Un basso livello di maturità relativamente alle tematiche di Sicurezza.
- Assenza di un modello uniforme di Governance della Cybersecurity, per la gestione del Rischio.
- Attività di operation legate alla cybersecurity principalmente demandate a fornitori esterni.
- Adozione in larga parte di soluzioni tecnologiche valide, sebbene non omogenee tra ente ed ente.
- Consapevolezza da parte dei referenti dei singoli enti delle tematiche di cybersecurity, che portano avanti un corretto presidio dei diversi processi, tuttavia, emerge l'importanza di attuare modelli di coordinamento e di servizio tipici di un CERT (Computer Emergency Response Team), inclusivo di un HyperSOC (Security Operation Center) che possano monitorare la sicurezza e gestire gli incidenti a livello regionale.

In particolare, nel seguito si riporta quanto emerso per lo specifico ambito di analisi preso in considerazione:

- **Organizzazione della cybersecurity**
  - Assenza di una strategia uniforme per la gestione del rischio (IT-Cyber, Privacy, Gestione Fornitori) e dei criteri di accettazione, mitigazione e trasferimento del rischio.
  - Assenza di un modello di Governance della Cybersecurity (framework di lavoro) unico e omogeneo.
  - Assenza o presenza parziale di un framework documentale (Policy, Processi e Procedure).

- **Processi e servizi di cybersecurity**
  - Parziale presenza o assenza di una strategia di Business Continuity e Disaster Recovery omogenea per i servizi erogati dai vari Enti.
  - Parziale capacità di ripristinare secondo un piano e metriche definite, dati e servizi a seguito di un incidente di sicurezza o un Data Breach.
  - Potenziale inefficacia nel coordinamento e nella gestione del processo di comunicazione e notifica a seguito di un evento di crisi.
  - Parziale o assente copertura del monitoraggio di sicurezza (principalmente fuori orario lavorativo).
  - Parziale presenza o assenza di una soluzione di Governance per il Vulnerability Management ed il Patch Management.
  - Carenza nella pianificazione delle attività di Vulnerability Management (VA/PT) e nel processo di monitoraggio dei piani di rientro.
  - Parziale presenza o assenza di un piano strutturato in tema di Awareness e Training per il personale degli Enti in ambito Cybersecurity e Data Protection.
    Parziale presenza o assenza di strumenti per l'erogazione della formazione e la verifica del livello di preparazione del personale.

- **Sistemi e strumenti in uso**
  - Parziale presenza o assenza di un sistema di monitoraggio applicativo.

- Soluzioni antimalware eterogenee, talvolta deprecate (Kaspersky) e non sempre assicurano funzionalità avanzate EDR (sistema di sicurezza avanzato di rilevamento e risposta per gli endpoint).

- **Interesse per i servizi offerti**.
  L'interesse degli Enti risulta rivolto principalmente ai seguenti servizi:
  - Allarmi e avvisi.
  - Sensibilizzazione, istruzione e formazione.
  - Coordinamento della risposta agli incidenti.
  - Analisi e gestione delle vulnerabilità.
  - Monitoraggio applicativo.
  - Analisi del rischio.

Dall'assessment condotto ed in particolare durante la fase delle interviste dedicate, è emerso che gli enti sono disposti ad intraprendere una collaborazione con un CERT Regionale per la gestione dei servizi di cybersecurity, salvo un'efficace ed efficiente configurazione rispetto ai processi in essere nelle rispettive organizzazioni.

7.1 Definizione dei gruppi

Al fine di coadiuvare la definizione del modello organizzativo e operativo del CERT Regionale, sulla base degli esiti dell'analisi, è stato effettuato un raggruppamento degli enti coinvolti in funzione di alcuni criteri esplicitati sotto e del loro relativo peso.

In particolare, al fine di procedere al raggruppamento degli enti sono state prese in considerazione e valutate le seguenti dimensioni:
- Tipo Ente / N. di dipendenti.
- Presenza di risorse interne per la gestione IT /Cybersecurity.
- Livello di maturità di gestione della cybersecurity.
- Livello di rischio (alto, medio o basso) per dati trattati/ tipologia di servizi erogati.

Il livello di maturità, utilizzato come parametro per la classificazione degli enti, rappresenta il livello di maturità **atteso** e non è necessariamente rappresentativo del contesto attuale. Ad esempio, può prendere in considerazione anche progetti in corso, non ancora finalizzati.
I parametri utilizzati per la definizione dei gruppi non risultano esaustivi e comprensivi di tutte le casistiche possibili, per tale motivo, in caso di introduzione di un nuovo ente, quest'ultimo sarà valutato e contestualizzato dando priorità al livello di rischio. Per tale motivo sono stati definiti dei pesi per ognuna delle metriche sopra rappresentate:
- Livello di Rischio per dati trattati / tipologia di servizi erogati: **34%**
- Numero di Dipendenti: **22%**
- Livello di maturità (che nella prima fase sarà quello atteso): **22%**
- Presenza di risorse interne per la gestione dell'IT/ Cybersecurity: **22%**

In base al gruppo di riferimento, gli Enti agiranno con differenti gradi di responsabilità e compiti all'interno del modello organizzativo, come descritto nel capitolo seguente. Tuttavia, per garantire un modello efficiente, saranno considerate eventuali specificità del singolo Ente e determinate eventuali deroghe al raggruppamento standard.

22%	TIPO DI ENTE – N° Dipendenti	
Grande	➢	N° DIP > 300
Medio	➢	15 < N° DIP < 300
Piccolo	➢	N° DIP < 15

LIVELLO DI MATURITA' DI GESTIONE DELLA CYBERSECURITY	22%	
AVVIATO	➢	L'implementazione dei controlli di sicurezza si avvale di processi, procedure e soluzioni tecniche definite
DEFINITO	➢	L'implementazione dei controlli di sicurezza si avvale di processi, procedure e soluzioni tecniche parzialmente definiti
CONSIDE-RATO	➢	L'implementazione dei controlli è affidata a processi, procedure e soluzioni tecniche con risultati non prevedibili, non documentati, non organizzati e spesso eseguiti su richiesta

22%	RISORSE INTERNE PER LA GESTIONE IT / CYBER	
SI	➢	Sono presenti delle risorse demandate alla gestione IT
No	➢	La gestione delle risorse IT è demandata a fornitori esterni

LIVELLO DI RISCHIO PER DATI TRATTATI/ TIPOLOGIA DI SERVIZI EROGATI	34%	
ALTO	➢	Livello di rischio Alto per il tipo di dati trattati/ tipologia di servizi erogati
MEDIO	➢	Livello di rischio Medio per il tipo di dati trattati/ tipologia di servizi erogati
BASSO	➢	Livello di rischio Basso per il tipo di dati trattati/ tipologia di servizi erogati

Figura 2 – Metriche per la definizione dei gruppi di appartenenza degli Enti

	Tipo di Ente	Risorse Interne IT	Livello di Maturità	Livello di Rischio	N° Enti	Enti
GRUPPO 1	Grande	SI	Avviato	Alto	1	▪ Azienda Zero
GRUPPO 2	Grande	SI	Avviato	Medio	3	▪ Arpav ▪ Avepa ▪ Veneto Lavoro
GRUPPO 3	Medio	SI	Avviato	Medio	3	▪ Consiglio Veneto ▪ Infrastrutture Venete/Sistemi Territoriali ▪ Veneto Strade Spa
GRUPPO 4	Medio	SI	Definito	Medio	12	▪ A.T.E.R. PD, TV, VR, VE, BL RO, VI ▪ ESU PD, VE, VR ▪ Veneto Agricoltura
GRUPPO 5	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

Figura 3 – Gruppi afferenti al CERT Regionale

8 PROGETTO ESECUTIVO DI CERT REGIONALE

Per la definizione del Progetto esecutivo di CERT Regionale si rende necessaria l'identificazione di un modello di governo, dei principali ruoli e responsabilità degli attori coinvolti nonché l'individuazione e caratterizzazione dei servizi inclusi e del relativo modello operativo.
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.
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. Infatti, il perimetro del CERT Regionale potrà essere modificato con l'inclusione progressiva di nuovi enti che ne facciano richiesta.
I servizi erogati dal CERT Regionale sui 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**: 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.

Come sopra anticipato e descritto in dettaglio nei capitoli seguenti, 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 perimetro considerato nel presente progetto esecutivo potrà essere riadattato sulla base di quanto anticipato sopra, ed in particolare con l'introduzione di nuovi enti o gruppi come evidenziato nella figura sottostante.

Figura 4 – Il CERT Regionale

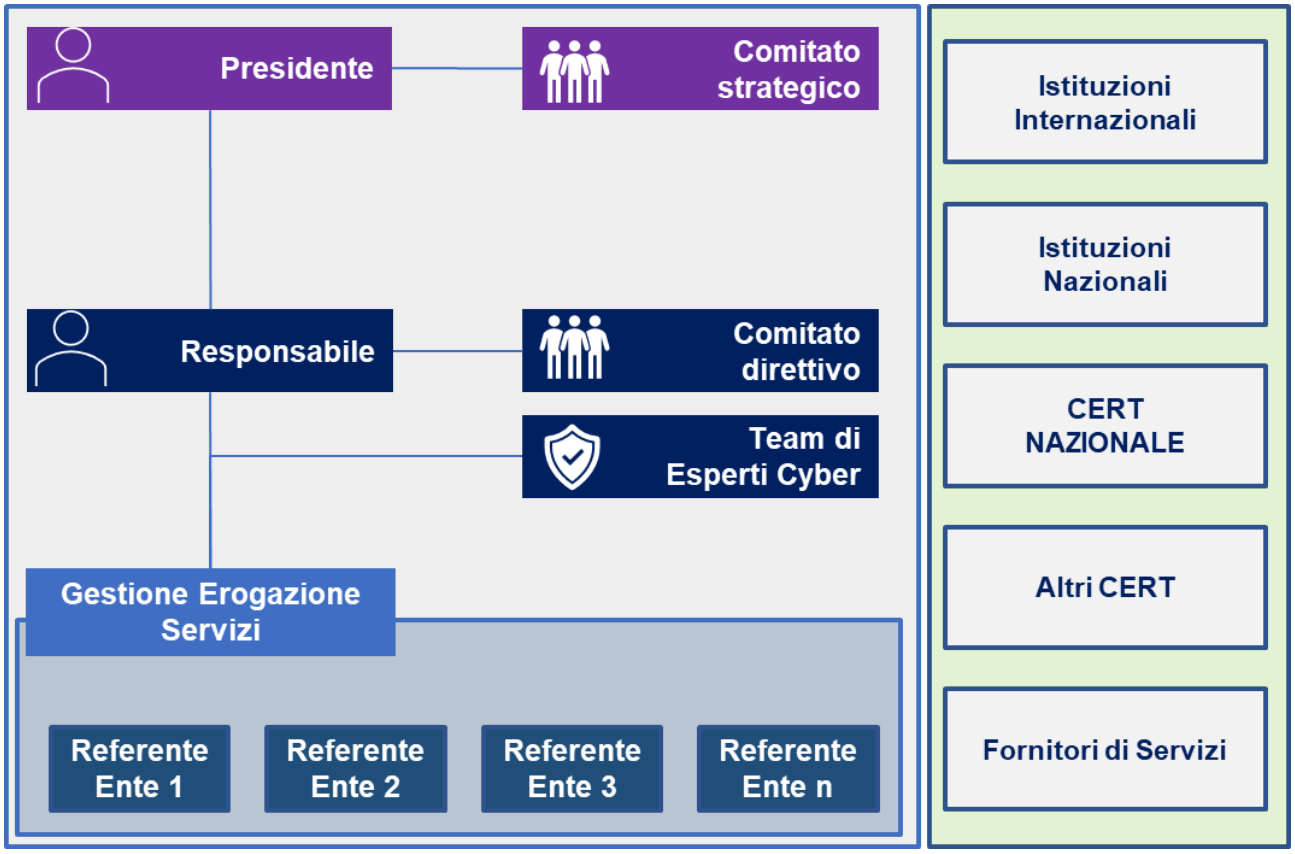
8.1 Modello Organizzativo del CERT Regionale

8.1.1 Modello di governo

La struttura organizzativa del CERT Regionale è stata definita sia sulla base della suddivisione degli enti in cinque gruppi, sia della complessità tecnica e organizzativa nella quale dovrà nascere.
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.

Figura 5 - Modello Di Governance

- **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. Il livello strategico del CERT Regionale è costituito da un referente di Regione del Veneto - che ne è il Presidente -, da referenti degli enti aderenti (GRUPPO 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. Il livello Direttivo è presieduto dal Responsabile del CERT Regionale e da un numero predefinito di 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. Il Livello Operativo è costituito dalle risorse che indirizzano le tematiche di sicurezza all'interno del singolo ente (GRUPPI 1, 2, 3, 4, 5) aderente e di Regione del Veneto.



8.1.2 Ruoli e responsabilità

Di seguito sono elencate le principali responsabilità degli attori ai diversi livelli, in coerenza con il modello di governo finalizzato all'implementazione e mantenimento del CERT Regionale.

Il **Comitato Strategico** ha ruolo di **indirizzo strategico** sulle politiche di conduzione del CERT Regionale, di approvazione del modello di adesione degli enti, nonché del modello di funzionamento dello stesso.

In particolare, il Comitato Strategico ha le seguenti responsabilità:

- Definisce ed approva le linee guida strategiche e gli obiettivi di Cyber Security.
- Definisce la governance generale, inclusa l'assegnazione dei ruoli e delle responsabilità delle diverse entità coinvolte.
- Definisce il piano strategico degli ambiti di intervento nonché le relative tempistiche di attuazione.
- Definisce la modalità di partecipazione alla spesa del CERT di Regione del Veneto.
- Approva il Piano per la Cyber Security connesso ai servizi centralizzati.

Il **Comitato Direttivo** è **responsabile dell'attuazione** di quanto definito dal Comitato Strategico. Supporta le iniziative del CERT Regionale tramite la definizione di processi e procedure, la relazione con gli enti aderenti, garantendo le risorse necessarie.

In particolare, il Comitato Direttivo ha le seguenti responsabilità:

- Definisce ed indirizza i processi e le procedure atte a realizzare la strategia definita dal Comitato strategico in linea con gli standard (ISO & NIST).
- È tenuto informato, attraverso incontri periodici delle principali minacce/ eventi/ incidenti, della loro evoluzione, delle misure di contenimento applicate e delle analisi post incidente.
- Definisce gli abilitatori tecnici/ tecnologici necessari a erogare i servizi.

Il **Comitato Operativo gestisce le attività operative** in ambito sicurezza che devono essere eseguite e manutenute localmente, con l'eventuale supporto di un gruppo di esperti di Cybersecurity.

In particolare, il Comitato Operativo ha le seguenti responsabilità:

- È responsabile dello svolgimento dei servizi che il Comitato Strategico intende indirizzare.
- Implementa le soluzioni tecnologiche necessarie ad erogare i servizi.

8.1.3 Requisiti di adesione

Di seguito sono riportati i requisiti che gli enti dovranno rispettare per poter aderire al CERT regionale, sulla base della suddivisione in gruppi descritta nel capitolo *Analisi preliminare e relativi risultati*:

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. Tale figura non dovrà necessariamente avere competenze di Security in quanto potrà essere affiancata da un esperto designato.

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 sulla base dell'assessment svolto durante la fase iniziale del progetto, 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 deprecati (e.g. Kaspersky).

3. **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. **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. **Budget** dedicato a tematiche di sicurezza per i GRUPPI (1,2,3,4,5). Per gli enti del gruppo 5, può essere previsto l'utilizzo di budget regionale a copertura di alcuni specifici servizi da concordare di volta in volta con Regione del Veneto.

Requisiti di adesione	GRUPPO 1	GRUPPO 2	GRUPPO 3	GRUPPO 4	GRUPPO 5
1. **Nomina di un Referente** per la sicurezza delle informazioni	✓	✓	✓	✓	✓
2. **Raggiungimento di un livello minimo di sicurezza**	✓	✓	✓	✓	✓
3. **Personale** dedicato alla gestione della sicurezza	✓	✓			
4. **Personale parzialmente** dedicato alla gestione della sicurezza			✓	✓	✓
5. **Budget** dedicato a tematiche di sicurezza	✓	✓	✓	✓	✓

Figura 6 – Requisiti di adesione per gruppo

8.1.4 Obiettivi a seguito della costituzione del CERT Regionale

Di seguito sono riportati gli obiettivi che gli enti dovranno raggiungere a seguito della costituzione del CERT Regionale.

1. **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.
2. **Adeguamento** alla **Direttiva NIS 2** per gli enti operanti nei **settori critici.**

8.2 Descrizione dei Servizi inclusi

Per l'identificazione dei servizi da includere all'interno del CERT Regionale si è tenuto conto degli ambiti di interesse riportati all'interno delle *Linee Guida per lo sviluppo e definizione del modello nazionale di riferimento per i CERT Nazionali* AGID e dell'elenco dei servizi CERT previsti secondo ENISA. A partire da tali liste, è stato quindi definito un catalogo di servizi suddivisi ulteriormente rispetto alle categorie definite nei paragrafi precedenti (Gestione della Qualità della Sicurezza, Servizi Reattivi, Servizi Proattivi, Gestione degli Artefatti), sulla base dell'analisi del contesto di riferimento effettuata durante la prima fase di assessment finalizzata a determinare il livello di maturità di sicurezza attuale e l'interesse di adesione da parte degli Enti.

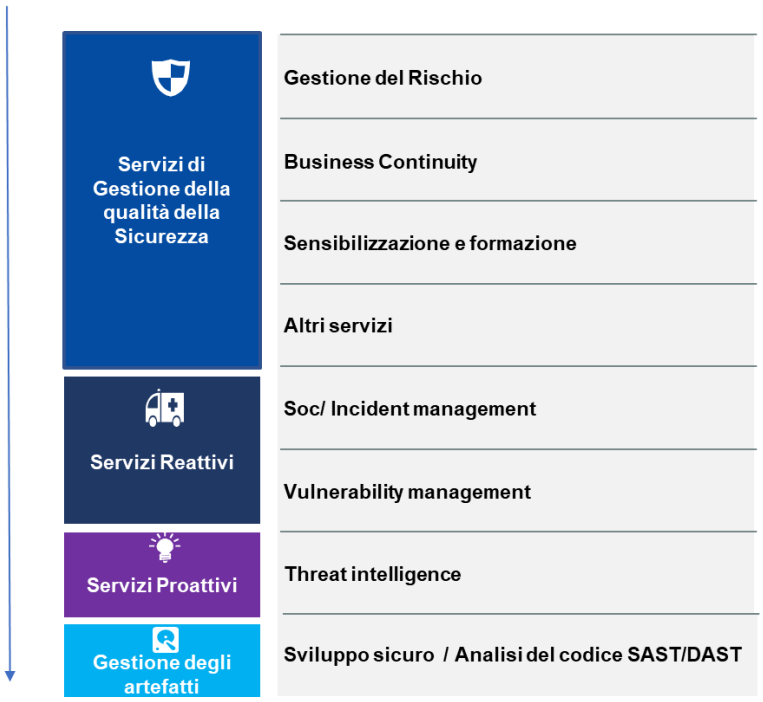


Figura 7 – Servizi Inclusi nel CERT Regionale

Vengono di seguito descritti nel dettaglio i servizi inclusi all'interno del CERT Regionale di Regione del Veneto.

8.2.1 Gestione del rischio

Conoscere e gestire i rischi è fondamentale per il successo di ogni organizzazione a causa dei potenziali impatti che, qualora si verificassero, potrebbero minare la stabilità e la continuità del business. Inoltre, la valutazione e la gestione del rischio della sicurezza delle informazioni è un punto centrale per la conformità allo standard ISO 27001.
Tramite il servizio di **Gestione del rischio,** il CERT Regionale mira ad implementare un framework di gestione dei rischi e ad eseguire specifici assessment al fine di **misurare e stimare il rischio di sicurezza** correlato alle specificità del singolo Ente aderente (contesto, asset e loro valore, minacce, vulnerabilità e controlli implementati), al fine di sviluppare le opportune strategie di governo del rischio (prevenzione, riduzione, trasferimento, accettazione).
Di seguito sono elencate le attività erogate nell'ambito del Servizio di Gestione del Rischio:

1. **Definizione delle linee guida:** Definizione delle linee guida da seguire al fine di produrre un set di regole comuni, stabilire e mantenere determinati criteri di rischio per la sicurezza delle informazioni per la conformità allo standard ISO 27001. Identificazione di un framework di riferimento (e.g. NIST) che definisca l'approccio da seguire per l'IT Risk assessment; identificazione delle soglie per una classificazione del rischio sulla base di impatto e probabilità di accadimento. Tale attività viene svolta dal CERT Regionale.
2. **Esecuzione dell'assessment:** Comprensione del contesto, degli asset in scope e del loro valore, delle minacce e relative probabilità di accadimento, delle vulnerabilità ed i relativi controlli di sicurezza. Tale attività è in carico al CERT di Regione del Veneto**.** Risulta imprescindibile partire da un assessment iniziale che identifichi le informazioni, la loro tipologia e le correli agli asset aziendali ovvero alle risorse soggette a rischio, ma soprattutto ne misuri il livello iniziale di esposizione al rischio. Tale attività viene svolta dal CERT Regionale.

3. **Analisi dei Risultati:** Stabilito successivamente il livello di copertura ottimale, è necessario prendere decisioni su come affrontare il rischio, ossia individuare, per ogni valore di rischio, appropriate azioni di mitigazione o trasferimento del rischio oppure di accettazione dello stesso. Tale attività viene svolta dal CERT Regionale.
4. **Implementazione azioni di rimedio:** Applicazione di eventuali azioni di rimedio per abbassare il livello di rischio e renderlo accettabile. Tale attività viene svolta dal singolo ente ad accezione degli enti afferenti al gruppo 5.
5. **Verifica e monitoraggio delle azioni di rimedio** che sono state implementate al punto precedente. Tale attività viene svolta dal CERT Regionale.

