RegioneLombardia

LA GIUNTA

DELIBERAZIONE N° XII / 1224 Seduta del 30/10/2023

Presidente **ATTILIO FONTANA**

Assessori regionali

MARCO ALPARONE *Vicepresidente*	ROMANO MARIA LA RUSSA
ALESSANDRO BEDUSCHI	ELENA LUCCHINI
GUIDO BERTOLASO	FRANCO LUCENTE
FRANCESCA CARUSO	GIORGIO MAIONE
GIANLUCA COMAZZI	BARBARA MAZZALI
ALESSANDRO FERMI	MASSIMO SERTORI
PAOLO FRANCO	CLAUDIA MARIA TERZI
GUIDO GUIDESI	SIMONA TIRONI

Con l'assistenza del Segretario Riccardo Perini

Su proposta dell'Assessore Guido Bertolaso

Oggetto

APPROVAZIONE PIANO DI CYBER SECURITY PER GLI ENTI SANITARI 2023-2025 E AGGIORNAMENTO PIANO TRIENNALE DG WELFARE 2023-2025 GDR XII/842 DEL 08/08/2023

Si esprime parere di regolarità amministrativa ai sensi dell'art.4, comma 1, l.r. n.17/2014:

Il Direttore Generale Giovanni Pavesi

Il Dirigenti Giovanni Delgrossi

L'atto si compone di 27 pagine

di cui 18 pagine di allegati

parte integrante

RICHIAMATE la Legge Regionale n.12 del 10/08/2018, la Legge Regionale n. 6 del 03/04/2019 "Disposizioni in merito alla fusione delle società partecipate in modo totalitario Azienda regionale centrale acquisti S.p.A. (Arca S.p.A.), Lombardia informatica S.p.A. (Lispa) e Infrastrutture Lombarde S.p.A. (Ilspa) – Nuova determinazione della società incorporante: Azienda regionale per l'innovazione e gli acquisti S.p.A. (Aria Spa)";

RICHIAMATA la Convenzione Quadro tra la Giunta Regionale della Lombardia e l'Azienda regionale per l'innovazione e gli acquisti S.p.A. (Aria Spa) sottoscritta sulla base della Delibera di Giunta Regionale n. XI/7409 del 30/11/2022 ed inserita nella raccolta di Regione Lombardia "Convenzioni e Contratti" RCC n. 13200 del 13/12/2022;

VISTI:

- il Regolamento UE 2016/679 "GDPR" che introduce un nuovo quadro giuridico per la protezione dei dati personali nell'Unione Europea focalizzato sulla tutela dei dati dell'interessato;
- il Decreto Legislativo 10 agosto 2018, n. 101 riportante le disposizioni per l'adeguamento della normativa nazionale alle prescrizioni del GDPR;
- la Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

CONSIDERATO che:

- in un mondo sempre più digitalizzato e connesso l'attuazione di una adeguata politica di cybersicurezza è diventata di fondamentale importanza per la tutela degli interessi regionali e nazionali nel campo della sicurezza informatica, della protezione dei dati e della resilienza cibernetica;
- il decreto-legge n. 82 del 14 giugno 2021 ha istituito l'Agenzia per la Cybersicurezza Nazionale (ACN) con l'obiettivo di predisporre la strategia nazionale di cybersicurezza, di rappresentare un punto di riferimento centrale di sinergia e coordinamento, di razionalizzare e semplificare il frammentato sistema di competenze nazionali ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

RICHIAMATO il PRSS (Programma Regionale di Sviluppo Sostenibile) della XII

legislatura che ha come obiettivo strategico il rafforzamento della digitalizzazione della pubblica amministrazione e la garanzia della sicurezza dei dati e dei servizi attraverso il potenziamento della resilienza dei sistemi regionali per la prevenzione degli incidenti, la protezione degli asset aziendali e la tutela della sicurezza dei dati e delle operazioni.

CONSIDERATO che:

- da molti anni Regione Lombardia, con il supporto dell'Azienda Regionale per l'Innovazione e gli Acquisti (ARIA Spa), ha investito nell'ambito della sicurezza informatica raggiungendo un consistente livello di maturità a livello organizzativo, procedurale e tecnologico soprattutto nell'ambito della gestione ed erogazione di servizi digitali di livello regionale;
- la sempre più diffusa e capillare informatizzazione dei servizi e la sempre maggiore integrazione e interdipendenza dei sistemi in uso presso il livello centrale regionale e il livello locale degli Enti Sanitari pubblici e privati richiede di adottare misure di sicurezza tecnologiche ed organizzative sempre più sofisticate che consentano di prevenire attacchi informatici, preservare l'integrità dei dati e delle informazioni gestite nell'ambito dell'intero sistema sociosanitario regionale e assicurare la continuità dei servizi per i cittadini;

CONSIDERATO che la sicurezza delle informazioni e la protezione dei dati, in particolare riferiti all'ambito dei servizi sociosanitari, rappresentano elementi fondamentali e abilitanti per innovare i servizi ed incrementare la produttività del Sistema Regionale nonché per migliorare la qualità della vita dei cittadini e la competitività delle imprese lombarde;

CONSIDERATO che Regione Lombardia, le Aziende Sanitarie pubbliche (ASST, ATS, IRCCS), gli Enti Erogatori Privati Accreditati (EEPA) e l'Azienza Regionale per l'Innovazione e gli Acquisti (ARIA Spa) costituiscono un unico sistema federato nella gestione dei dati sociosanitari;

VERIFICATO che la U.O. Sistemi Informativi e Sanità Digitale della Direzione Generale Welfare, al fine di rafforzare il livello di sicurezza informatica delle infrastrutture tecnologiche di tutti gli Enti Sanitari pubblici e di avviare un percorso tecnico e organizzativo condiviso e coordinato centralmente che porti ad un graduale e costante miglioramento del livello di sicurezza informatica dell'intero sistema sociosanitario regionale, nel 2022 ha affidato ad ARIA Spa l'incarico per il coordinamento e la conduzione delle seguenti attività:

- svolgimento di attività di assessment generale per verificare il livello di maturità di cybersicurezza di tutti gli Enti Sanitari pubblici;
- attivazione di una Task Force straordinaria per il coordinamento centrale e il supporto specialistico agli Enti Sanitari pubblici nella identificazione, programmazione e attuazione degli interventi tecnici e organizzativi considerati prioritari per il miglioramento e il rafforzamento della sicurezza informatica a livello centrale e locale;
- attuazione delle prime azioni e interventi per migliorare il livello di sicurezza informatica degli Enti Sanitari pubblici e dell'intero sistema sociosanitario regionale.

VISTA la nota "*Richiesta di predisposizione della relazione sullo stato di avanzamento degli interventi e del piano di miglioramento del livello di sicurezza informatica degli Enti Sanitari*" Prot. G1.2023.0025578 del 07/07/2023 con cui la Direzione Generale Welfare ha chiesto ad Aria Spa di predisporre una relazione che descriva lo stato di avanzamento degli interventi centrali e locali previsti per l'anno 2022, gli eventuali benefici e miglioramenti introdotti dall'attuazione di tali interventi e il piano di continuo miglioramento del livello di sicurezza informatica degli Enti Sanitari pubblici e dell'intero sistema sociosanitario regionale, con particolare riferimento ai seguenti aspetti principali:

- metodologia adottata e condivisa a livello regionale per misurare il livello di maturità dell'infrastruttura tecnologica degli Enti Sanitari pubblici e per pianificare gli interventi di continuo miglioramento nell'ambito della cybersicurezza;
- stato di avanzamento degli interventi effettuati dagli Enti Sanitari pubblici con il supporto specialistico della Task Force regionale ed eventuali evidenze del miglioramento riscontrato a livello locale e centrale;
- elenco e tipologia di interventi proposti e programmati per i prossimi 12 mesi da parte degli Enti Sanitari pubblici con previsione del miglioramento del livello di sicurezza informatica atteso a livello locale e centrale;
- stima dei costi previsti per il prossimo triennio per il mantenimento dell'attuale livello di servizio e per l'implementazione e la diffusione degli interventi di miglioramento programmati.

VISTA la nota "*Invio seconda versione della Relazione sullo stato di avanzamento degli interventi e del piano di miglioramento del livello di sicurezza informatica degli Enti Sanitari e relativo allegato*" (Prot. G1.2023. 0037249 del 22/09/2023) inviata da Aria Spa per relazionare sullo stato di avanzamento degli interventi per la sicurezza informatica e contenente:

- "Relazione sulle attività svolte nel 2022 e programmazione degli interventi per il triennio 2023-2025", parte integrante e sostanziale del presente atto, in cui viene descritto a) il cronoprogramma delle attività svolte dal 2022 a partire dall'assessment tecnologico degli Enti Sanitari e dall'attivazione della Task Force Regionale di Cybersecurity, b) il modello adottato per valutare il grado di adeguatezza dei sistemi informativi degli Enti Sanitari per far fronte alle minacce informatiche, modello che in una scala di 1 a 5 considera come primari i sei ambiti di intervento relativi a Identify, Protect, Detect, Recover e Cloud e c) il piano di miglioramento del livello di sicurezza informatica degli Enti Sanitari;
- "*Allegato alla Relazione sulle attività svolte nel 2022 e programmazione degli interventi per il triennio 2023-2025 - Risultati raggiunti*" contente la Valutazione preliminare della maturità degli Enti sanitari pubblici ed il livello di maturità stimato a fronte delle azioni pianificate;

CONSIDERATO che dalla relazione presentata da Aria Spa risulta, tra l'altro, che:

- in base alla valutazione congiunta da parte di Aria Spa e dei tecnici degli Enti Sanitari, si sono avviate azioni che hanno permesso di migliorare il grado di sicurezza complessiva dei sistemi;
- il miglioramento raggiunto, seppure non ancora pienamente sufficiente a raggiungere gli obiettivi minimali definiti, conferma che la metodologia adottata per la misurazione del livello di maturità degli Enti Sanitari e per la programmazione degli interventi di miglioramento prioritari è risultata efficace e può essere, pertanto, ulteriormente utilizzata per perseguire una politica di continuo miglioramento del livello di cybersicurezza dell'intero sistema sociosanitario regionale;
- al fine di raggiungere un livello di sicurezza informatica considerato adeguato è necessario proseguire anche nel prossimo triennio con le attività di programmazione e attuazione di nuovi interventi da parte degli Enti sanitari Pubblici, perseguendo la metodologia già adottata con successo nel corso del 2022.

CONSIDERATO che anche gli Enti Erogatori Privati Accreditati gestiscono e producono dati sanitari e svolgono un ruolo rilevante nel sistema federato regionale partecipando attivamente all'alimentazione del Fascicolo Sanitario Elettronico, si ritiene opportuno valutare il loro coinvolgimento anche nelle attività di miglioramento del livello di cybersicurezza e, in particolare, nell'adozione del modello di maturità già adottato dagli Enti Sanitari Pubblici.

VISTA la DGR n. XII/842 del 08/08/2023 "*INTEGRAZIONE AL DOCUMENTO TECNICO DI ACCOMPAGNAMENTO AL BILANCIO DI PREVISIONE 2023-2025 E AGGIORNAMENTO DEI PROSPETTI PER IL CONSOLIDAMENTO DEI CONTI DEL BILANCIO REGIONALE E DEGLI ENTI DIPENDENTI, DEI PROGRAMMI PLURIENNALI DELLE ATTIVITÀ DEGLI ENTI E DELLE SOCIETÀ IN HOUSE, DEL PIANO DI STUDI E RICERCA, DELL'ELENCO RIPORTANTE GLI APPALTI AFFIDATI AD ARIA SPA E DEI PROSPETTI DELLA PROGRAMMAZIONE GARE PER L'ACQUISIZIONE DI BENI E SERVIZI PER L'ANNO 2023 IN RACCORDO CON LE DISPONIBILITÀ DI BILANCIO DI CUI ALLA DGR XII/248/2023, A SEGUITO DELLA L.C.R N. 2 DEL 27/07/2023 "ASSESTAMENTO AL BILANCIO DI PREVISIONE 2023-2025 CON MODIFICHE DI LEGGI REGIONALI*" con cui sono stati approvati il Piano Pluriennale delle attività di ARIA Spa 2023-2025 e il prospetto di raccordo che individua i finanziamenti autorizzati a carico del bilancio regionale;

DATO ATTO che la sopracitata DGR XII/842 del 08/08/2023 all'allegato A approva, tra gli altri, il prospetto di raccordo di Aria Spa, tra cui l'Attività 168 "Sicurezza informatica per gli Enti sociosanitari" per euro 8.573.000,00 per l'anno 2023 e per euro 6.573.000,00 sulle annualità 2024 e 2025.