In figura si riporta una sintesi delle attività previste per il servizio, con un'indicazione dell'area di appartenenza di tali attività secondo il Ciclo di Deming (PLAN-DO-CHECK-ACT), alla base di molteplici standard internazionali, ed in particolare della famiglia degli standard ISO, che permette la correlazione alle fasi di gestione del rischio di individuazione, quantificazione, valutazione e controllo. Viene inoltre individuato il responsabile per ogni attività.

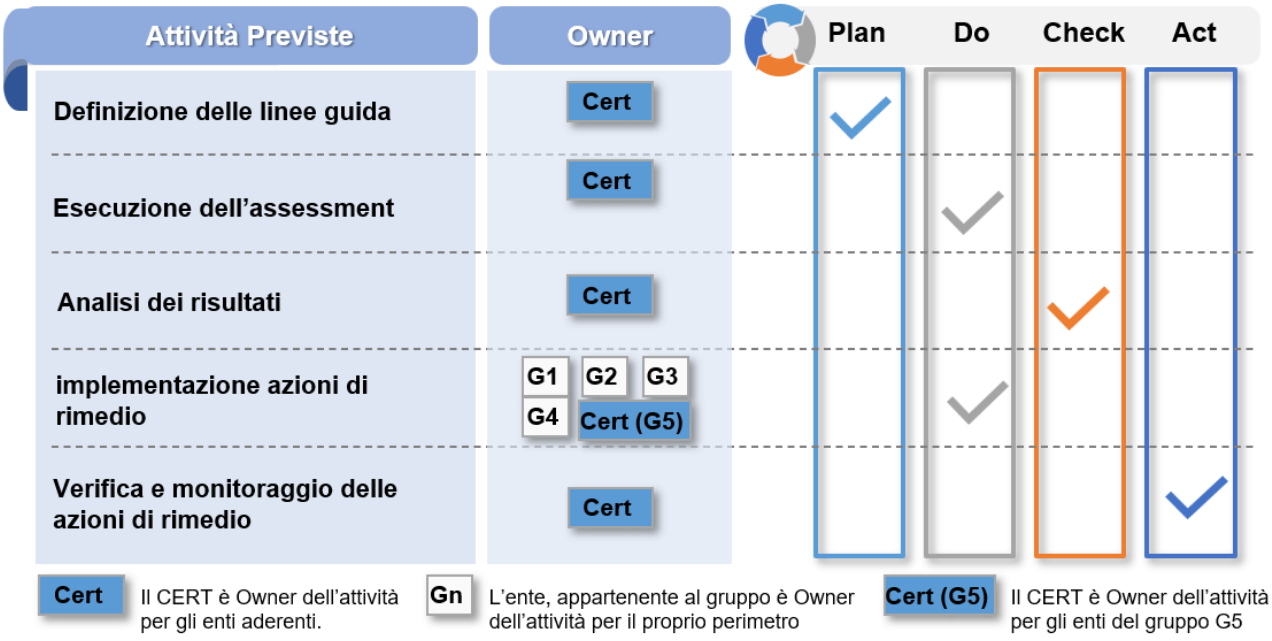


Figura 8 – Sintesi del servizio Gestione del Rischio

8.2.2 Business Continuity

Per poter essere resiliente, un'azienda deve tenere in forte considerazione gli impatti di un'eventuale interruzione sia sulle tecnologie che su tutti gli aspetti che esulano dalla tecnologia in senso stretto, ad esempio risorse umane, organizzazione, logistica e commerciale. Il concetto di Business Continuity fa quindi leva sulla prevenzione tramite un'analisi d'impatto operativo (Business Impact Analysis) per garantire sostenibilità e recupero di tutti i processi in caso di interruzione.
Tramite il servizio di **Business Continuity**, il CERT Regionale definisce le opportune strategie (e.g. **Disaster Recovery**) che possano permettere al singolo Ente di **continuare a erogare servizi ad un livello predefinito ed accettabile**, a seguito di un incidente con impatto sul sistema informativo. Resta inteso che la responsabilità dell'implementazione di tali strategie è in carico all'Ente.
Di seguito sono elencate le attività erogate nell'ambito del Servizio di Business Continuity:

1. **Definizione delle linee guida:** Definizione delle linee guida da seguire al fine di produrre un set di regole comuni che guidino gli enti nel rispondere, recuperare, riprendere e ripristinare a un livello predefinito le attività a seguito di un'interruzione (disruption). Tale attività viene svolta dal CERT Regionale.
2. **Esecuzione della BIA:** Processo di analisi delle attività e degli effetti che un'interruzione potrebbe avere su di esse, consentendo di stabilire le priorità per il recupero dei processi critici, definendo Recovery Time Objective (RTO) e i Recovery Point Objective (RPO). Tale attività viene svolta dal CERT Regionale.
3. **Implementazione dei piani di BC &DR:** Creazione di una struttura di risposta agli incidenti e delle soluzioni tecnologiche necessarie a reagire ad un evento critico, fino al ritorno alla normalità. Tale attività viene svolta dal singolo ente e l'output è condiviso con il CERT.
4. **Esecuzione dei test di BC &DR e analisi dei risultati:** Verifica delle strategie e delle soluzioni definite nel piano di BCM e DR tramite la predisposizione delle checklist. Tale attività viene svolta dal singolo ente e l'output è condiviso con il CERT.
5. **Implementazione delle azioni di rimedio:** Implementazione di eventuali azioni di rimedio a valle delle risultanze dei test eseguiti. Tale attività viene svolta dal singolo ente ad accezione degli enti afferenti al gruppo 5.

In figura si riporta una sintesi delle attività previste per il servizio, con un'indicazione dell'area di appartenenza di tali attività secondo il Ciclo di Deming (PLAN-DO-CHECK-ACT), alla base di molteplici standard internazionali, ed in particolare della famiglia degli standard ISO, che permette la correlazione alle fasi della Business Continuity. Viene inoltre individuato il responsabile per ogni attività.

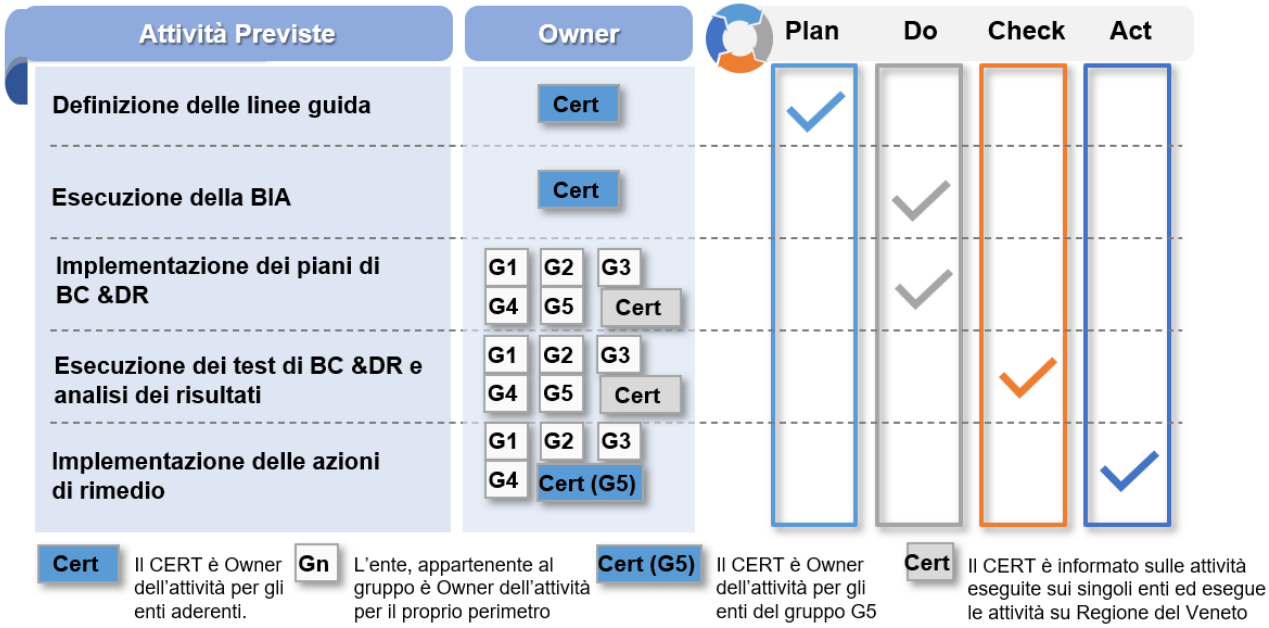


Figura 9 – Sintesi del servizio Business Continuity

8.2.3 Sensibilizzazione e Formazione

Tramite il servizio di **Sensibilizzazione e Formazione**, il CERT Regionale definisce gli obiettivi formativi e formalizza un **programma di awareness** su specifiche tematiche di sicurezza per il rispetto dei controlli previsti dalla ISO 27001 e per il raggiungimento degli stessi, da erogare ai singoli enti tramite l'utilizzo di una **specifica piattaforma.**

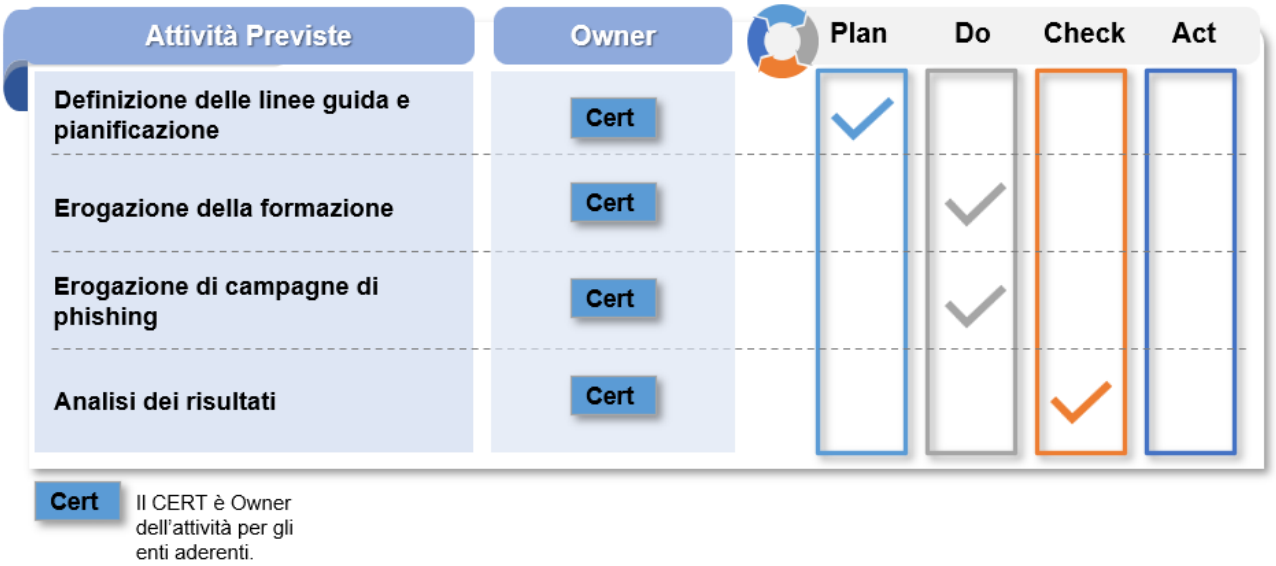


Figura 10 – Sintesi del servizio Sensibilizzazione e Formazione

Di seguito sono elencate le attività erogate nell'ambito del Servizio di sensibilizzazione e formazione:

1. **Definizione delle linee guida:** Definizione degli obiettivi formativi e del programma di formazione per accrescere la consapevolezza legata ai rischi cyber e indirizzare le risorse verso le opportune pratiche. Tale attività viene svolta dal CERT.
2. **Erogazione della formazione:** Erogazione e monitoraggio del piano di formazione per il raggiungimento degli obiettivi prefissati. Tale attività viene svolta dal CERT e l'output è condiviso con i singoli enti. Tale attività viene svolta dal CERT.
3. **Erogazione di campagne di phishing:** Pianificazione ed erogazione di campagne di phishing. Tale attività viene svolta dal CERT e l'output è condiviso con i singoli enti.
4. **Analisi dei risultati:** Valutazione dei risultati per determinare le azioni da intraprendere per il miglioramento continuo rispetto a quanto svolto. Tale attività viene svolta dal CERT.

In figura si riporta una sintesi delle attività previste per il servizio, con un'indicazione dell'area di appartenenza di tali attività secondo il Ciclo di Deming (PLAN-DO-CHECK-ACT), alla base di molteplici standard internazionali, ed in particolare della famiglia degli standard ISO, che permette la correlazione alle fasi di sensibilizzazione e formazione. Viene inoltre individuato il responsabile per ogni attività.

8.2.4 Altri servizi

Tramite gli «altri servizi» il CERT Regionale, supporta gli enti aderenti a livello tecnico e strategico attraverso l'erogazione di attività consulenziali per la gestione di servizi di sicurezza o per la loro attivazione. Il CERT si avvale di un team di esperti cyber che su richiesta può erogare dei servizi di varia natura.

Di seguito sono elencate le attività erogate nell'ambito del Servizio altri servizi:

1. **Supporto specialistico - Gestione del rischio:** Erogazione di un supporto specialistico da parte del Team di esperti Cyber del CERT su tematiche di gestione del rischio per indirizzare le attività in carico all'Ente. Tale attività viene svolta dal CERT.
2. **Supporto specialistico - Business Continuity:** Erogazione di un supporto specialistico da parte del Team di esperti Cyber del CERT su tematiche di Business Continuity per indirizzare le attività in carico all'Ente. Tale attività viene svolta dal CERT.

3. **Supporto specialistico - Sensibilizzazione e Formazione:** Erogazione di un supporto specialistico da parte del Team di esperti Cyber del CERT su tematiche di formazione per indirizzare le attività in carico all'Ente. Tale attività viene svolta dal CERT.
4. **Supporto specialistico - Sviluppo Sicuro:** Erogazione di un supporto specialistico da parte del Team di esperti Cyber del CERT su tematiche di sviluppo sicuro per indirizzare le attività in carico all'Ente. Tale attività viene svolta dal CERT.
5. **Supporto specialistico – Certificazione ISO 27001:** Erogazione di un supporto specialistico da parte del Team di esperti Cyber del CERT su tematiche di certificazione ISO 27001. Tale attività viene svolta dal CERT.

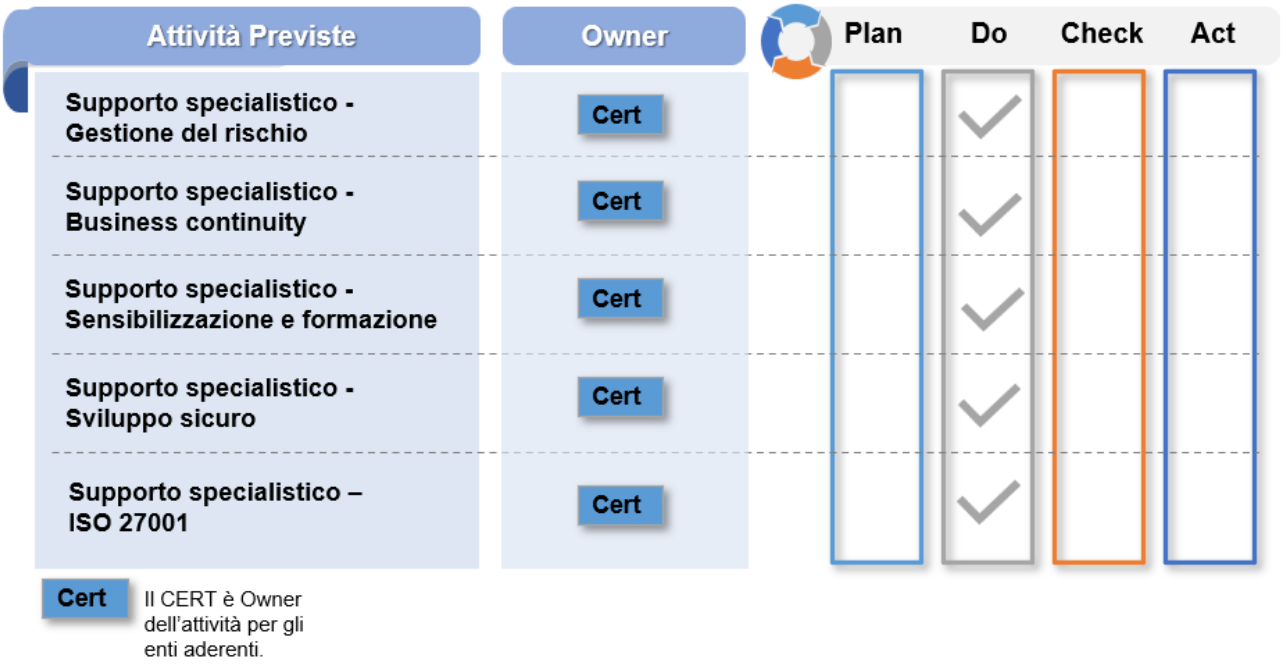


Figura 11 – Sintesi del servizio Altri servizi

In figura si riporta una sintesi delle attività previste per il servizio, con un'indicazione dell'area di appartenenza di tali attività secondo il Ciclo di Deming (PLAN-DO-CHECK-ACT), alla base di molteplici standard internazionali, ed in particolare della famiglia degli standard ISO. Viene inoltre individuato il responsabile per ogni attività.

8.2.5 SOC/ Incident Management

Tramite il servizio di SOC/ Incident Management, il CERT Regionale attiva azioni di monitoraggio e verifica per gli enti. Il Security Operations Center (SOC) è operativo in modalità 24x7x365 e si avvale di soluzioni tecnologiche SIEM e SOAR. Tramite il SOC vengono svolte attività di prevenzione, gestione, monitoraggio, analisi di eventi e risoluzione di eventuali incidenti di sicurezza. Di seguito sono elencate le attività erogate nell'ambito del Servizio di SOC/Incident management:

- **Definizione delle linee guida:** Definizione della strategia e delle linee guida da seguire al fine di produrre un set di regole comuni (es. classificazione degli incidenti e metriche di monitoraggio). Tale attività viene svolta dal CERT.
- **Formalizzazione del piano di risposta agli incidenti:** Definizione del piano di risposta agli incidenti, che definisca le attività, i ruoli e le responsabilità in caso di

minaccia o incidente. Tale attività viene svolta dal singolo ente e l'output è condiviso con il CERT.

- **L1 – Triage – Monitoraggio console ed eliminazione falsi positivi:** Monitoraggio tramite SIEM/ SOAR del perimetro e rilevazione degli alert. il processo garantisce il monitoraggio continuo delle informazioni prodotte dal SOC attraverso dashboard e canali necessari al monitoraggio continuo e completo dei sistemi, che permettano di avere visibilità sulla postura di sicurezza degli Enti aderenti al CERT. Questa attività di Triage viene effettuata dal CERT di Regione del Veneto per gli Enti aderenti non dotati di piattaforma SIEM o eventualmente dai singoli enti (appartenenti al gruppo G2) dotati di SIEM. Il SIEM del CERT di Regione del Veneto in questo ultimo caso funge da HyperSIEM rispetto ai SIEM degli enti aderenti.
- **L2 – Contenimento – Gestione Evento:** Gestione dell'evento segnalato dal livello L1 per identificarne delle possibili azioni correttive da intraprendere nell'immediato per contenere l'attacco e prevenirne la propagazione o caratterizzarlo come incidente di Sicurezza. Tale attività viene svolta dal CERT di Regione del Veneto ad accezione degli enti appartenenti al Gruppo 1. L'ente appartenete al Gruppo 1 può tuttavia richiedere supporto al Team CERT di Regione del Veneto On Demand.
- **L1 – Gestione dell'Incidente di Sicurezza di livello 1:** Gestione dell'incidente di sicurezza a livello del singolo ente. Tale attività viene svolta dal singolo ente. Si prevede il supporto di Regione Veneto a coordinamento delle attività. Eventuale supporto operativo da parte di terze partipotrà essere acquistato on demand direttamente dall'ente.
- **L2 – Gestione dell'Incidente di Sicurezza di livello 2:** Si attiva nel momento in cui l'Incidente abbia impatto particolarmente critico o impatto a livello regionale. Tale attività viene coordinata da Regione del Veneto. Eventuale supporto operativo da parte di terze parti potrà essere acquistato on demand direttamente dall'ente.

In figura si riporta una sintesi delle attività previste per il servizio, con un'indicazione dell'area di appartenenza di tali attività secondo il Ciclo di Deming (PLAN-DO-CHECK-ACT), alla base di molteplici standard internazionali, ed in particolare della famiglia degli standard ISO, che permette la correlazione alle fasi di SOC/Incident Management. Viene inoltre individuato il responsabile per ogni attività.

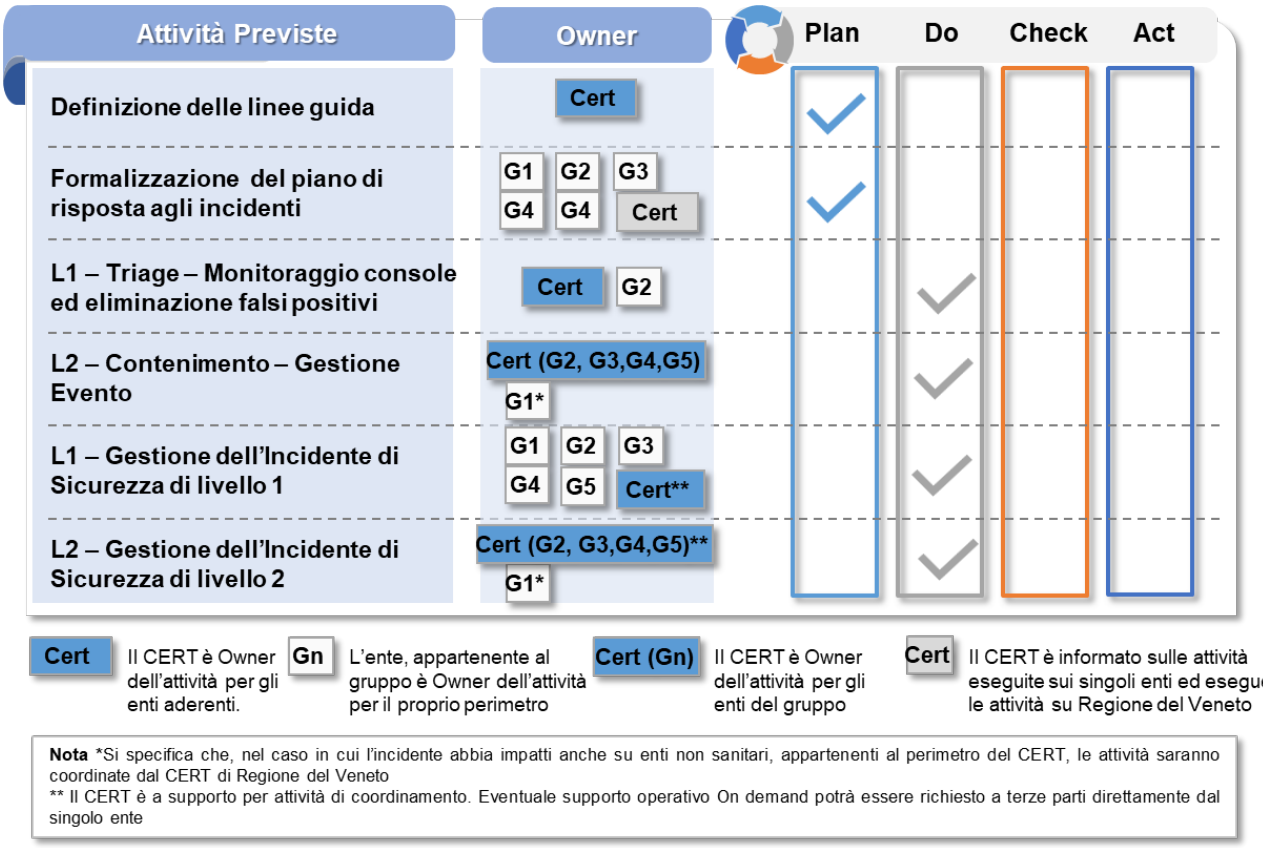


Figura 12 – Sintesi del servizio SOC / Incident Management

8.2.6 Vulnerability Management

Tramite il servizio di Vulnerability management, il CERT Regionale definisce delle linee guida per l'identificazione, analisi e caratterizzazione delle vulnerabilità che riguardano l'intera infrastruttura IT, gli asset e i sistemi tecnologici. Definisce le linee guida anche per la fase di remediation e di verifica delle azioni implementate. Di seguito sono elencate le attività erogate nell'ambito del Servizio di vulnerability management:

1. **Definizione delle linee guida:** Definizione della strategia e delle linee guida da seguire al fine di produrre un set di regole comuni per la gestione delle vulnerabilità. Tale attività è in carico al CERT Regionale. Tale attività viene svolta dal CERT.
2. **Pianificazione attività:** Pianificazione delle attività per l'esecuzione di Vulnerability assessment e penetration testing. Tale attività viene svolta dal CERT.
3. **Vulnerability Assessment:** Identificazione, classificazione e prioritizzazione delle vulnerabilità che interessano i sistemi presenti all'interno di ogni ente. Per tale attività sono utilizzati i tool di scansione continua automatici identificati. Tale attività viene svolta dal CERT.
4. **Penetration testing**: Esecuzione di penetration test per valutare opportunamente l'efficacia delle attività di correzione eseguite. Sono inoltre utili per garantire che non siano state create nuove vulnerabilità durante le attività di risoluzione. Tale attività viene svolta dal CERT.
5. **Esecuzione delle azioni di rimedio:** Definizione, condivisione e monitoraggio del piano di rimedio definito sulla base degli esiti delle scansioni automatiche continue e dei PT. (Owner: CERT). Implementazione delle azioni di rimedio. Tale attività viene svolta dal singolo ente e l'output è condiviso con il CERT.

6. **Monitoraggio delle azioni di rimedio:** Monitoraggio delle vulnerabilità e delle relative attività di rimedio in carico al singolo ente. Tale attività viene svolta dal CERT.

In figura si riporta una sintesi delle attività previste per il servizio, con un'indicazione dell'area di appartenenza di tali attività secondo il Ciclo di Deming (PLAN-DO-CHECK-ACT), alla base di molteplici standard internazionali, ed in particolare della famiglia degli standard ISO, che permette la correlazione alle fasi di Vulnerability Management. Viene inoltre individuato il responsabile per ogni attività.

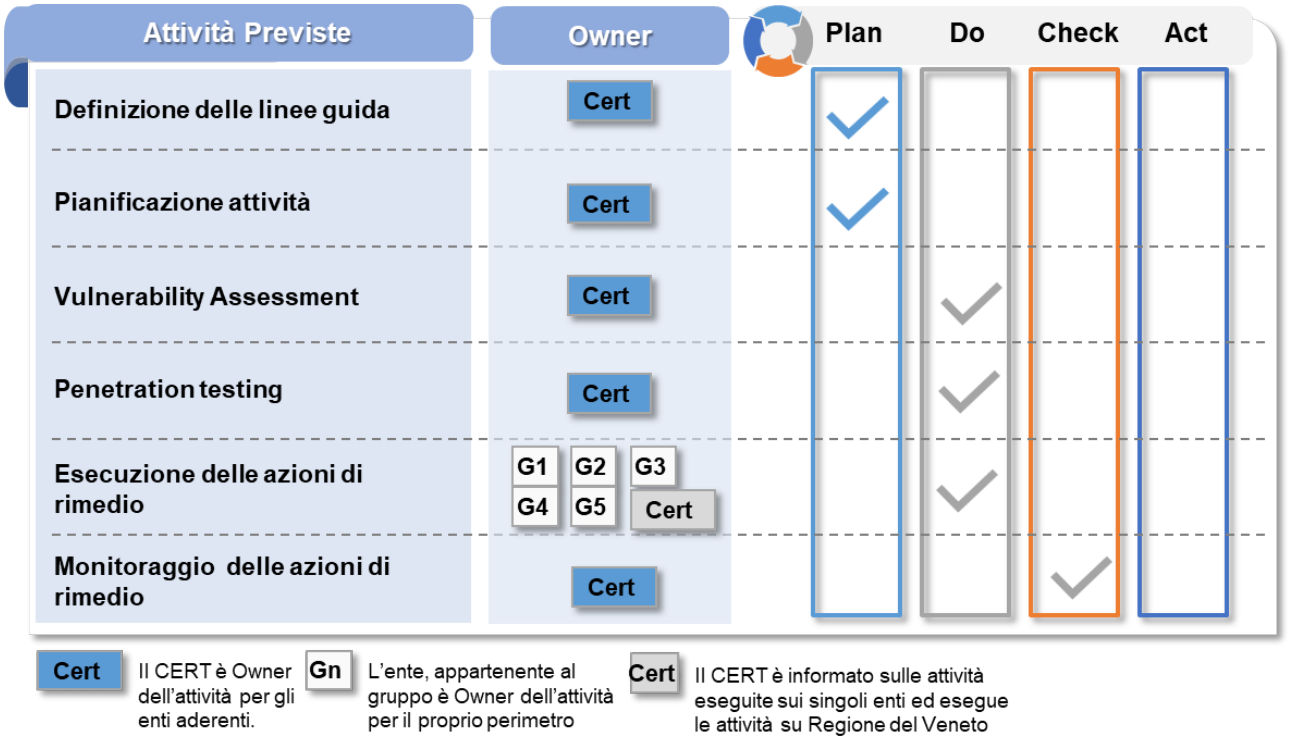


Figura 13 – Sintesi del servizio Vulnerability Assessment

8.2.7 Threat Intelligence

Il servizio di Threat intelligence del CERT Regionale agevola la diffusione di informazioni tempestive e immediatamente utilizzabili su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cibernetici. Raccoglie informazioni provenienti da varie fonti che possono essere utilizzate tramite una piattaforma per finalità strategiche, tattiche e operative. Di seguito sono elencate le attività erogate nell'ambito del Servizio di threat intelligence:

1. **Definizione delle linee guida:** Definizione delle linee guida, per le informazioni e comunicazioni. Tale attività viene svolta dal CERT.
2. **Monitoraggio delle minacce e vulnerabilità:** Servizi di monitoraggio e avviso sulle minacce e sulle vulnerabilità dei Sistemi. Tale attività viene svolta dal CERT.
3. **Monitoraggio del Web, deep e dark web:** Servizi di Credential Leakage, Deep & Dark Web Monitoring e Domain Squatting. Tale attività viene svolta dal CERT.
4. **Elaborazione e condivisione di report e alert:** Elaborazione di report relativi agli scenari di rischio, le vulnerabilità, e su attività di analisi svolte tramite richieste di informazioni da parte degli enti. Tale attività viene svolta dal CERT.

In figura si riporta una sintesi delle attività previste per il servizio, con un'indicazione dell'area di appartenenza di tali attività secondo il Ciclo di Deming (PLAN-DO-CHECK-ACT), alla base di

molteplici standard internazionali, ed in particolare della famiglia degli standard ISO, che permette la correlazione alle fasi della Threat Intelligence. Viene inoltre individuato il responsabile per ogni attività.

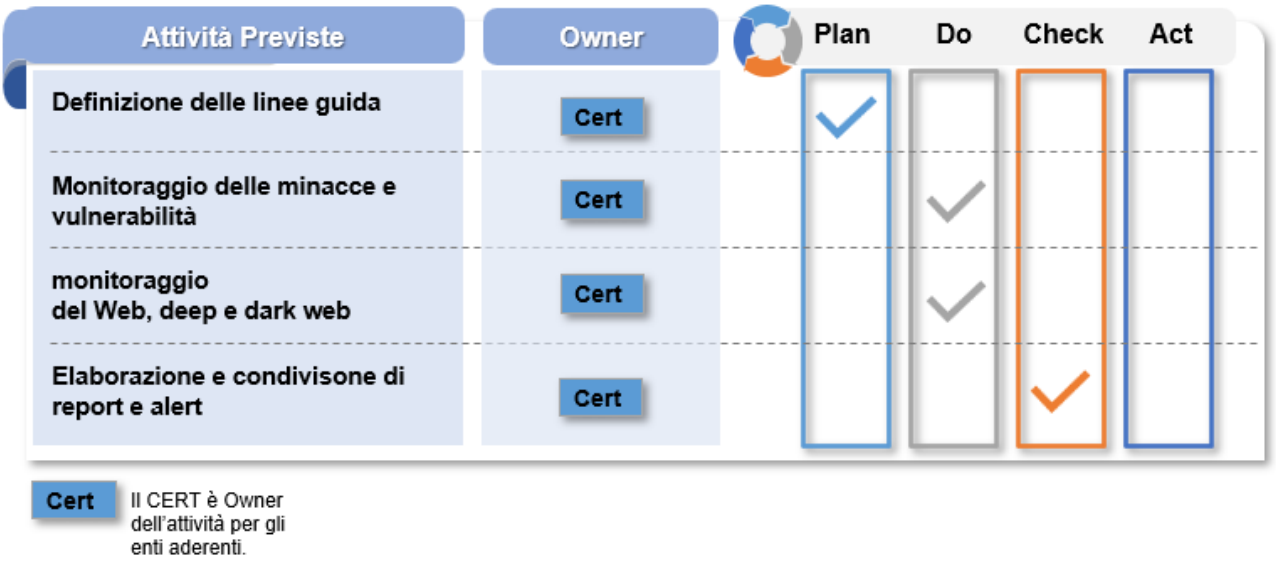


Figura 14 – Sintesi del servizio Threat Intelligence

8.2.8 Sviluppo sicuro

Tramite il servizio di Sviluppo sicuro / Analisi del codice SAST/DAST, il CERT Regionale mira ad individuare vulnerabilità legate alla progettazione e implementazione scorretta delle applicazioni web. SAST e DAST sono procedure eseguibili con l'ausilio di strumenti automatizzati, in grado anche fornire un report immediato sulla situazione. Di seguito sono elencate le attività erogate nell'ambito del Servizio di Sviluppo sicuro:

1. **Definizione delle linee guida:**
    a. Definizione delle linee guida per lo sviluppo sicuro del software e sviluppo dei linguaggi di programmazione. Tale attività viene svolta dal CERT e prevede:
        i. Definizione dei requisiti di sicurezza di application security da applicare alla fase di design dello sviluppo del software interno e di terze parti.
        ii. Definizione modello di minaccia, creazione template e linea guida per l'adozione della pratica all'interno del SDLC.
        iii. Esecuzione del Threat Modeling su un sottoinsieme di applicazioni ad elevato rischio potenziale per il CERT e i vari enti.
2. **Attività Operative:** Supporto on demand ai processi di sviluppo software tramite un Security Champion e strumenti di scansione continua. Tale attività viene svolta dal CERT.

In figura si riporta una sintesi delle attività previste per il servizio, con un'indicazione dell'area di appartenenza di tali attività secondo il Ciclo di Deming (PLAN-DO-CHECK-ACT), alla base di molteplici standard internazionali, ed in particolare della famiglia degli standard ISO, che permette la correlazione alle fasi di gestione del rischio individuazione, quantificazione, valutazione e controllo. Viene inoltre individuato il responsabile per ogni attività.

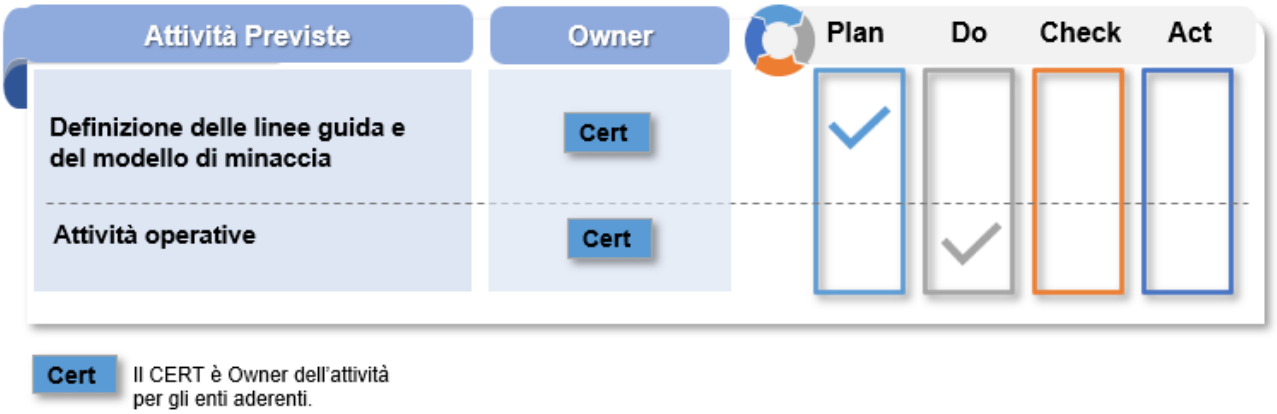


Figura 15 – Sintesi del servizio Sviluppo Sicuro

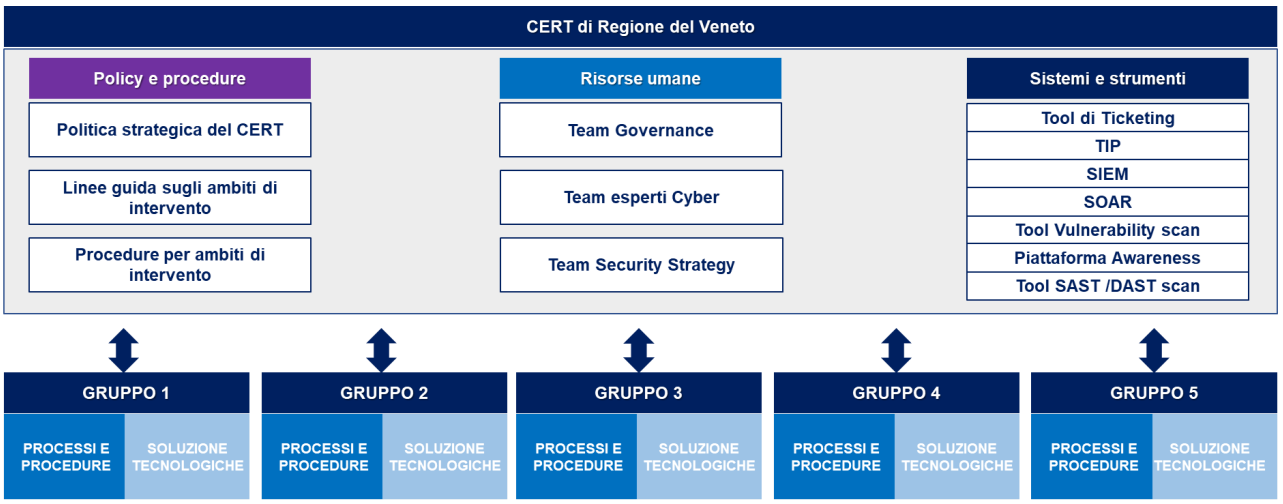
8.3 Modello Operativo

Al fine di comprendere il modello operativo del CERT regionale nel suo complesso è necessario declinarne l'operatività per ogni singolo servizio. Nello specifico vengono presentati:

- Regole e flussi di funzionamento del CERT Regionale nel suo complesso
- Struttura di riferimento del CERT Regionale.
- Modello Tecnologico.
- Modello di riferimento, basato su un approccio a fasi per consentire che tutti i servizi siano implementati e gestiti in modo efficace ed efficiente.
- Regole e flussi di funzionamento di ciascun servizio previsto all'interno del CERT Regionale.

8.3.1 Regole e flussi di funzionamento del CERT Regionale

Il modello operativo del CERT Regionale prevede un modello ibrido con l'accentramento di alcuni servizi di sicurezza che verranno erogati da parte del CERT di Regione del Veneto a beneficio degli enti aderenti ed altri servizi che, almeno parzialmente, verranno gestiti dal singolo Ente, sulla base della propria appartenenza ai gruppi di riferimento.



N.B. *Si intende che il CERT Regionale erogherà i servizi per la Regione Veneto stessa, oltre che per gli Enti aderenti*

Figura 16 – Modello Operativo del CERT Regionale

A livello amministrativo il Team di Governance avrà il compito di:

- Gestire i fornitori coinvolti a vario titolo nel CERT Regionale e, in particolare, nell'erogazione dei servizi afferenti il CERT stesso.
- Garantire una corretta approvazione, allocazione e gestione del budget dedicato al CERT Regionale.
- Svolgere un ruolo di contatto, di coordinamento e di monitoraggio dei servizi erogati verso singolo Ente.

Le strutture operative (Team esperti cyber e Team security strategy) saranno responsabili dell'erogazione dei servizi come da modello operativo di ogni singolo servizio, sulla base del gruppo di appartenenza.

I processi operativi su singolo ente sono definiti sulla base della politica e delle linee guida comuni del CERT al fine di garantire l'autonomia per l'Ente nella definizione ed implementazione delle iniziative di sicurezza e nella gestione di eventi di sicurezza con impatto locale. Con riferimento agli enti sanitari, il modello operativo prevede il ruolo di coordinamento di Azienda Zero, che supporta gli enti sanitari nella gestione della propria sicurezza e in tal senso avrà il compito di erogare per questi i servizi demandati a singolo ente e di intermediare tra il CERT di Regione del Veneto e gli enti sanitari per quei servizi erogati centralmente dal CERT di Regione del Veneto.
Ogni ente manterrà l'autonomia nella gestione dei controlli di Cybersecurity per i quali non interviene il CERT Regionale.
Come già accennato, è stato quindi definito un modello ibrido che prevede la suddivisione delle attività operative tra CERT Regionale e singoli Enti, sulla base dell'appartenenza ai gruppi sopra descritti. Tale modello declina per singolo servizio le attività che devono essere erogate dal CERT di Regione del Veneto e le attività che devono essere invece gestite dal singolo ente, in funzione del gruppo di appartenenza.

Si riporta di seguito una Tabella riassuntiva che raffigura il responsabile (CERT di Regione del Veneto o gruppo) delle diverse attività.

Ambito	CERT Regione del Veneto	G1	G2	G3	G4	G5
Gestione del rischio	• Definizione delle linee guida • Esecuzione dell'assessment • Analisi dei risultati • Verifica e monitoraggio delle azioni di rimedio • Implementazione azioni di rimedio (G5)	• Implementazione azioni di rimedio	• Implementazione azioni di rimedio	• Implementazione azioni di rimedio	• Implementazione azioni di rimedio	
Business Continuity	• Definizione delle linee guida • Esecuzione della BIA • Implementazione delle azioni di rimedio (G5)	• Implementazione dei piani di BC &DR • Esecuzione dei test di BC & DR e analisi dei risultati • Implementazione delle azioni di rimedio	• Implementazione dei piani di BC &DR • Esecuzione dei test di BC & DR e analisi dei risultati • Implementazione delle azioni di rimedio	• Implementazione dei piani di BC &DR • Esecuzione dei test di BC & DR e analisi dei risultati • Implementazione delle azioni di rimedio	• Implementazione dei piani di BC &DR • Esecuzione dei test di BC & DR e analisi dei risultati • Implementazione delle azioni di rimedio	
Sensibilizzazione e formazione	• Definizione delle linee guida • Erogazione della formazione • Erogazione di campagne di phishing • Analisi dei risultati					

Ambito	CERT Regione del Veneto	G1	G2	G3	G4	G5
Altri servizi	• Supporto specialistico per gestione del rischio • Supporto specialistico per Business continuity • Supporto specialistico per Sensibilizzazione e formazione • Supporto specialistico per Sviluppo sicuro					
SOC/ Incident management	• Definizione delle linee guida • L1 – Triage – Monitoraggio console ed eliminazione falsi positivi (G1, G3, G4, G5) • Contenimento – Gestione Evento (G2, G3, G4, G5) • L1 – Gestione dell'Incidente di Sicurezza di livello 1 (a coordinamento) • L2 – Gestione dell'Incidente di Sicurezza di livello 2 (G2, G3, G4, G5) - coordinamento	• Formalizzazione del piano di risposta agli incidenti • Contenimento – Gestione Evento (con l'eventuale supporto del CERT) • L1 – Gestione dell'Incidente di Sicurezza di livello 1 – eventuale supporto operativo potrà essere richiesto a terze parti • L2 – Gestione dell'Incidente di Sicurezza di livello 2 (con l'eventuale supporto del CERT)	• Formalizzazione del piano di risposta agli incidenti • L1 – Triage – Monitoraggio console ed eliminazione falsi positivi • L1 – Gestione dell'Incidente di Sicurezza di livello 1– eventuale supporto operativo potrà essere richiesto a terze parti	• Formalizzazione del piano di risposta agli incidenti • L1 – Gestione dell'Incidente di Sicurezza di livello 1– eventuale supporto operativo potrà essere richiesto a terze parti	• Formalizzazione del piano di risposta agli incidenti • L1 – Gestione dell'Incidente di Sicurezza di livello 1 – eventuale supporto operativo potrà essere richiesto a terze parti	• Formalizzazione del piano di risposta agli incidenti • L1 – Gestione dell'Incidente di Sicurezza di livello 1 – eventuale supporto operativo potrà essere richiesto a terze parti
Vulnerability Management	• Definizione delle linee guida Vulnerability Assessment • Penetration testing • Definizione e monitoraggio del piano di rimedio	• Implementazione delle azioni di rimedio	• Implementazione delle azioni di rimedio	• Implementazione delle azioni di rimedio	• Implementazione delle azioni di rimedio	• Implementazione delle azioni di rimedio
Threat Intelligence	• Definizione delle linee guida • Monitoraggio delle minacce e vulnerabilità • Monitoraggio del Web, deep e dark web • Elaborazione e condivisone di report e alert					
Sviluppo sicuro	• Definizione delle linee guida • Attività operative					

Tabella 01 – Ambiti di intervento e attività del CERT Regionale

8.3.2 Struttura di riferimento del CERT Regionale

Il modello operativo del CERT Regionale per la gestione dei servizi di sicurezza prevede la strutturazione di un ufficio dedicato presso la Direzione ICT della Regione del Veneto, come riportato nell'immagine seguente:

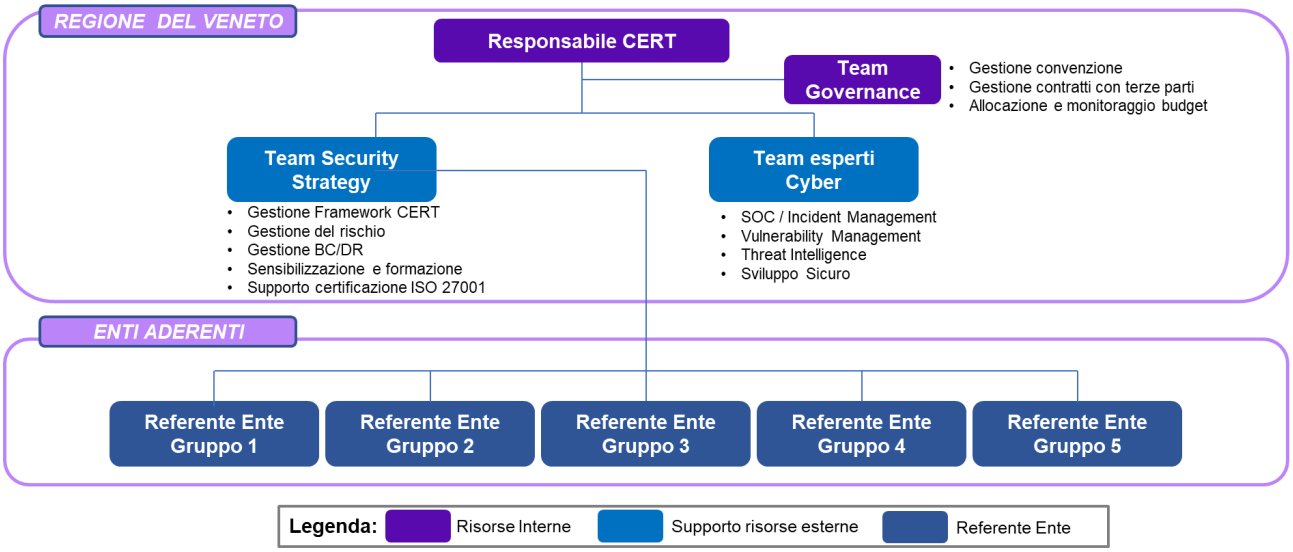


Figura 17 – Ufficio operativo del CERT Regionale

Il CERT Regionale è caratterizzato da una squadra in grado di supportare gli Enti nella risposta agli incidenti nonché fornire risorse specialistiche in grado di erogare supporto agli enti su tematiche di sicurezza ad alta specializzazione e nell'utilizzo dei diversi sistemi e strumenti in uso. L'ufficio del CERT Regionale è governato da un responsabile al quale afferiscono i diversi team incaricati allo svolgimento delle attività operative. In particolare, all'interno del CERT sono individuate tre funzioni:

- **Funzione Governance**, si occupa di gestire le attività amministrative dell'ufficio. In particolare, si occupa della gestione delle terze parti (convenzioni e/o contratti con gli Enti aderenti) e della gestione del budget.
- **Funzione Security Strategy**, si occupa di gestire il framework di monitoraggio del CERT nonché di erogare le attività consulenziali relative alla gestione del rischio, alla business continuity, al disaster recovery, la sensibilizzazione e formazione e di supporto alla certificazione ISO 27001. La funzione può avvalersi di risorse esterne.
- **Funzione esperti Cyber**, si occupa del monitoraggio di vulnerabilità e minacce e delle attività di risposta agli incidenti cyber. Inoltre, eroga attività consulenziali per lo sviluppo sicuro del codice. Tale funzione può avvalersi di risorse esterne.

8.3.3 Modello Tecnologico

Il modello tecnologico del CERT Regionale si basa su una combinazione di tecnologie integrate tra loro, volte a garantire la raccolta, l'analisi e la gestione delle informazioni sulle minacce di sicurezza informatica. Le singole tecnologie, laddove necessario per assicurare la confidenzialità delle informazioni, si baseranno su logiche Multi-tenant. Le tecnologie in uso al CERT Regionale includono:

- **Tool di Awareness**: piattaforma dedicata al personale identificato, finalizzata all'apprendimento e al consolidamento nel tempo della consapevolezza necessaria ad affrontare la continua evoluzione delle tecniche utilizzate dal cyber crime. L'obiettivo principale dei percorsi formativi è quello di incidere sui comportamenti degli utenti sviluppando le principali caratteristiche difensive di ogni individuo: la conoscenza, la percezione del pericolo, la prontezza.
- **TIP *Threat Intelligence Platform***: contribuisce ad innalzare le capacità di un'organizzazione di contrastare le minacce informatiche in continua evoluzione, fornendo informazioni pertinenti, tempestive e attuabili sulle minacce alla sicurezza

informatica. I servizi di Cyber Threat Intelligence sono in grado di identificare il contesto di una minaccia, gli strumenti, le identità, le tecniche e le procedure utilizzate dagli avversari, in modo che i team di sicurezza del CERT possano velocizzare le attività di detection e di remediation.

- **SIEM *Security Information & Event Management***: soluzione che ha come obiettivo la raccolta centralizzata, la correlazione e l'analisi dei log e degli eventi generati da applicazioni e sistemi.
- **SOAR *Security Orchestration, Automation and Response***: è costituito da una serie di programmi software che consentono ad un'organizzazione di raccogliere dati sulle minacce alla sicurezza, limitando al minimo l'intervento umano.
- **Tool di ticketing**: raccoglie tutte le richieste di "assistenza" durante tutto il workflow per la gestione degli eventi all'interno del CERT e le convoglia verso punti di contatto stabiliti.
- **Tool di Vulnerability Scanning:** per le scansioni continue dei dispositivi di rete, i server, le reti wireless, le applicazioni web e i database.
- **Tool SAST:** effettua una analisi del codice sorgente o bytecode per identificare le vulnerabilità nelle applicazioni dall'interno. Identifica le problematiche nel codice custom e di terze parti.
- **Tool DAST:** effettua test di sicurezza dinamici (applicazioni in esecuzione) automatizzati seguiti da un'analisi manuale dei falsi positivi dei problemi di sicurezza identificati nelle Web Application e API.

Di seguito vengono esplicitate le tecnologie che saranno in uso per ognuno dei servizi inclusi nel CERT di Regione del Veneto. Specifichiamo che i servizi "Gestione del Rischio", "Continuità Operativa" e "Altri Servizi" non necessitano di alcuna soluzione tecnologica.

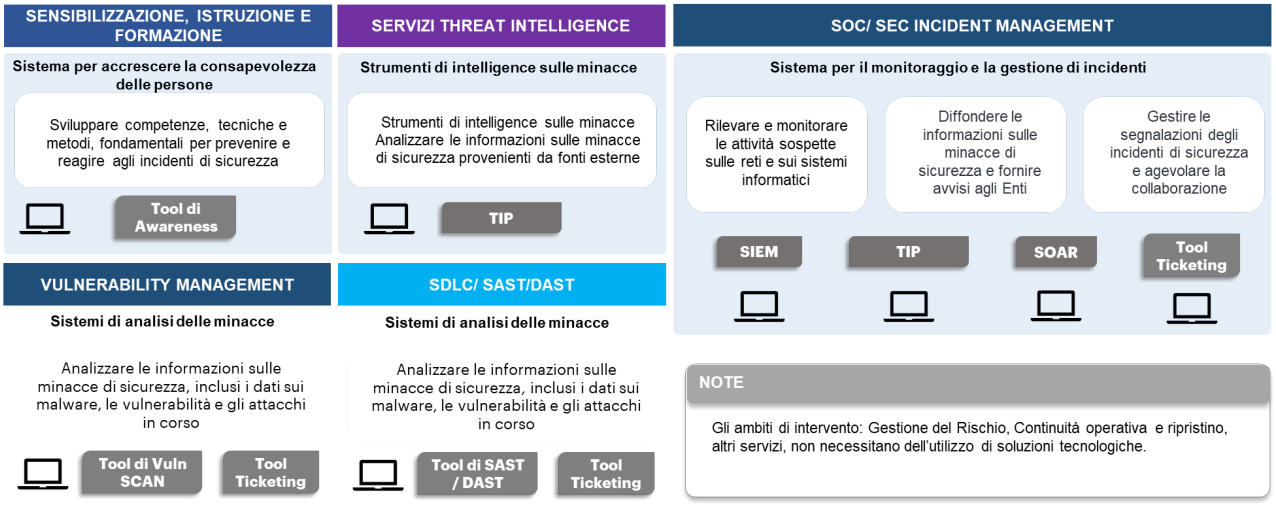


Figura 18 – Modello delle tecnologie in uso

Qualora un ente fosse già dotato delle presenti soluzioni tecnologie (es. SIEM) potrà mantenere tali soluzioni, prevedendone una gestione autonoma ed una eventuale integrazione con le soluzioni del CERT al fine di garantire un efficace scambio informativo. Resta inteso che il CERT di Regione del Veneto erogherà i servizi centralizzati tramite le soluzioni identificate in fase di progettazione del CERT stesso.

Il CERT di Regione del Veneto raccoglie, oltre alle segnalazioni di incidenti informatici, le vulnerabilità e le potenziali minacce, analizzando gli impatti che si potrebbero verificare sulle

infrastrutture informatiche del proprio perimetro (o sull'organizzazione stessa di Regione del Veneto) così da identificare i rischi e dunque le più adeguate contromisure.

Nella Figura seguente è descritto il flusso di interazione tra le varie tecnologie facenti parti dell'ecosistema del CERT Regionale.

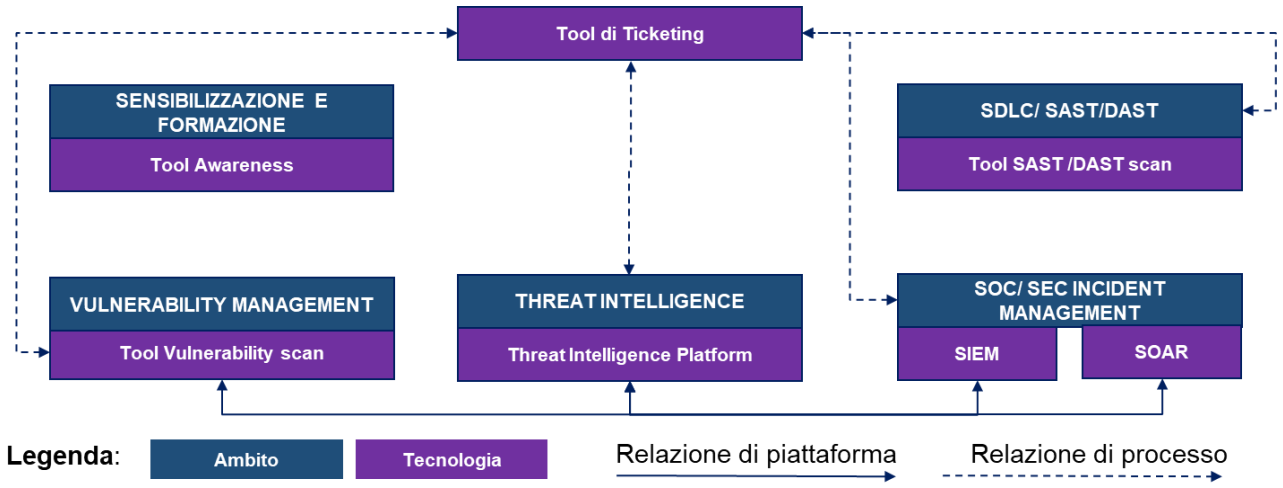


Figura 19 – Modello relazionale delle tecnologie in uso

8.3.4 Modello di riferimento

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.

Nel proseguo, tale modello operativo viene declinato per ciascun servizio che verrà erogato dal CERT Regionale.

In una prima fase del progetto esecutivo tale modello sarà, inoltre, applicato all'implementazione stessa del CERT Regionale, durante la quale il modello prevederà per ciascuna fase:

- **Attivazione**: fase che ricomprenderà le attività preliminari di identificazione delle risorse a supporto, l'esecuzione delle attività preliminari per la strutturazione e l'implementazione del CERT Regionale quale ingaggio delle terze parti, contrattualizzazione dei servizi, condivisione di ruoli e responsabilità, formalizzazione di policy e procedure.

- **Configurazione**: tale fase prevederà, una volta ingaggiati tutti gli stakeholder, le attività di implementazione vera e propria del CERT Regionale tramite l'esecuzione di specifici progetti di trasformazioni necessari per permettere al CERT Regionale di operare come riportato all'interno del presente documento.
- **Erogazione**: una volta implementato il CERT, tale fase prevede l'attivazione dei servizi, l'ingaggio degli Enti e la fase di operatività standard del CERT Regionale, come da modello definito.

8.3.5 Caratterizzazione dei servizi

Vengono di seguito descritti i modelli operativi di ogni singolo servizio. In particolare, per ciascuno di essi, viene riportato:

- Una descrizione di dettaglio del servizio stesso.
- Regole e flussi di funzionamento del servizio.
- Modello operativo.

8.3.5.1 Gestione del rischio

Dettagli del servizio

Il servizio ha l'obiettivo di valutare il livello di rischio di un Ente, basandosi sulla normativa di riferimento e sugli standard internazionali (quali ad es. NIST, ISO 27001, ISO 31000) e identificare quindi le priorità di intervento in ambito sicurezza.
La metodologia di riferimento prevede l'implementazione di un Framework specifico che identifichi tutti i controlli che devono essere effettuati per determinare se gli ambiti di sicurezza presi in considerazione sono opportunamente presidiati.
Tale framework prevederà una matrice di riferimento al fine di calcolare, per ciascun ambito ed ogni specifico controllo, il livello di rischio, confrontare tale livello con la soglia di accettazione del rischio stabilita, censire i controlli attualmente adottati dall'Ente e identificare le principali aree di scopertura.
Il framework di riferimento prevederà inoltre specifici interventi standard in base alle scoperture rilevate, così da garantire un processo efficiente ed efficace nella definizione delle azioni di rimedio che ogni singolo Ente dovrà poi implementare.
Durante la fase di implementazione delle azioni di rimedio, il CERT Regionale avrà il compito di monitorare l'andamento di tali implementazioni così da raccogliere ed indirizzare eventuali problematiche.
Il processo di valutazione del rischio verrà svolto con **cadenza annuale**, in ottica di miglioramento continuo e per assicurare il rispetto allo standard ISO 27001.
Tale servizio verrà erogato tramite giornate uomo e non prevede alcun tool a supporto.

Modello operativo

Di seguito viene riportato il modello operativo per il servizio Gestione del rischio.

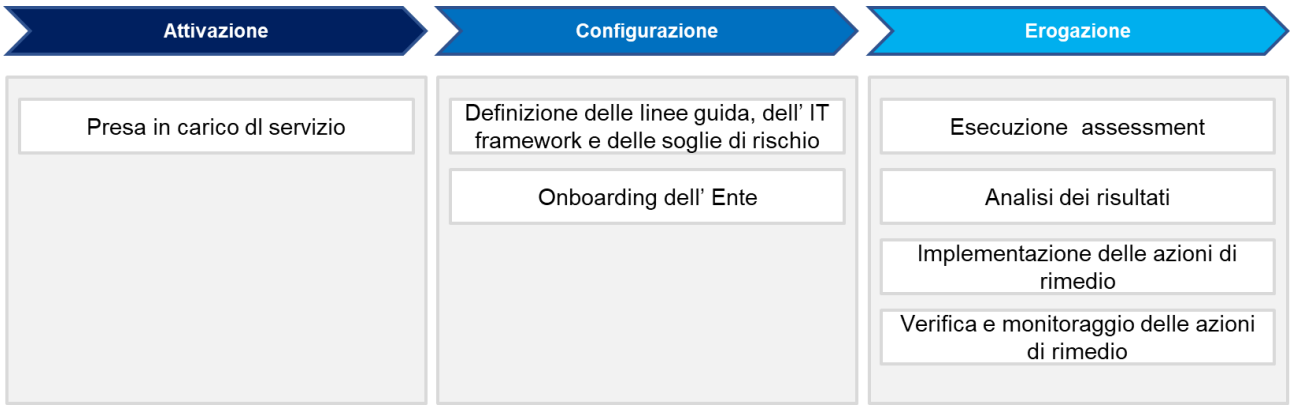


Figura 20 - Fasi del Servizio della gestione del rischio

Regole e flussi di funzionamento del servizio

Il modello operativo prevede una fase di progettazione finalizzata alla definizione delle linee guida e delle soglie di rischio in carico al CERT di Regione del Veneto con il supporto consulenziale di una terza parte, al fine di identificare il framework di riferimento per l'analisi del rischio adottato dal CERT Regionale; è prevista una successiva fase di esecuzione del servizio in carico parzialmente al CERT di Regione del Veneto che ha il compito di effettuare gli assessment su ogni singolo ente aderente e analizzare e condividere con ogni singolo ente gli esiti delle attività di analisi svolte. L'implementazione delle azioni di rimedio è in carico al singolo ente ad eccezione degli Enti appartenenti al gruppo 5 per i quali l'attività potrebbe essere in carico al CERT di Regione del Veneto.
È compito del CERT di Regione del Veneto monitorare l'implementazione di tali azioni di rimedio.
Il modello operativo del CERT Regionale prevede l'esecuzione delle fasi di operation con **cadenza annuale** nonché la revisione delle linee guida e delle soglie di rischio **ogni qual volta ne emergesse l'esigenza a seguito di emanazione di specifiche norme oppure a seguito dell'evoluzione del contesto di riferimento**.

Di seguito è rappresentato il modello operativo del servizio "Gestione del Rischio" del CERT di Regione del Veneto e la caratterizzazione del processo in termini di attori coinvolti, dati in input ed output e presenza o meno di una tecnologia dedicata.

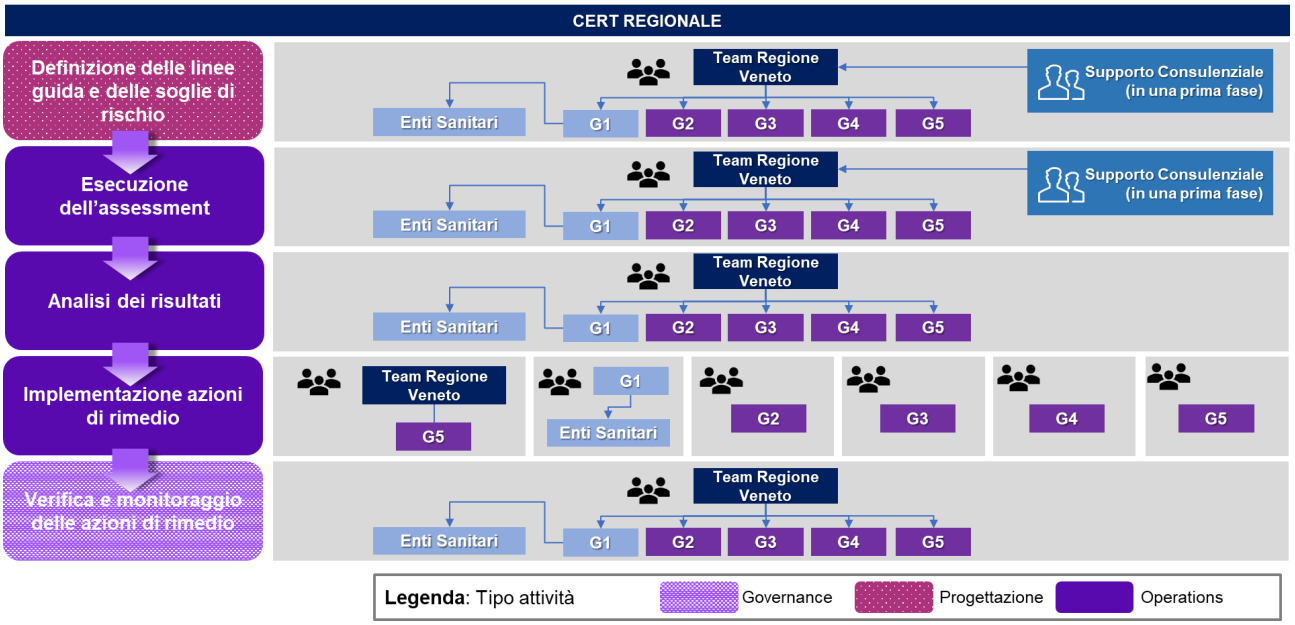


Figura 21 – Modello Operativo della gestione del rischio

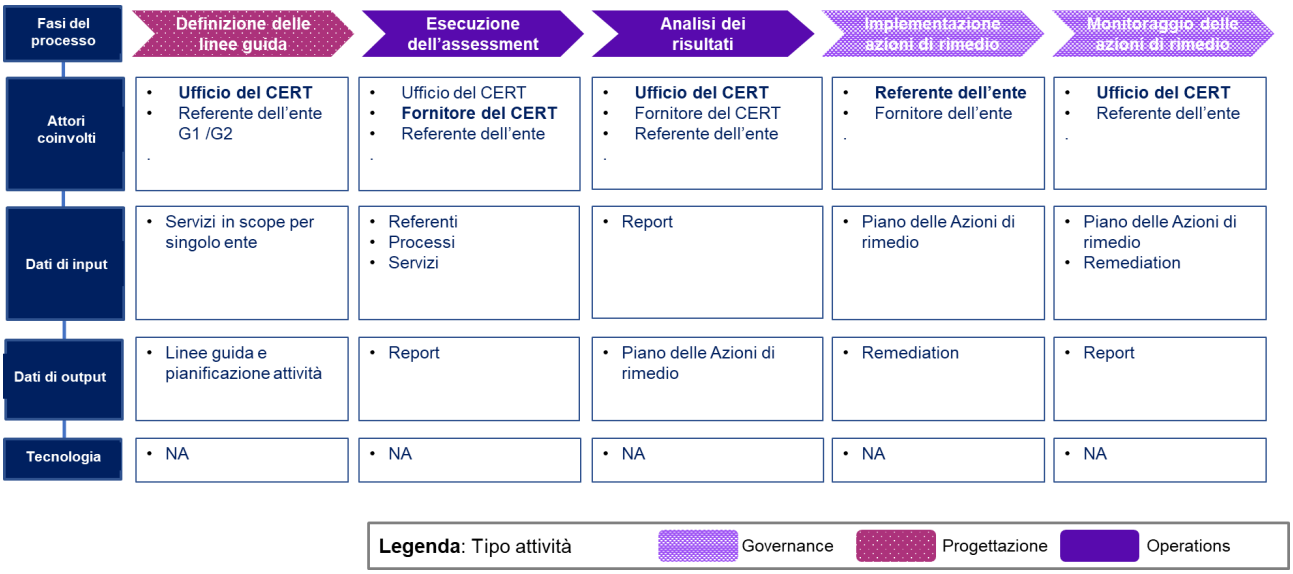


Figura 22 - Caratterizzazione del Modello Operativo della gestione del rischio

8.3.5.2 Business Continuity

Dettagli del servizio

Il servizio ha l'obiettivo di supportare l'Ente nel proteggere e ridurre la probabilità di incidenti e assicurare le attività la ripresa in seguito a interruzioni.

Nel dettaglio il servizio erogato dal CERT prevede un supporto nella fase di definizione delle esigenze e valutazione delle soluzioni adottate dall'Ente. Sono escluse invece dall'ambito dei servizi l'implementazione delle soluzioni di Business Continuity e Disaster Recovery.
La metodologia prevede la definizione di linea guida per garantire un approccio standardizzato alla continuità operativa basato sulla normativa di riferimento e sugli standard internazionali (quali ad es. ISO 27001 e 22301). Tali linee guida consentiranno inoltre di definire dei requisiti minimi che ciascun Ente dovrà garantire in termini di disponibilità del sistema informativo, sulla base dei servizi erogati e la loro relativa criticità.
In particolare, verranno definiti i tempi di ripristino ed i livelli minimi da garantire, sulla base dei servizi erogati. Il CERT supporterà gli enti nella fase di analisi e di formalizzazione delle procedure di continuità operativa, così da garantire un approccio standard a livello regionale.

Modello operativo

Di seguito viene riportato il modello operativo per il servizio Business Continuity.

Figura 23 - Fasi del Servizio della Business Continuity

Regole e flussi di funzionamento del servizio

Il modello operativo prevede una fase di progettazione finalizzata alla definizione delle linee guida e delle regole per la stesura e aggiornamento dei Piani di Business Continuity e Disaster Recovery in carico a Regione del Veneto, eventualmente con il supporto consulenziale di una terza parte, al fine di identificare le best practices di riferimento e la strategia per la Business Continuity adottata dal CERT Regionale. Il modello operativo prevede una successiva fase di esecuzione del servizio, in carico parzialmente a Regione del Veneto, che ha il compito di effettuare la Business Impact Analysis su ogni singolo ente aderente e analizzare e condividere con ogni singolo ente gli esiti delle attività svolte ed i relativi impatti sul Business, ad eccezione degli enti (di qualsiasi gruppo) che hanno il Data Center in outsourcing presso Regione del Veneto o degli Enti appartenenti al gruppo 5 per i quali l'attività è in carico a al CERT di Regione del Veneto. La pianificazione dei Test BC/DR (antecedente tale fase) è in carico al CERT di Regione del Veneto. L'implementazione dei piani di rimedio è parzialmente in carico al singolo ente, ad eccezione degli enti (di qualsiasi gruppo) che hanno il Data Center in outsourcing presso Regione del Veneto o degli Enti appartenenti al gruppo 5 per i quali l'attività potrebbe essere in carico al CERT di Regione del Veneto.
È compito del CERT di Regione del Veneto monitorare l'implementazione di tali azioni di rimedio.
Il modello operativo del CERT Regionale prevede l'esecuzione delle fasi di operation con cadenza annuale nonché la revisione delle linee guida e delle soluzioni di BC/DR ogni qual volta ne emergesse la necessità.

Di seguito è rappresentato il modello operativo del servizio "Business Continuity" del CERT di Regione del Veneto e la caratterizzazione del processo in termini di attori coinvolti, dati in input ed output e presenza o meno di una tecnologia dedicata.

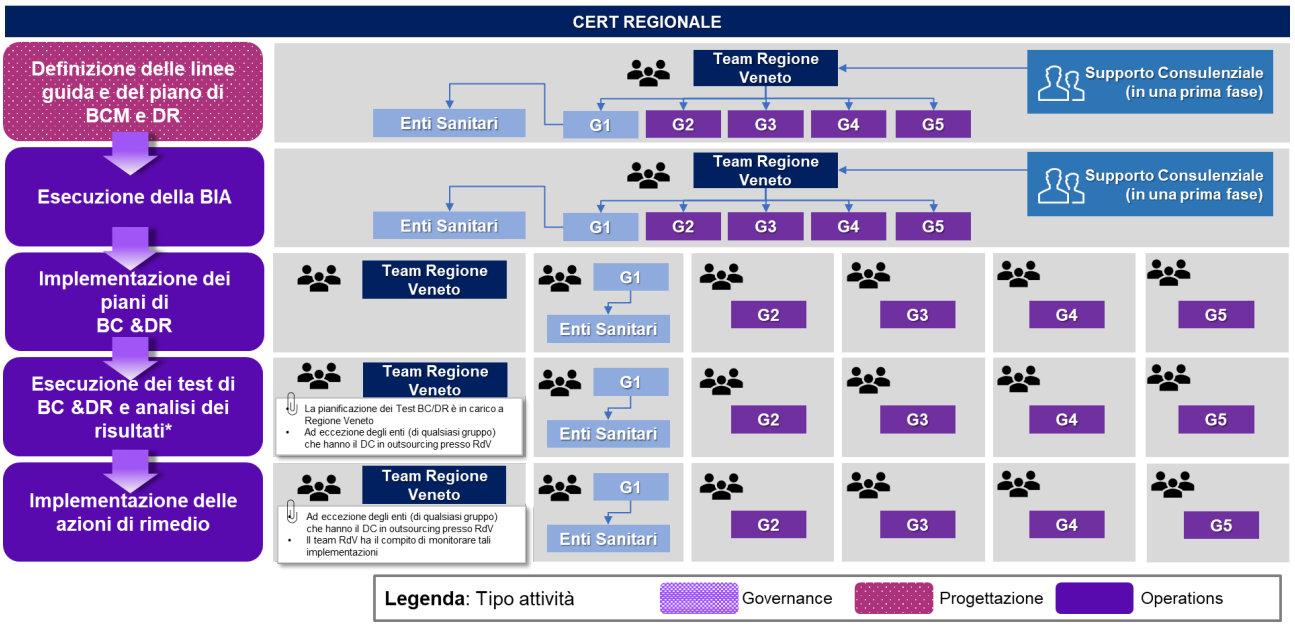


Figura 24 – Modello Operativo della Business Continuity

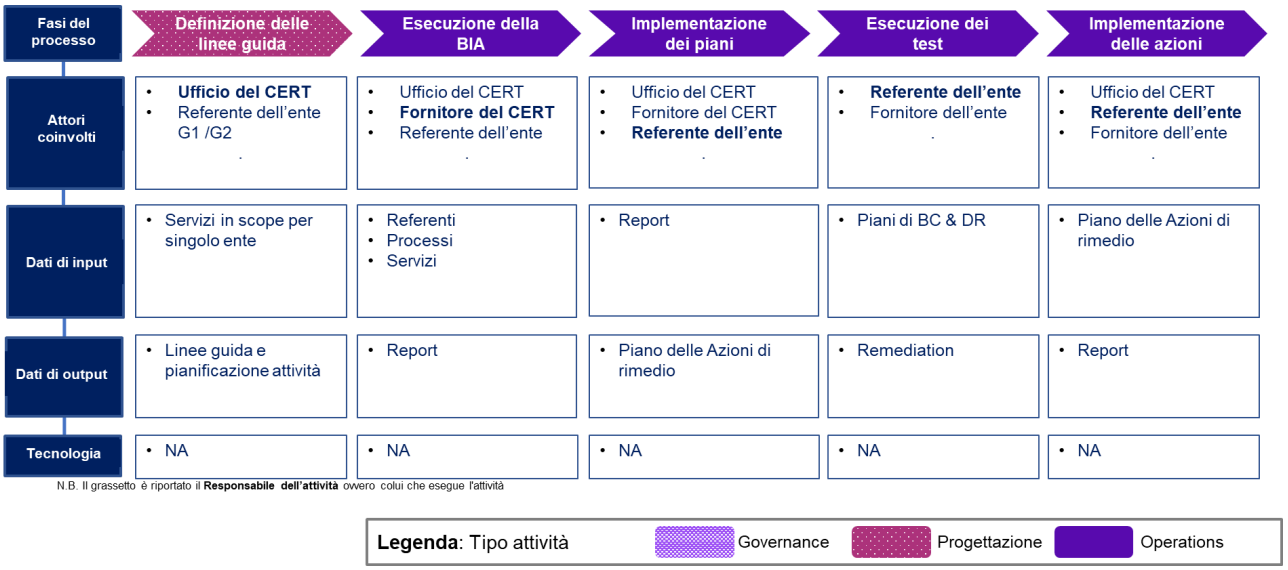


Figura 25 - Caratterizzazione del Modello Operativo della Business Continuity

8.3.5.3 Sensibilizzazione e Formazione

Dettagli del servizio

I contenuti di sicurezza informatica richiedono approcci specialistici per poter essere efficaci in quanto si rivolgono ad una platea molto eterogenea in termini di competenze e necessità. Come prima cosa, occorre definire quali sono i target dell'iniziativa, successivamente quali contenuti devono essere sviluppati e qual è il mezzo di comunicazione più efficace, tenuto conto dei messaggi da veicolare e dei target a cui questi sono rivolti. È inoltre previsto che lo sviluppo della consapevolezza nelle persone e l'efficacia del programma siano supportati da metriche e strumenti di monitoraggio appropriati. Per ogni iniziativa è impostato e analizzato un KPI specifico.
Tale approccio consente di definire un modello di servizio specifico per il CERT Regionale che prevede:

- **Segmentazione audience**: identificazione e clusterizzazione dei target da coinvolgere nel programma di formazione distinguendo il personale operativo dal personale con ruoli di responsabilità.
- **Definizione canale di erogazione**: identificazione del canale di erogazione delle iniziative (privilegiando il canale e-learning ritenuto il più efficace per raggiungere il personale).
- **Sviluppo dei contenuti**: definizione dei contenuti da erogare in funzione del target identificato e aggiornamento degli stessi con cadenza periodica in base all'evoluzione delle minacce di sicurezza e del contesto operativo degli enti aderenti.
- **Erogazione dei contenuti**: fornitura del servizio di e-learning tramite piattaforma dedicata su cui vengono abilitati gli utenti e che include i moduli di verifica dell'apprendimento e programmazione, su specifica richiesta, di sessioni in aula e/o da remoto con specialisti di sicurezza per l'approfondimento di specifiche tematiche.
- **Verifica apprendimento**: introduzione di strumenti di verifica delle competenze tramite campagne interattive (es. simulazioni di phishing) e campagne di gaming.

I servizi di awareness saranno erogati utilizzando canali e strumenti studiati specificamente per rispondere alle esigenze dei singoli utenti e che saranno definite in funzione di:

- Rischi di sicurezza indotti da ruolo/mansione ricoperti e dagli strumenti informatici utilizzati.
- Livello di conoscenza di partenza verificato tramite test di valutazione.

- Disponibilità di tempo e strumenti per accedere ai servizi di awareness. Tra i canali e gli strumenti che si intende utilizzare si evidenziano: training online, corsi in aula, newsletter e e-card, webinar, brochure, quiz, campagne di simulazione, podcast, consigli del giorno, ebook.
- La piattaforma sarà realizzata in modo da essere utilizzabile secondo le indicazioni dell'AgID e nel rispetto delle linee guida di accessibilità che garantiscono la fruizione a tutte le categorie di utente.

Modello operativo

Di seguito viene riportato il modello operativo per il servizio Sensibilizzazione e Formazione.

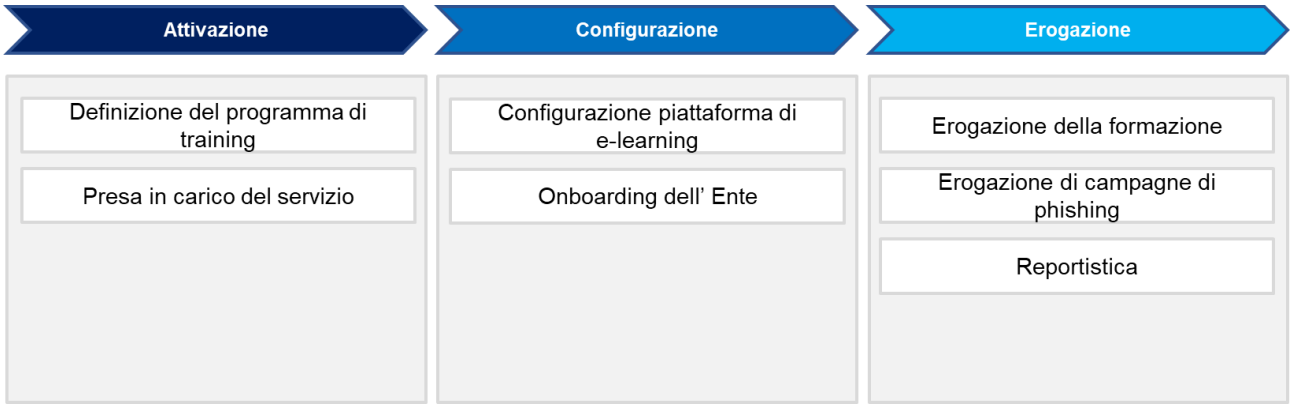


Figura 26 - Fasi del Servizio della Sensibilizzazione e formazione

Regole e flussi di funzionamento del servizio

Il servizio si compone di una prima fase di progettazione finalizzata alla definizione delle linee guida e degli obiettivi di formazione in carico al CERT di Regione del Veneto. Le due attività operative relative alla predisposizione delle campagne di formazione e di phishing sono in carico al CERT di Regione del Veneto e verranno erogate a tutti gli enti aderenti tramite l'utilizzo di una piattaforma di e-learning.
L'ultima fase di governance per l'analisi ed il reporting risulta in carico al CERT di Regione del Veneto ma gli output saranno condivisi con i singoli enti aderenti; tale attività sarà effettuata sempre tramite la piattaforma di e-learning selezionata.

Di seguito è rappresentato il modello operativo del servizio "Sensibilizzazione e Formazione" del CERT di Regione del Veneto.

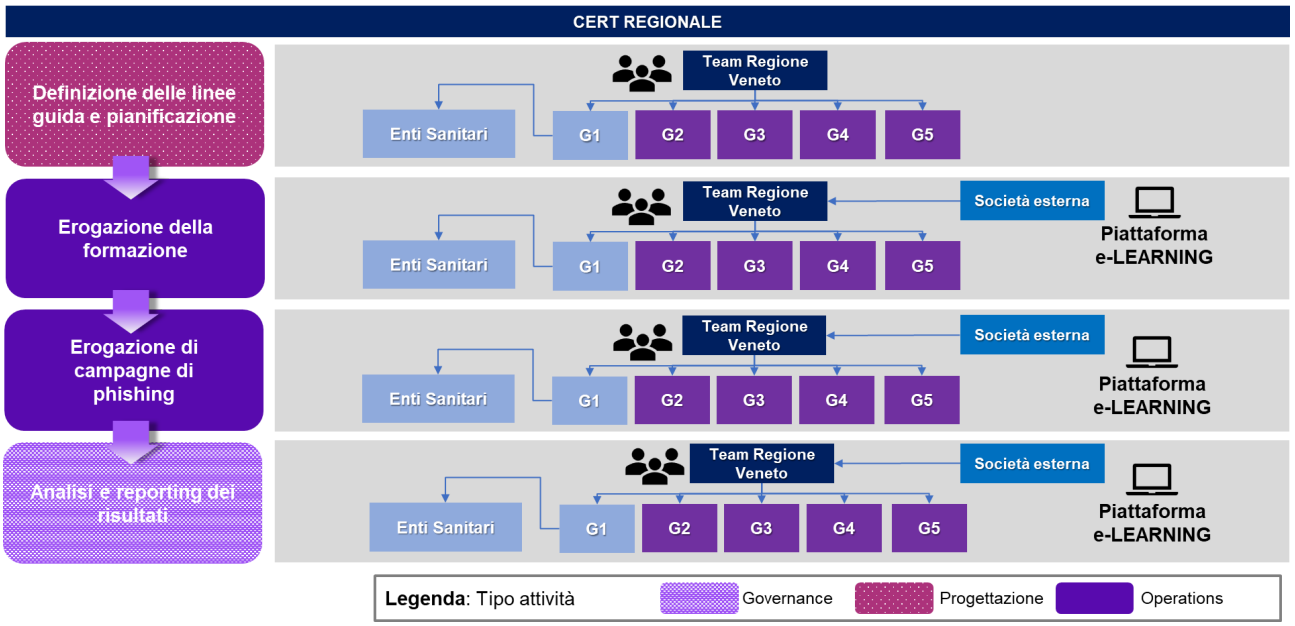


Figura 27 – Modello Operativo della Sensibilizzazione e formazione

8.3.5.4 Altri servizi

Dettagli del servizio

Il servizio ha l'obiettivo di garantire un supporto specialistico aggiuntivo per alcuni servizi specifici, sulla base di esigenze e peculiarità di singolo Ente.
Tali servizi verranno erogati tramite una terza parte con competenze approfondite nei seguenti ambiti:

- Gestione del rischio.
- Business Continuity.
- Sensibilizzazione e formazione.
- Sviluppo Sicuro.
- ISO 27001.

Tale servizio verrà erogato tramite giornate uomo e non prevede alcun tool a supporto.

Modello operativo

Di seguito viene riportato il modello operativo per il servizio Altri servizi.

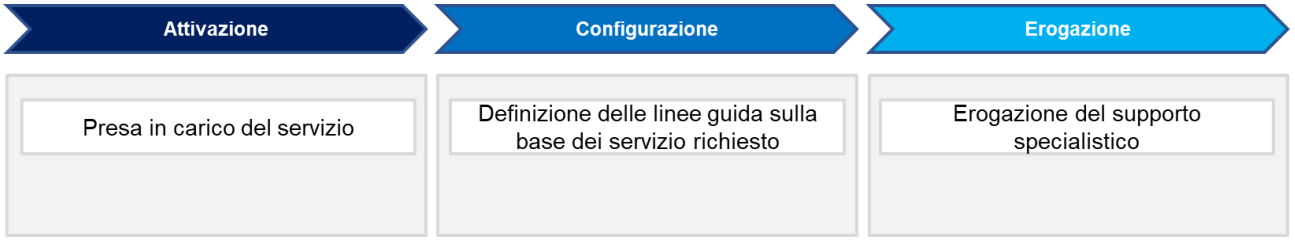


Figura 28 - Fasi del Servizio -Altri Servizi

Regole e flussi di funzionamento del servizio

Gli "altri servizi" prevedono l'erogazione di attività consulenziali di una terza parte, finalizzate alla gestione dei servizi di sicurezza o alla loro attivazione, supportando gli enti aderenti a livello tecnico e strategico. Il servizio sarà erogato dal CERT di Regione del Veneto verso tutti gli enti aderenti.

Di seguito è rappresentato il modello operativo del servizio "Altri Servizi" del CERT di Regione del Veneto.

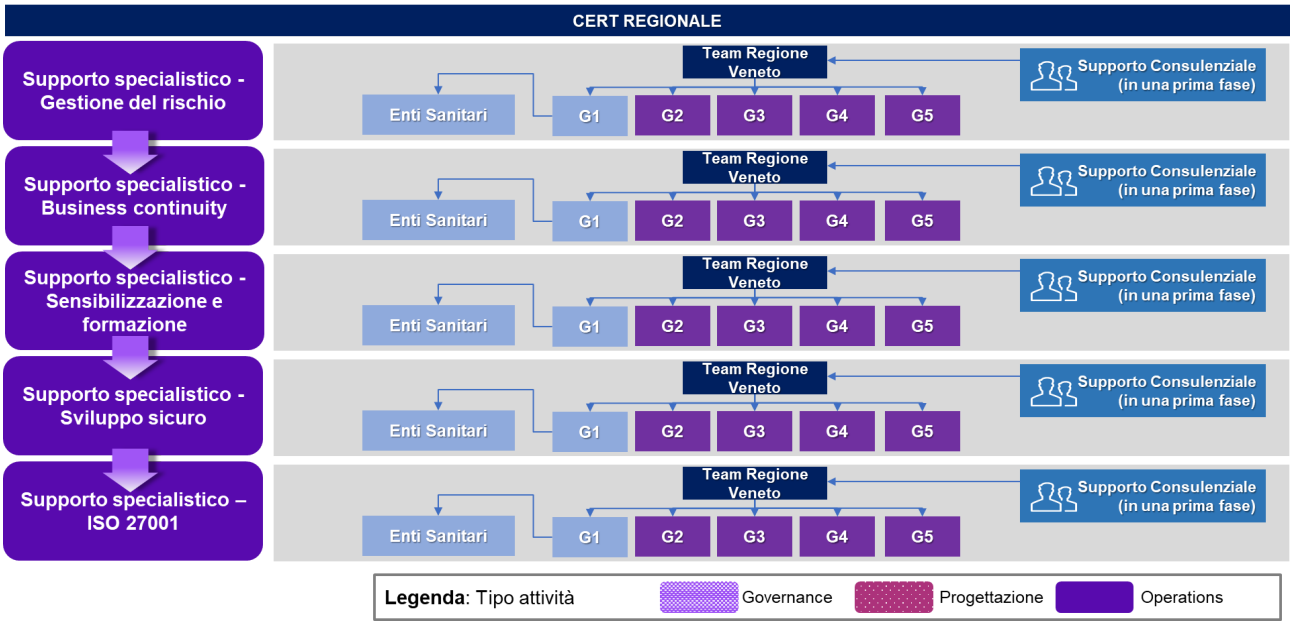


Figura 29 – Modello Operativo "Altri Servizi"

8.3.5.5 SOC/ Incident Management

Dettagli del servizio

Il servizio proposto di SOC / Incident Management ha l'obiettivo di individuare nel minor tempo possibile gli attacchi ai danni dell'Integrità, Confidenzialità e/o Disponibilità del patrimonio informativo degli Enti aderenti al CERT Regionale. A fronte della rilevazione e della convalida dell'incidente, viene innescato il processo di Incident Management supportato dalle informazioni di dettaglio fornite in fase di rilevazione evento, contestualizzate e arricchite per assegnare la corretta priorità all'incidente e per correlare informazioni sugli Indicatori di Compromissione (IOC) e Tactics Techniques and Procedure (TTP) del MITRE ATT&CK relative al potenziale Threat Actor.

Il modello operativo del SOC si basa su una stretta collaborazione tra i macro-processi di Rilevazione Evento e Gestione Incidente.
Nello specifico, il macro-processo Rilevazione Evento si articola nei sottoprocessi seguenti:

- **Raccolta delle sorgenti dati**: repository consolidato e scalabile di dati di sicurezza, inclusi eventi, asset, flussi e informazioni di contesto.
- **Attivazione di use case e regole di correlazione**: include la definizione, consolidamento e attivazione di un insieme di regole di correlazione di interesse per lo specifico contesto dell'Ente aderente. I presenti use case e regole di correlazione saranno implementati tenendo in considerazione le peculiarità infrastrutturali dei singoli enti.
- **Monitoraggio del SIEM e alerting**: il processo garantisce il monitoraggio continuo delle

informazioni prodotte dal SOC. Questo include l'utilizzo di dashboard e canali necessari al monitoraggio continuo e completo dei sistemi, che permettano di avere visibilità sulla postura di sicurezza degli Enti aderenti al CERT.
- **Contenimento di breve periodo**: Identificazione delle possibili azioni correttive da intraprendere nell'immediato per contenere l'attacco e prevenirne la propagazione.

Il macro-processo di Gestione Incidente, si articola nei seguenti sottoprocessi:
- **Raccolta e trasmissione delle evidenze**: Acquisizione di eventuali evidenze digitali da utilizzare nella ricostruzione di quanto accaduto in seguito all'incidente.
- **Risoluzione dell'incidente e ripristino**: Azioni necessarie per rispondere all'incidente in maniera pervasiva. La risoluzione dell'incidente include inoltre una valutazione a posteriori, in modo da individuare possibili azioni migliorative da implementare sui sistemi di sicurezza e aumentare l'efficacia del SOC.
- **Supporto escalation incidenti critici**: In caso di incidenti di sicurezza critici, è previsto un processo di escalation al fine di investigare in maniera estesa sulla natura del problema.

Il servizio prevede oltre alle attività sopraelencate tipiche di un SOC, le seguenti funzionalità:

- **Contestualizzazione e arricchimento eventi:** Tutti gli eventi di sicurezza raccolti dal servizio SOC del CERT di Regione del Veneto sono correlati e arricchiti con le informazioni fornite dagli altri servizi integrati attivi sugli enti aderenti, in modo da calare i dati raccolti e gli alert identificati sullo specifico contesto e velocizzare le attività degli analisti.
- **Use case Tuning & Improvement**: L'esperienza maturata sui casi/incidenti gestiti sui singoli Enti viene utilizzata per migliorare continuamente la libreria di use case sviluppati dal servizio SOC del CERT, minimizzando il numero di falsi positivi, migliorando l'efficienza dei team di analisti ed eventualmente inferendo soglie di alert o use case aggiuntivi rilevanti tramite ML/deep learning. Nel caso in cui l'ente sia dotato di una propria piattaforma SIEM il fine tuning degli use case potrà essere effettuato dall'ente stesso. Nella definizione delle responsabilità per la definizione del fine tuning saranno inoltre considerate le peculiarità del singolo ambiente (es. Gestione degli apparati medicali)
- **Contenimento automatico delle minacce**: Il servizio SOAR implementato dal SOC, integrato con le soluzioni di sicurezza in ambito al CERT offre una risposta automatica efficace di primo intervento sulle piattaforme tecnologiche relative ai servizi attivi sui singoli Enti, permettendo di ridurre sensibilmente i tempi di intervento.
- **Case Management Assistito**: Implementazione di playbook di automazione che permettono di arricchire automaticamente le informazioni collezionate con le fonti di Intelligence oppure assegnare la priorità ai case aperti.
- **Threat Intelligence & Vulnerability Data feed**: Le soluzioni di Threat Intelligence e Vulnerability Data feed sono utilizzate internamente dal SOC come fonte di arricchimento degli eventi di sicurezza raccolti in relazione al contesto del panorama delle minacce globale di interesse per il CERT di Regione del Veneto.

Modello operativo

Al netto della fase di setup iniziale delle soluzioni tecnologiche in uso dal SOC, l'attivazione del servizio passa per un approccio a fasi, con l'obiettivo di identificare e predisporre la raccolta dei log di interesse e attivare le regole di correlazione per lo specifico contesto. Si riporta nel seguito il modello operativo per il servizio SOC/Incident Management nonché una descrizione delle singole fasi.

Figura 30 - Fasi del Servizio SOC / Incident Management

Regole e flussi di funzionamento del servizio

Il modello operativo prevede una fase di progettazione finalizzata alla definizione delle linee guida e del piano di risposta agli incidenti, che definisce le attività, i ruoli e le responsabilità in caso di minaccia o incidente in carico al CERT di Regione del Veneto, eventualmente con il supporto consulenziale di una terza parte.
La parte di Operations si divide in due fasi di **Rilevazione Evento** e di **Gestione dell'Incidente**, ognuna delle quali si suddivide in due livelli di azione.

- Il **livello L1** della fase di Rilevazione evento "**Monitoraggio console**" è un'attività di Triage che viene effettuata dal CERT di Regione del Veneto per gli Enti aderenti non dotati di piattaforma SIEM o dai singoli enti (appartenenti al gruppo G2) in caso questi siano dotati di SIEM. In questo ultimo caso, il SIEM del CERT di Regione del Veneto funge da HyperSIEM rispetto ai SIEM degli enti aderenti.
- Il **livello L2** della fase di Rilevazione evento "**Gestione Evento**" è un'attività di Contenimento in cui il CERT di Regione del Veneto prende in gestione l'evento segnalato dal livello L1 per identificare le azioni preliminari di contenimento o caratterizzarlo come incidente di Sicurezza. Gli Enti aderenti al gruppo G1 possono chiedere supporto al team CERT di Regione del Veneto On Demand.
- Il **livello L1** della fase di "**Gestione dell'Incidente**" è un'attività di gestione degli incidenti di Sicurezza che viene effettuata dai singoli Enti. Si prevede il supporto di Regione del Veneto a coordinamento delle attività. Eventuale supporto operativo da parte di terze parti potrà essere acquistato on demand direttamente dall'ente.
- Il **livello L2** della fase di "**Gestione dell'Incidente**" è un'attività di gestione di quegli incidenti che abbiano un impatto particolarmente critico o un impatto a livello regionale Tale attività viene coordinata da Regione del Veneto. Eventuale supporto operativo da parte di terze parti potrà essere acquistato on demand direttamente dall'ente.

Di seguito è rappresentato il modello operativo del servizio "SOC / Incident Management" del CERT di Regione del Veneto e la caratterizzazione del processo in termini di attori coinvolti, dati in input ed output e presenza o meno di una tecnologia dedicata.

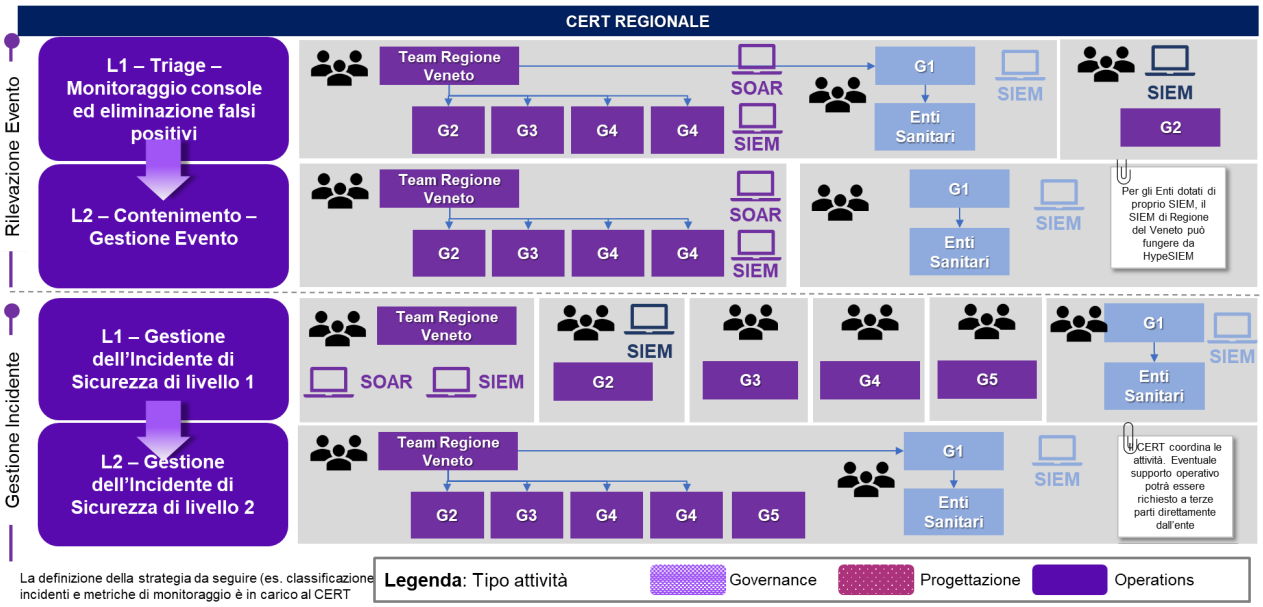


Figura 31 – Modello Operativo SOC / Incident Management

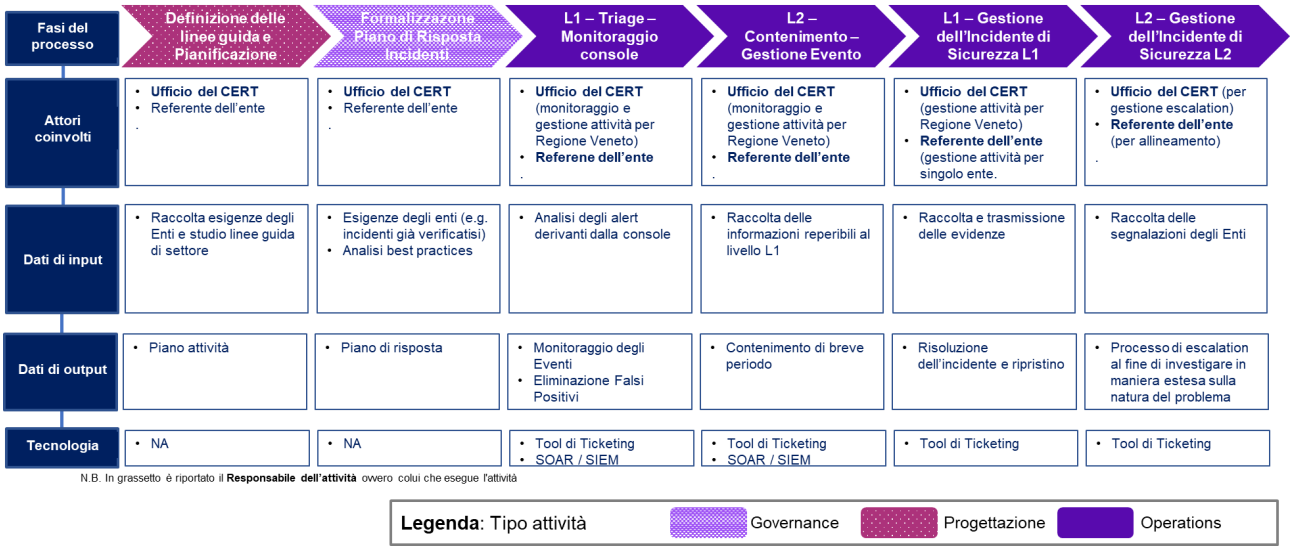


Figura 32 - Caratterizzazione del Modello Operativo

Di seguito uno schema di sintesi dei flussi informativi tra SOC Regionale e SOC degli Enti aderenti.

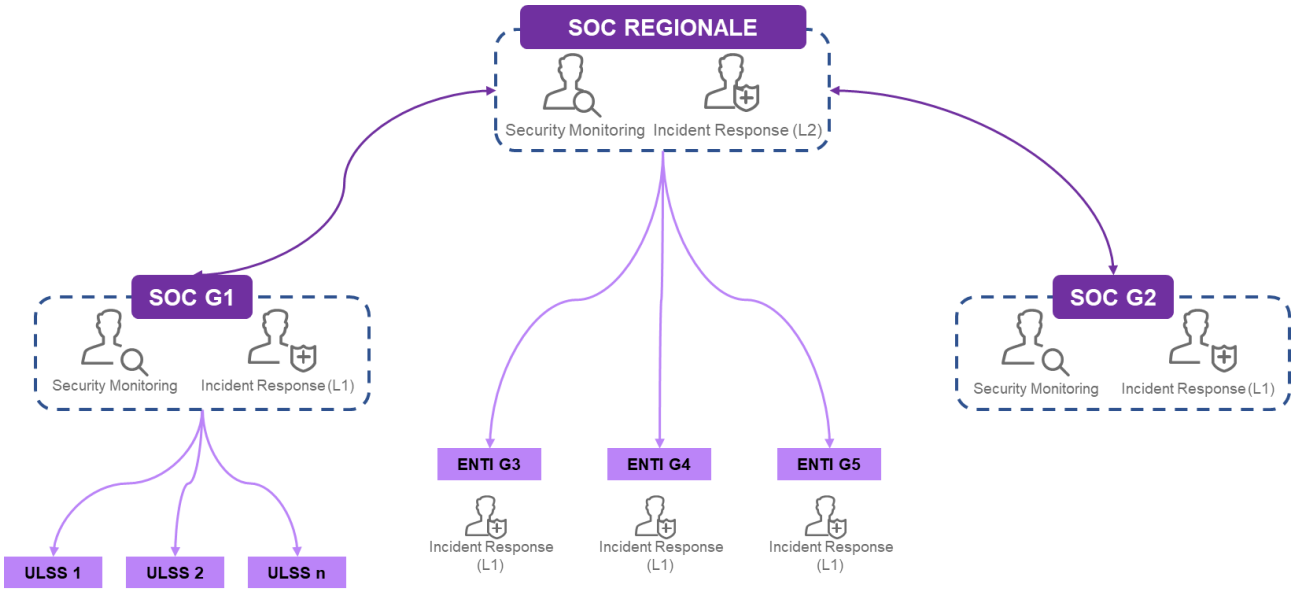


Figura 33 – Flussi Informativi del servizio SOC / Incident Management

8.3.5.6 Vulnerability Management

Dettagli del servizio

Il servizio in oggetto ha lo scopo di rilevare, monitorare e ridurre la superfice d'attacco esposta dagli enti aderenti al CERT Regionale.
Il servizio prevede la gestione dell'intero ciclo di vita delle vulnerabilità attraverso l'adozione da parte del CERT Regionale di una piattaforma integrata con gli altri sistemi di controllo (SIEM/ SOAR, Threat Intelligence). All'interno del servizio saranno erogate anche attività di penetration testing.
Di seguito sono rappresentate le principali features del tool di Vulnerability Management:

- Rilevazione delle vulnerabilità presenti in sistemi, apparati di rete, applicazioni (web, mobile, client-server, etc.), dispositivi ad uso professionale e personale, con rendicontazione delle tecniche, dirette od articolate (OWASP, MITRE kill-chain, etc.) capaci di sfruttarle;
- Categorizzazione, classificazione e misura del potenziale impatto delle vulnerabilità rilevate, sulla base della misura del rischio ponderato con il livello di criticità associato all'asset e derivante dalla rilevanza dei processi degli Enti che l'asset abilita, dalla sensibilità dei dati trattati e delle interdipendenze (con altre funzioni e/o sistemi), unitamente alle indicazioni sulle modalità tecniche, organizzative e procedurali di risoluzione (o mitigazione) delle problematiche riscontrate.
- Pianificazione, su base priorità delle azioni di risoluzione o mitigazione delle problematiche di sicurezza individuate e delle fasi di controllo orientate al rientro dalle non conformità e al miglioramento continuo.
- Reportistica relativa alle scansioni continue con un alto grado di personalizzazione di elementi quali: superficie d'attacco esposta, livelli di rischio residuo, vulnerabilità associate agli asset (pregresse ed attuali) e stato d'avanzamento dei piani di rientro.

Modello operativo

Di seguito viene riportato il modello operativo per il servizio Vulnerability Management.

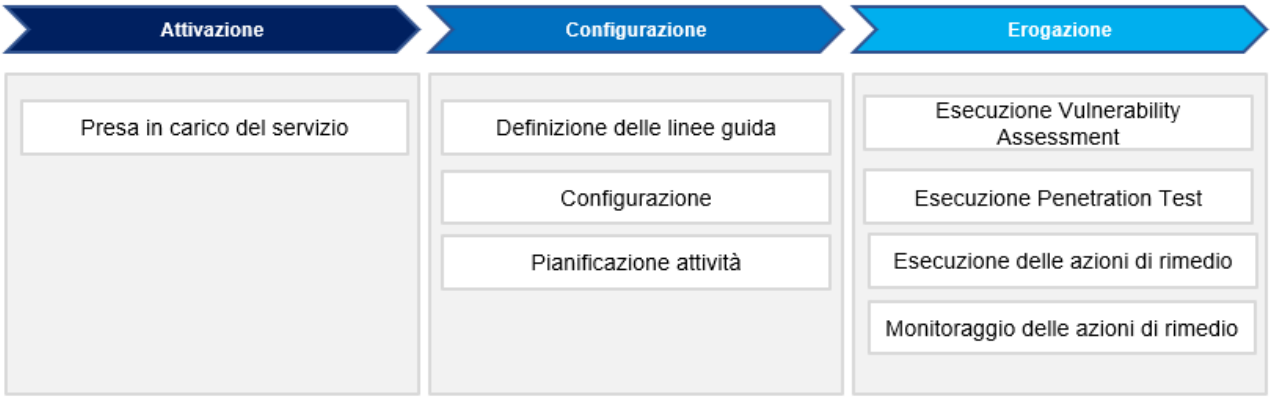


Figura 34 - Fasi del Servizio di Vulnerability Management

Regole e flussi di funzionamento del servizio

Il modello operativo prevede una prima fase di progettazione in carico a Regione del Veneto, eventualmente con il supporto consulenziale di una terza parte, che definisca le linee guida e un set di regole comuni per l'identificazione, la classificazione e il monitoraggio delle vulnerabilità che riguardano l'intera infrastruttura IT, gli asset e i sistemi tecnologici di Regione del Veneto e degli Enti aderenti.
Il CERT di Regione del Veneto coordina le attività tra i team degli Enti aderenti per l'aggiornamento e il miglioramento continuo con l'obiettivo di aumentare il livello di automazione del servizio.
La successiva fase è relativa all'identificazione e caratterizzazione delle vulnerabilità tramite l'utilizzo di strumenti di scansione automatica continua o tramite l'esecuzione di penetration test da parte di personale qualificato. Anche tale fase è in carico a Regione del Veneto, eventualmente con il supporto consulenziale di una terza parte.
Il CERT di Regione del Veneto predispone inoltre le dashboard/ reportistica per gli Enti Aderenti e supervisiona le attività di risoluzione o mitigazione delle problematiche di sicurezza individuate (hardening, bug fixing, upgrading, fine tuning, replatforming, etc.). L'implementazione di tali azioni di rimedio è in carico al singolo Ente.

Di seguito è rappresentato il modello operativo complessivo del servizio "Vulnerability Management" del CERT di Regione del Veneto e la caratterizzazione del processo in termini di attori coinvolti, dati in input e output e presenza o meno di una tecnologia dedicata.

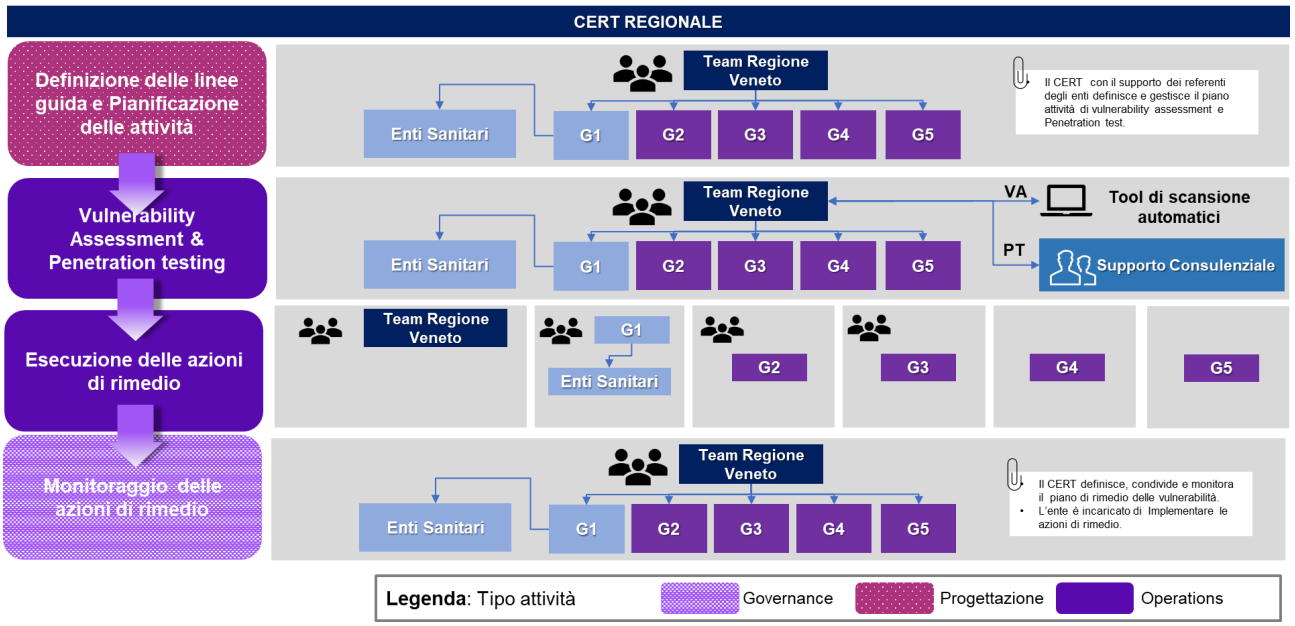


Figura 35 – Modello operativo Vulnerability management

Fasi del processo	Definizione delle linee guida e Pianificazione	Esecuzione test VA o PT	Esecuzione azioni di rimedio	Monitoraggio delle azioni di rimedio
Attori coinvolti	• **Ufficio del CERT** • Referente dell'ente	• Ufficio del CERT • **Fornitore (VA/PT)** • Referente dell'ente • Application Owner	• **Referente dell'ente** • Application Owner	• **Ufficio del CERT** • Referente dell'ente
Dati di input	• Esigenze degli enti in termini di richieste di servizi VA/PT	• Tipo di test (VA o PT) • Informazioni utili, IP, Url	• Report Tecnico	• Piano di rientro
Dati di output	• Piano attività	• Report Tecnico	• Piano di rientro • Remediation della vulnerabilità	• Report
Tecnologia	• Tool di Ticketing	• Tool Vulnerability scan	• Tool di Ticketing	• Console del CERT

N.B. In grassetto è riportato il **Responsabile dell'attività** ovvero colui che esegue l'attività

Figura 36 - Caratterizzazione del Modello Operativo

8.3.5.7 Threat Intelligence

Dettagli del servizio

Il servizio in oggetto è erogato avvalendosi di una piattaforma di Threat Intelligence che fornisce informative complete e continuative (feed) relative alle minacce e vulnerabilità di sicurezza, specificamente adattate al contesto del CERT di Regione del Veneto, grazie alla possibilità di utilizzare un'ampia quantità di fonti informative OSINT (Open Source Intelligence ad accesso libero) e CLOSINT (Closed Source Intelligence non liberamente disponibili).
Il servizio di TI consente di elaborare ed estrarre le informazioni necessarie attraverso le funzionalità offerte, di seguito descritte.

- **Accesso web**: la piattaforma basata sul linguaggio STIX fornisce un modello di rappresentazione dei dati che consente agli analisti di mettere in relazione nodi di informazioni su threat actor, malware, vulnerabilità, campagne, target, domini, e-mail di phishing, ecc. Tale struttura di da-ti consente un accesso più rapido ai dati rilevanti e la capacità di visualizzare le relazioni tra i diversi dati.
- **Personalizzazione delle informazioni**: la piattaforma consente di personalizzare le informazioni richieste in funzione dei sistemi adottati. Tramite l'interfaccia è possibile consultare i bollettini predisposti dal team di Threat Intelligence (TI) e generare report personalizzati.
- **Intelligence**: la piattaforma è gestita da un team specialistico di intelligence che ha l'obiettivo di arricchire le informazioni e contestualizzarle rispetto al contesto operativo della PA.

Analisi / Prioritizzazione: la piattaforma dispone di funzionalità atte a filtrare le informazioni in funzione delle necessità del CERT Regionale secondo meccanismi dinamici e continuativi che consentono di focalizzare l'attenzione sui fenomeni più rilevanti.

Modello operativo

Di seguito viene riportato il modello operativo per il servizio Threat Intelligence.

Figura 37 - Fasi del Servizio di Threat Intelligence

Regole e flussi di funzionamento del servizio

Il modello operativo prevede una prima fase di progettazione in carico a Regione del Veneto, che definisce le linee guida per lo scambio di informazioni e comunicazioni al fine di agevolare la diffusione di note tempestive e immediatamente utilizzabili su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cibernetici indirizzati a specifici settori o organizzazioni.
Una seconda fase, sempre in carico a Regione del Veneto, eventualmente con il supporto consulenziale di una terza parte, è dedicata alla raccolta di informazioni provenienti da varie fonti (e.g. feed OSINT / CLOSINT). Tali informazioni, raccolte tramite piattaforma designata, possono essere utilizzate per finalità strategiche, tattiche e operative, quali ad esempio, monitoraggio delle minacce e delle vulnerabilità, monitoraggio del Web, deep e dark web.
Inoltre, sarà possibile l'elaborazione e condivisione di report relativi agli scenari di rischio, alle vulnerabilità e alle attività di analisi svolte tramite richieste di informazioni da parte degli Enti.

Di seguito è rappresentato il modello operativo complessivo del servizio "Threat Intelligence" del CERT di Regione del Veneto e la caratterizzazione del processo in termini di attori coinvolti, dati in input ed output e presenza o meno di una tecnologia dedicata.

Figura 38 – Modello operativo Threat Intelligence

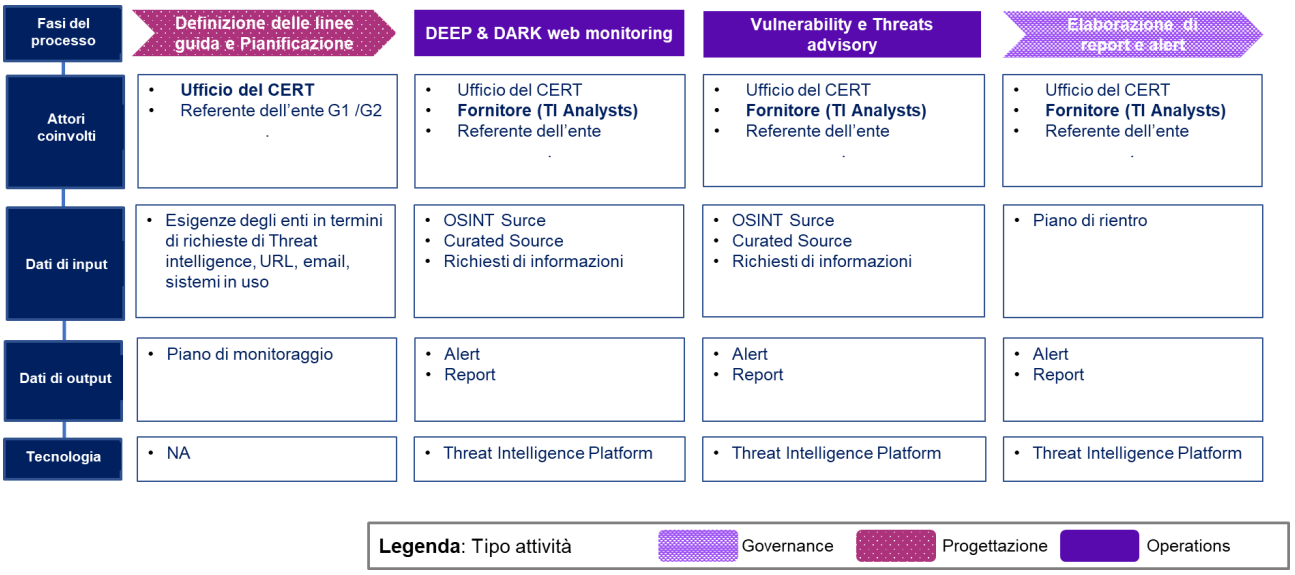


Figura 39 - Caratterizzazione del Modello Operativo

8.3.5.8 Sviluppo sicuro

Dettagli del servizio

Uno degli obiettivi del servizio è quello di incorporare la sicurezza nelle prime fasi del ciclo di vita del software attraverso un monitoraggio continuo delle nuove versioni delle applicazioni.
Il servizio in oggetto è erogato avvalendosi di tool automatici **SAST** e **DAST**.

Static Application Security Testing (SAST) è una metodologia AppSec che testa le applicazioni dall'interno verso l'esterno, esamina il codice binario e il codice dell'applicazione senza eseguirli per poter identificare eventuali "debolezze" e stabilire delle "buone abitudini" nello sviluppo sicuro del codice.

Questa attività in ambito al CERT Regionale è composta dalle seguenti fasi:

- **Codice sorgente**, che include l'attività di raccolta del codice sorgente e le informazioni necessarie per svolgere l'attività (ad esempio linguaggio, versione, strumenti, ecc.).
- **Controllo delle dipendenze**, che include le attività di compilazione del codice e il controllo delle dipendenze all'interno del codice.
- **Scansione del codice**, che include la scansione del codice utilizzando lo strumento per identificare la vulnerabilità di quest'ultimo.
- **Analisi dei risultati e remediation**, che include l'analisi dei falsi positivi e l'identificazione di azioni di rimedio alle vulnerabilità.
- **Reporting**, relativo gli esiti dell'attività.
- **Retest**, che prevede di ripetere il test delle attività sullo stesso codice dopo un tempo predeterminato o sul codice mitigato

Figura 40 – Fasi della Metodologia

I linguaggi di programmazione coperti da questa metodologia sono:

- Java(Script) / .NET / HTML5
- Mobile Source Code
- Technical (C / C++ / Delphi)
- ERP Code (ABAP, .NET, Java)
- Scripting Languages
- Data base Languages
- Native / Assembly / Firmware
- Siebel and Tibco (only manual checks)

Dynamic Application Security Tests (DAST) è un AppSec che permette di osservare nel dettaglio come si comporta l'applicazione quando è in esecuzione, di trovare defect prima di proseguire con le fasi successive del ciclo di vita del software, senza bisogno di condurre analisi approfondite del codice sorgente.

Questa attività in ambito al CERT Regionale è composta dalle seguenti fasi:

- **Prioritizzazione degli Asset**, che include il calcolo delle priorità per la definizione delle criticità delle vulnerabilità.
- **Asset Discovery** che include il processo di catalogazione delle risorse IT e il loro monitoraggio su base regolare.
- **Scansione delle vulnerabilità**, include la ricerca delle vulnerabilità mediante scansione su un perimetro definito.
- **Analisi dei risultati e remediation**, include l'analisi dei falsi positivi e della criticità delle vulnerabilità trovate e l'identificazione delle azioni di rimedio a tali vulnerabilità.
- **Reporting**, che include la preparazione dei deliverable dell'attività migliorando il livello di questi **Reporting**, relativo gli esiti dell'attività.
- **Retest**, che prevede di ripetere il test delle attività sullo stesso codice dopo un tempo predeterminato o sul codice mitigato.

Figura 41 – Fasi della Metodologia

Questa metodologia permette di coprire:

- Open-source Cores & customizzazioni basate su .NET, Java, PHP
- Web Services e applicazioni Cloud Based
- Android, iOS, applicazioni Windows Phone Mobile e Enterprise

Altri tipi di test eseguiti sul codice possono riguardare:

- **Black Box test:** in un test black-box, il tester viene inserito nel ruolo di hacker medio, senza alcuna conoscenza interna del sistema di destinazione.
- **Grey Box test**: in un test grey-box, il tester ha i livelli di accesso e conoscenza di un utente, potenzialmente con privilegi elevati su un sistema.
- **White Box test**: in un test white box, il tester ha pieno accesso al sistema, ai dati, al flusso di rete, alla documentazione dell'architettura e così via.

Modello operativo

Di seguito viene riportato il modello operativo per il servizio Sviluppo Sicuro.

Figura 42 – Fasi del Servizio di Sviluppo Sicuro

Regole e flussi di funzionamento del servizio

Il modello operativo prevede una prima fase di progettazione in carico a Regione del Veneto, che definisce le linee guida per lo sviluppo sicuro del software e lo sviluppo dei linguaggi di programmazione.
Questa prima fase prevede anche:

- La definizione dei requisiti di sicurezza delle applicazioni da adottare in fase di design dello sviluppo del software (interno e di terze parti).
- La definizione del modello di minaccia, la creazione di template e le linea guida per l'adozione della pratica di SDLC (Secure Development Life Cycle).
- L'esecuzione del Threat Modeling su un sottoinsieme di applicazioni ad elevato rischio potenziale per il CERT e i vari enti.

Una seconda fase, sempre in carico a Regione del Veneto, eventualmente con il supporto consulenziale di una terza parte, prevede il supporto on demand ai processi di sviluppo software tramite un Security Champion e l'utilizzo di strumenti di scansione.

Di seguito è rappresentato il modello operativo complessivo del servizio "Sviluppo Sicuro" del CERT di Regione del Veneto e la caratterizzazione del processo in termini di attori coinvolti, dati in input e output e presenza o meno di una tecnologia dedicata.

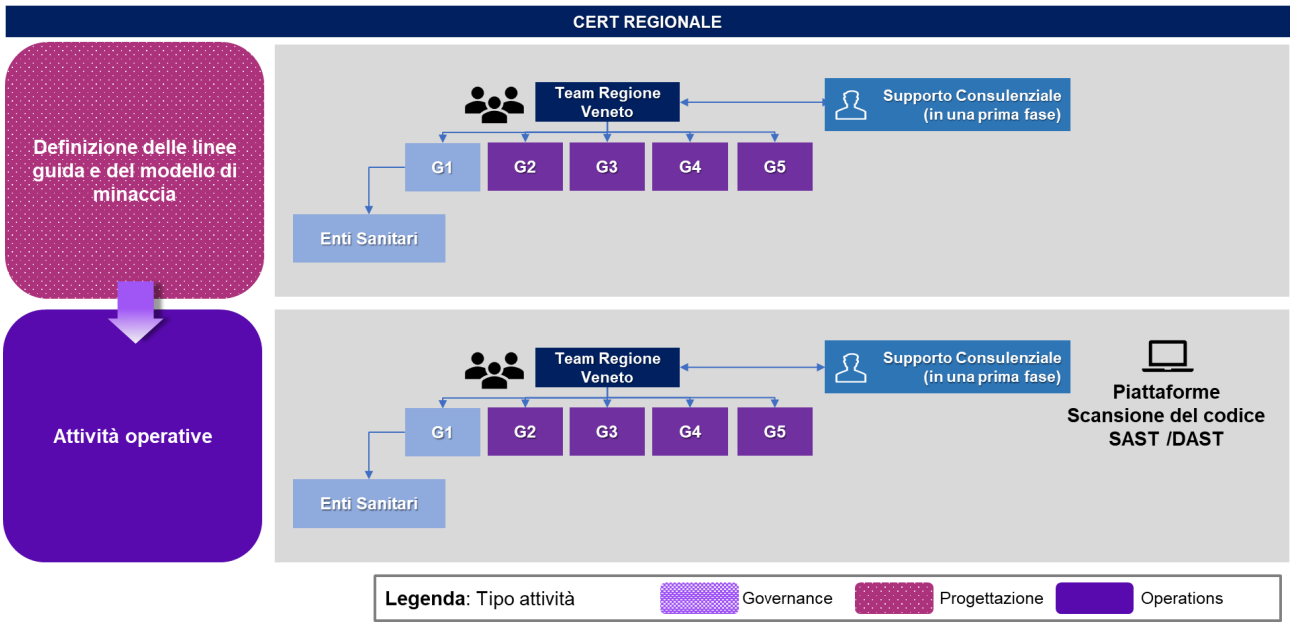


Figura 43 – Modello operativo Sviluppo Sicuro

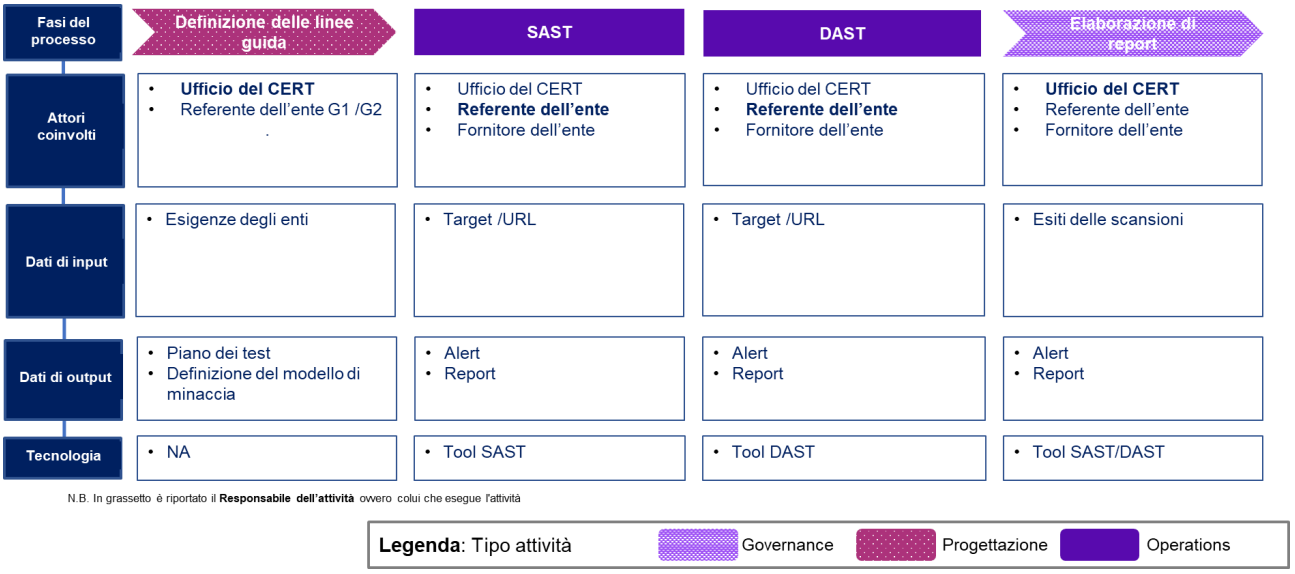


Figura 44 - Caratterizzazione del Modello Operativo

9 Modalità di adesione e partecipazione

Tramite la Deliberazione della Giunta Regionale n. 1174 / DGR del 27/09/2022 è stato approvato il progetto del CERT (Computer Emergency Response Team) Regionale ed è stato dato il mandato della sua esecuzione alla **Direzione ICT e Agenda Digitale Regione del Veneto.**

il CERT Regionale opererà i servizi di sicurezza sopradescritti (o parte di questi) 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 perimetro considerato nel presente progetto esecutivo potrà essere riadattato con l'introduzione di nuovi enti o gruppi.

L'adesione e partecipazione da parte degli enti/organizzazioni al CERT di Regione del Veneto sarà declinata tramite la firma di una convenzione ad hoc, attraverso cui gli enti aderenti:

- Si impegneranno a rispettare i requisiti definiti nel Paragrafo *Requisiti di Adesione*, sulla base della suddivisione in gruppi descritta nel capitolo *Analisi preliminare e relativi risultati.*
- Potranno scegliere i servizi da implementare, 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.

Ogni ente, secondo quanto definito dal comitato strategico, parteciperà alla spesa del CERT in funzione del gruppo di appartenenza, nonché dei relativi servizi abilitati. La gestione delle convenzioni sarà a cura del CERT di Regione del Veneto.

10 Tempistiche di attuazione

Le tempistiche di attuazione dei servizi del CERT di Regione del Veneto sono definite dal comitato strategico del CERT e sono dipendenti dal modello di partecipazione degli enti/organizzazioni (tempistiche di emanazione della legge per la costituzione del CERT) nonché dal modello di finanziamento dello stesso. Si riporta di seguito una proposta di pianificazione per la costituzione del CERT nonché di ogni ambito di intervento del CERT, definita tenendo in considerazione, come da modello operativo una fase di attivazione, di configurazione e di erogazione dei servizi.

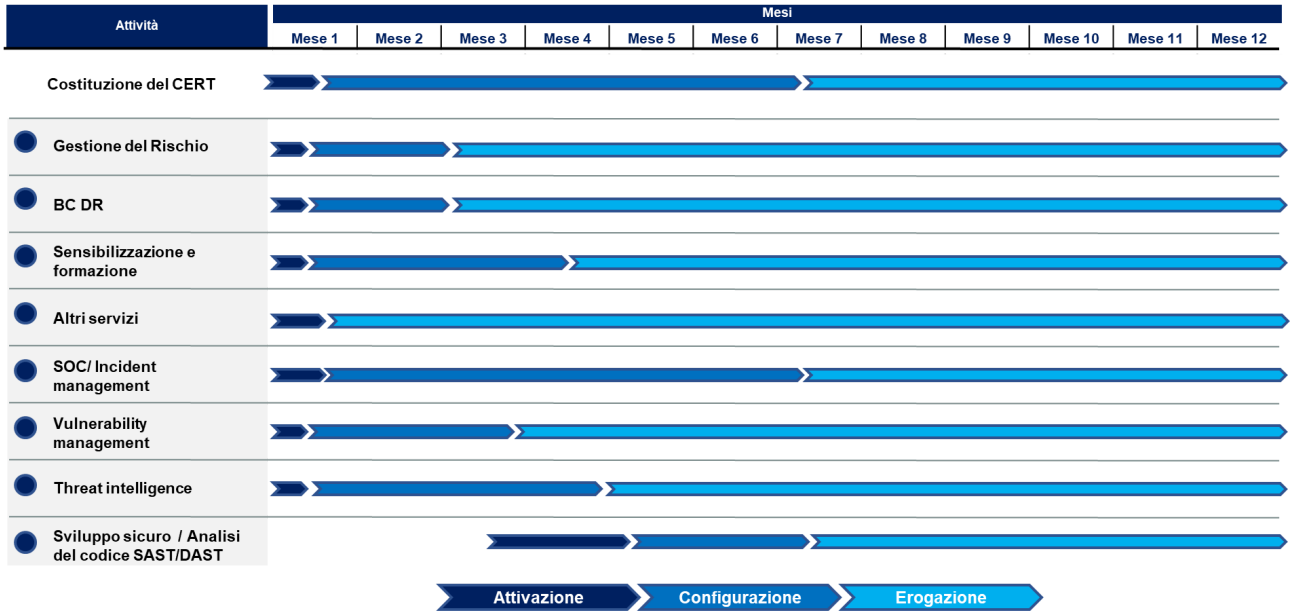


Figura 45 – Tempistiche di attuazione del CERT

11 Costi di gestione

Di seguito si riporta il prospetto economico per l'implementazione del CERT di Regione del Veneto, dettagliato per singolo Gruppo, con lo spaccato complessivo tra l'Area Sanità Sociale e

la Direzione ICT e Agenda Digitale. Il dimensionamento economico del CERT è stato effettuato tenendo in considerazione le metriche raccolte durante l'attività di analisi.

Ambiti di Intervento	Breve descrizione	Metrica	Quantità Anno 1	Stime Totali 1 Anno	Costo G1 + Enti Sanitari	Costo Direzione ICT e Agenda Digitale	Quantità Anni Successivi	Stime Totali Anni Successivi	Costo G1 + Enti Sanitari Anni Successivi	Costo Direzione ICT e Agenda Digitale Anni Successivi
Gestione del Rischio	Linee Guida + Assessment + Report	gg/team	1900	475.000 €	340.000 €	135.000 €	1480	370.000 €	265.000 €	105.000 €
BC/DR	Linea Guida + Predisposizione Template + Assessment + Report	gg/team	1900	475.000 €	340.000 €	135.000 €	1480	370.000 €	265.000 €	105.000 €
Sensibilizzazione e formazione	Piattaforma + (Custom x G1)	utenti	70000	1.300.000 €	962.000 €	338.000 €	70000	1.300.000 €	962.000 €	338.000 €
Altri servizi	Vari	gg/team	1200	300.000 €	150.000 €	150.000 €	1200	300.000 €	150.000 €	150.000 €
SOC/ Incident management	HyperSOC per G1 e G2 - SOC G3,4,5	EPS	65800	1.894.950 €	1.200.000 €	694.950 €	65800	1.894.950 €	1.200.000 €	694.950 €
Vulnerability management	Gestione Continua delle Vulnerabilità	IP	10000	200.000 €	150.000 €	50.000 €	10000	200.000 €	150.000 €	50.000 €
	Penetration Testing	App	90	900.000 €	650.000 €	250.000 €	90	900.000 €	650.000 €	250.000 €
Threat intelligence	Piattaforma	Data feed / moduli	71 / 9	425.000 €	289.000 €	136.000 €	71 / 9	425.000 €	289.000 €	136.000 €
Sviluppo sicuro / Analisi del codice	Linea Guida + SAST DAST	App	50 SAST / 50 DAST	695.000 €	390.000 €	305.000 €	50 SAST / 50 DAST	695.000 €	390.000 €	305.000 €
Governo dell'erogazione dei Servizi		gg/team	2.800 €	700.000 €	550.000 €	150.000 €	2.800 €	700.000 €	550.000 €	150.000 €
Totale IVA Esclusa				7.364.950 €	5.021.000 €	2.343.950 €		7.154.950 €	4.871.000 €	2.283.950 €
Totale IVA Inclusa				8.985.239 €	6.125.620 €	2.859.619 €		8.729.039 €	5.942.620 €	2.786.419 €

Figura 46 – Dimensionamento dei servizi – Costo Totale 1° anno e anni successivi

	G1	G2+G3+G4+G5+RdV	G2		G3		G4		G5		Regione Del Veneto
Ambiti di Intervento	Costo G1 + Enti sanitari	Costo Direzione ICT e Agenda Digitale	Costo G2	Costo Medio Singolo Ente G2	Costo G3	Costo Medio Singolo Ente G3	Costo Totale G4	Costo Medio Singolo Ente G4	Costo Totale G5	Costo Medio Singolo Ente G5	Costo Regione del Veneto
Gestione del Rischio	340.000 €	135.000 €	50.000 €	16.667 €	40.000 €	10.000 €	31.500 €	2.864 €	13.500 €	1.929 €	-
BC/DR	340.000 €	135.000 €	50.000 €	16.667 €	40.000 €	10.000 €	31.500 €	2.864 €	13.500 €	1.929 €	-
Sensibilizzazione e formazione	962.000 €	338.000 €	74.286 €	24.762 €	37.143 €	9.286 €	37.143 €	3.377 €	3.714 €	531 €	185.714 €
Altri servizi	150.000 €	150.000 €	23.000 €	7.667 €	20.500 €	5.125 €	39.500 €	3.591 €	17.000 €	2.429 €	50.000 €
SOC/ Incident management	1.200.000,00 €	694.950 €	150.000 €	50.000 €	76.500 €	19.125 €	78.000 €	7.091 €	7.500 €	1.071 €	382.950 €
Vulnerability management	150.000 €	50.000 €	11.000 €	3.667 €	5.500 €	1.375 €	6.000 €	545 €	1.500 €	214 €	26.000 €
	650.000 €	250.000 €	37.500 €	12.500 €	25.000 €	6.250 €	68.750 €	6.250 €	43.750 €	6.250 €	75.000 €
Threat intelligence	289.000 €	136.000 €	29.890 €	9.963 €	14.945 €	3.736 €	14.945 €	1.359 €	1.495 €	214 €	74.725 €
Sviluppo sicuro / Analisi del codice	390.000 €	305.000 €	43.571 €	14.524 €	58.095 €	14.524 €	79.881 €	7.262 €	50.833 €	7.262 €	72.619 €
Governo dell'erogazione dei Servizi	550.000 €	150.000 €	33.000 €	11.000 €	16.000 €	4.000 €	16.000 €	1.455 €	3.000 €	429 €	82.000 €
Totale IVA Esclusa	5.021.000 €	2.343.950 €	502.247 €	167.416 €	333.683 €	83.421 €	403.219 €	36.656 €	155.793 €	22.256 €	949.009 €
Totale IVA Inclusa	6.125.620 €	2.859.619 €	612.742 €	204.247 €	407.093 €	101.773 €	491.927 €	44.721 €	190.067 €	27.152 €	1.157.791 €

Figura 47 – Dimensionamento dei servizi 1° anno – Suddivisione per Gruppi

	G1	G2+G3+G4+G5+RdV	G2		G3		G4		G5		Regione del Veneto
Ambiti di intervento	Costo G1 + Enti Sanitari	Costo Direzione ICT e Agenda Digitale	Costo G2	Costo Medio Singolo Ente G2	Costo G3	Costo Medio Singolo Ente G3	Costo Totale G4	Costo Medio Singolo Ente G4	Costo Totale G5	Costo Medio Singolo Ente G5	Costo Regione del Veneto
Gestione del rischio	265.000 €	105.000 €	38.889 €	12.963 €	31.111 €	7.778 €	24.500 €	2.227 €	10.500 €	1.500 €	-
BC/DR	265.000 €	105.000 €	38.889 €	12.963 €	31.111 €	7.778 €	24.500 €	2.227 €	10.500 €	1.500 €	-
Sensibilizzazione e formazione	962.000 €	338.000 €	74.286 €	24.762 €	37.143 €	9.286 €	37.143 €	3.377 €	3.714 €	531 €	185.714 €
Altri servizi	150.000 €	150.000 €	23.000 €	7.667 €	20.500 €	5.125 €	39.500 €	3.591 €	17.000 €	2.429 €	50.000 €
SOC/Incident management	1.200.000 €	694.950 €	150.000 €	50.000 €	76.500 €	19.125 €	78.000 €	7.091 €	7.500 €	1.071 €	382.950 €
Vulnerability mgmnt	150.000 €	50.000 €	11.000 €	3.667 €	5.500 €	1.375 €	6.000 €	545 €	1.500 €	214 €	26.000 €
	650.000 €	250.000 €	37.500 €	12.500 €	25.000 €	6.250 €	68.750 €	6.250 €	43.750 €	6.250 €	75.000 €
Threat intelligence	289.000 €	136.000 €	29.890 €	9.963 €	14.945 €	3.736 €	14.945 €	1.359 €	1.495 €	214 €	74.725 €
Sviluppo sicuro / Analisi del codice	390.000 €	305.000 €	43.571 €	14.524 €	58.095 €	14.524 €	79.881 €	7.262 €	50.833 €	7.262 €	72.620 €
Governo dell'erogazione dei servizi	550.000 €	150.000 €	33.000 €	11.000 €	16.000 €	4.000 €	16.000 €	1.455 €	3.000 €	429 €	82.000 €
Totale IVA Esclusa	4.871.000 €	2.283.950 €	480.025 €	160.008 €	315.905 €	78.976 €	389.219 €	35.384 €	149.792 €	21.399 €	949.009 €
Totale IVA Inclusa	5.942.620 €	2.786.419 €	585.630 €	195.210 €	385.404 €	96.351 €	474.847 €	43.168 €	182.746 €	26.107 €	1.157.791 €

Figura 48 – Dimensionamento dei servizi anni successivi – Suddivisione per Gruppi

Si specifica inoltre che gli Enti sanitari (G1 e le AULSS) non sono stati oggetto diretto della fase iniziale di assessment ma i dati alla base delle valutazioni economiche sono la risultanza di un'analisi condotta in precedenza e fornitaci da Azienda Zero (G1).

12 Trattamento dei dati personali da parte del CERT-Direzione ICT e Agenda Digitale

Con l'obiettivo di definire i ruoli per il trattamento dei dati personali nel contesto del CERT di Regione del Veneto, si riporta quanto segue:

La Direzione ICT e Agenda Digitale nell'ambito dell'esecuzione delle attività inerenti il CERT regionale, si qualifica **Responsabile del Trattament**o, 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 che il Fornitore deve presentare a garanzia delle attività di trattamento specifiche del medesimo.
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. Predispone 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.

Allegato Tecnico 2

ENTE: AZIENDA ULSS 7 PEDEMONTANA

GRUPPO ENTE: ☒ G1 ☐ G2 ☐ G3 ☐ G4 ☐ G5

SERVIZI RICHIESTI:

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

Data _____

Azienda ULSS 7 Pedemontana
Il Direttore Generale
Dott. Carlo Bramezza

_____

Allegato 3

Atto di nomina del Responsabile del trattamento dei dati personali e istruzioni ai sensi e per gli effetti dell'art. 28 del Regolamento (UE) 2016/6792016/679.

Azienda ULSS 7 Pedemontana, con sede in Bassano del Grappa (VI), Via dei Lotti, 40, C.F. 00913430245 (di seguito Titolare del Trattamento), rappresentata dal Direttore Generale Dott. Carlo Bramezza, in qualità di Legale Rappresentante, d'ora in poi "Ente" o "Titolare del trattamento", preso atto che la seguente Convenzione comporta - per le finalità perseguite con i servizi dalla medesima previste e più sotto esplicitati - anche il trattamento di dati personali soggiacendo quindi alla normativa in materia di protezione dei dati personali ex Regolamento 2016/676/UE, *General Data Protection Regulation*, di seguito *"GDPR":*

- **Convenzione per l'adesione dei vari Enti regionali veneti al CERT (Computer Emergency Response Team) di Regione del Veneto - D.G.R. n. 1024 del 22/08/2023**.

Ricordato che, ai sensi dell'articolo 28 del predetto GDPR, il Responsabile del Trattamento è il soggetto <<*che tratta dati personali per conto del Titolare del trattamento*>>, operando in posizione subordinata e mettendo in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'Interessato (colui al quale i dati personali si riferiscono);

Tenendo conto dei compiti e responsabilità specifici del Responsabile del Trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'Interessato;

NOMINA

Regione del Veneto (di seguito denominata *"Regione"*), con sede legale in Venezia, Palazzo Balbi – Dorsoduro 3901, codice fiscale 02392630279, rappresentata dal Direttore pro tempore della Direzione ICT e Agenda Digitale, domiciliato per la sua carica presso la sede dell'Ente, il quale viene indicato altresì quale Delegato al trattamento ai sensi della Deliberazione della Giunta Regionale n. 596 dell'8 maggio 2018, quale Responsabile del Trattamento (di seguito denominato "Responsabile del trattamento") dei dati personali necessari per lo svolgimento del servizio affidato alla stessa dall'Ente in virtù della Convenzione sopra riportata.

1. Materia disciplinata

La nomina riguarda il trattamento di dati effettuato sia su supporto cartaceo sia con strumenti elettronici per dare esecuzione alla Convenzione in essere tra le parti, Ente e Regione e per adempiere agli obblighi derivanti dalla stessa. I dati non potranno essere trattati per finalità diverse o ulteriori.

2. Natura e finalità del trattamento

Il trattamento ha la natura e le finalità proprie della Convenzione, in relazione alla istituzione di un CERT regionale ed all'attuazione delle correlate misure di prevenzione ed azione.

3. Tipo di dati personali

I tipi di dati che il Responsabile del trattamento può trattare per conto dell'Ente, sono quelli di cui alle Checklist inviate all'Ente e processate nell'ambito delle operazioni di analisi dei rischi ed ogni altra attività successiva o correlata di cui alla Convenzione, che si intendono parte integrante del presente Atto.

4. Categorie di interessati

Le categorie di interessati dei cui dati personali sarà svolto trattamento dal Responsabile per conto del Titolare sono:

- personale aziendale, nei limiti di quanto strettamente necessario e pertinente;
- assistiti ed ogni altro paziente e/o utente dell'Ente, nei limiti di quanto strettamente necessario e pertinente;
- ogni altra persona fisica coinvolta dalle operazioni di analisi si cui alla Convenzione.

5. Obblighi e diritti

Con la sottoscrizione del presente Atto di nomina il Responsabile del Trattamento si impegna a garantire la correttezza del trattamento e adeguate misure di sicurezza a protezione dei dati trattati.

Il Responsabile del Trattamento si impegna in particolare a:

a) trattare i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adottare tutte le misure richieste ai sensi dell'articolo 32 GDPR;
d) rispettare le condizioni di cui ai paragrafi 2 e 4 dell'art. 28 GDPR per ricorrere a un altro responsabile del trattamento, per cui si rinvia a successivo paragrafo del presente Atto;
e) tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del GDPR;
f) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento: l'assistenza riguarderà pertanto l'adozione delle misure di sicurezza (art. 32 GDPR), la gestione delle eventuali violazioni di dati personali ("data breach") ai sensi degli artt. 33 e 34 GDPR, la valutazione di impatto nei casi richiesti dall'art. 35 GDPR ivi compresa l'eventuale consultazione preventiva del Garante nei casi di cui all'art. 36 GDPR;
g) su scelta del titolare del trattamento, cancellare o restituirgli tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
h) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente Atto e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo a tale lettera h) il Responsabile del trattamento si impegna ad informare immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Il Titolare avrà il diritto di accedere alle informazioni trattate dal Responsabile e dai propri Sub-Responsabili nell'ambito delle operazioni di trattamento, avvisando dell'intenzione di accedere con congruo preavviso.

6. Durata del trattamento

Il trattamento avrà durata pari alla durata della Convenzione tra le Parti, Ente e Regione. All'esaurirsi dello stesso il Responsabile del trattamento non sarà più autorizzato ad eseguire i trattamenti di dati e il presente Atto di nomina si considererà revocato a completamento dell'incarico.

7. Sub-Responsabili

Il Responsabile del trattamento può ricorrere ad un altro Responsabile del Trattamento ("sub-Responsabile del trattamento") per gestire attività di trattamento specifiche, informando il Titolare del trattamento di ogni nomina e/o sostituzione dei sub-responsabili.

Si riporta l'elenco dei sub-responsabili comunicati al Titolare del trattamento, che si intendono autorizzati anche a titolo di ratifica, a condizioni analoghe a quelle previste dal presente Atto, con gli stessi obblighi in materia di protezione dei dati e con la previsione in particolare di garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR, per cui gli stessi sono soggetti ad analogo Atto di nomina da parte della Regione. Qualora uno o più di tali Sub-Responsabili omettano di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserverà nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi di tali Sub-Responsabili:

Sub-responsabili	Sede legale
RTI composta da Deloitte Risk Advisory S.r.l. (mandataria), EY Advisory S.p.A. (mandante), Teleco S.r.l. (mandante).	Milano, Via Tortona 25 (mandataria)
RTI composta da Kyndryl Italia S.p.A. (mandataria) Accenture S.p.A, (mandante), Accenture Technology Solutions S.r.l., (mandante), Insirio S.p.A, (mandante), Expleo Italia S.p.A. (mandante)	Segrate (MI), Circonvallazione Idroscalo snc
Accenture S.p.A.	Milano, via Privata Nino Bonnet, 10

8. Varie

Per quanto non espressamente previsto nel presente atto di nomina, si fa rinvio alle norme del GDPR, al Codice Civile ed alle disposizioni legislative e regolamentari, nazionali e comunitarie vigenti in materia.

Si precisa che il presente Atto di nomina potrà essere integrato da successive disposizioni normative intervenute o da disposizioni ulteriori dell'Amministrazione regionale.

9. Responsabili della Protezione dei Dati (RPD) / Data Protection Officer (DPO)

L'Ente/Titolare del trattamento ha designato un proprio Responsabile della Protezione dei Dati ("RPD") / "Data Protection Officer" ("DPO"), come tale la Società tra Avvocati Cervato Law & Business s.r.l., con sede a Padova, Galleria Europa 3, C.F./P.IVA 05352130289, PEC cervato.sta@pec.it, dato di contatto rpd@aulss7.veneto.it, con indicazione dell'Avv. Piergiovanni Cervato quale persona fisica designata all'incarico ai sensi delle Linee Guida del Garante e dell'ANAC.

Parimenti, il responsabile del trattam,ento ha designato un proprio RPD/DPO, i cui dati di contatto sono:

Palazzo Sceriman
Cannaregio 168
30121 Venezia

Tel. 041.279.2498 / 2044 / 2593
Mail: dpo@regione.veneto.it
PEC: dpo@pec.regione.veneto.it

I RPD/DPO dei Sub-Responsabili sono indicati separatamente da tali soggetti.

Venezia / Bassano del Grappa _____

Il Direttore Generale/Legale Rappresentante
Azienda ULSS 7 Pedemontana
Dott Carlo Bramezza

_____

Per accettazione

Il Direttore della Direzione ICT e Agenda Digitale
Regione del Veneto
Dott. Idelfo Borgo

_____