RITENUTO, pertanto, di:

- di approvare l'Allegato 1, parte integrante e sostanziale del presente atto, "Relazione sulle attività svolte nel 2022 e programmazione degli interventi per il triennio 2023-2025" ed in particolare il "Modello di Sicurezza Informatica degli Enti Sanitari basato sugli ambiti di intervento relativi a Identify, Protect, Detect, Recover e Cloud", ivi contenuto;
- modificare e integrare di conseguenza l'incarico 168 "Sicurezza informatica per gli Enti sociosanitari", il cui valore aggiornato risulta pari a complessivi euro 31.531.560,00, indicato nella Relazione di cui al prot. 29318 del 25/07/2023, come di seguito dettagliato:
  - euro 7.775.080,00 per l'anno 2023
  - euro 11.878.240,00 per l'anno 2024
  - euro 11.878.240,00 per l'anno 2025

DATO ATTO che che la spesa sopraindicata trova copertura a valere del capitolo 13.01.103.8380 per gli esercizi interessati, precisando che le risorse per le attività ivi descritte relative alle annualità 2024 e 2025 trovano copertura per euro

13.146.000,00 sul Piano Attività 168 del Prospetto di Raccordo approvato con DGR 842 del 08/08/2023 e per la rimanente parte, pari ad euro 10.610.480,00, tramite economie su attività finanziate sul capitolo 13.01.103.8380.

CONSIDERATO che si rende necessario modificare il "Prospetto di raccordo delle attività di ARIA Spa per gli anni 2023-2025" approvato con la DGR XII/842 del 08/08/2023, al fine di poter ulteriormente finanziare l'Attività 168 "Sicurezza informatica per gli Enti sociosanitari" per euro 5.305.240,00 sulle annualità 2024 e 2025 e allo stesso tempo ridurre le seguenti PPA di un uguale importo complessivo come riportato nell'Allegato 2, parte integrante e sostanziale del presente atto:

- PPA2023_129 Evoluzione del Sistema Informativo Regionale per il Welfare
- PPA2023_133 Attività per la gestione e la manutenzione del Sistema Informativo Regionale per il Welfare
- PPA2023_138 Network Provider e Service Provider
- PPA2023_141 Piattaforma Regionale di Integrazione
- PPA2023_144 Rete Regionale di Prenotazione
- PPA2023_154 Supporto alla campagna vaccinale
- PPA2023_177 Infrastruttura Tecnologica Facility Welfare

VERIFICATO che:

- l'Ufficio Gestione Finanziaria ha preso atto che le modifiche apportate non incrementano le risorse a suo tempo assegnate, ma le distribuiscono diversamente all'interno delle varie commesse a valere sempre sullo stesso capitolo di spesa (13.01.103.8380) e non ha nulla da segnalare;
- l'Ufficio Presidio e coordinamento delle funzioni inerenti il Sireg non ha sollevato osservazioni in quanto le attività sono coerenti con la mission della società e con gli indirizzi regionali ad essa rivolti;

ALL'UNANIMITA' dei voti, espressi nelle forme di legge;

DELIBERA

Per tutto quanto in premessa:

1. di approvare l'Allegato 1, parte integrante e sostanziale del presente atto, "*Relazione sulle attività svolte nel 2022 e programmazione degli interventi per il triennio 2023-2025*" ricevuto con nota "*Invio seconda*

versione della Relazione sullo stato di avanzamento degli interventi e del piano di miglioramento del livello di sicurezza informatica degli Enti Sanitari e relativo allegato" Prot. G1.2023. 0037249 del 22/07/2023;

2. di approvare il "*Modello di Sicurezza Informatica degli Enti Sanitari basato sugli ambiti di intervento relativi a Identify, Protect, Detect, Recover e Cloud*" contenuto nel suddetto Allegato 1;

3. di dare mandato alla Direzione Generale Welfare di verificare la possibilità di estendere il Modello di Sicurezza Informatica di cui al punto precedente anche agli Enti Erogatori Privati Accreditati (EEPA);

4. di affidare ad ARIA Spa la realizzazione delle azioni contenute nel Programma degli interventi per il triennio 2023-2025, di cui al punto precedente, modificando la PPA 168 "Sicurezza informatica per gli Enti sociosanitari", e che trovano copertura sul capitolo 13.01.103.8380 per euro 31.531.560,00 sulle annualità 2023, 2024 e 2025 rispettivamente pari a:
   - euro 7.775.080,00 per l'anno 2023
   - euro 11.878.240,00 per l'anno 2024
   - euro 11.878.240,00 per l'anno 2025;

5. di approvare l'allegato 2 "Aggiornamento Prospetto di raccordo delle attività di ARIA Spa per gli anni 2023-2025", che costituisce parte integrante e sostanziale del presente atto e che modifica il Prospetto approvato nella DGR XII/842 del 08/08/2023 "INTEGRAZIONE AL DOCUMENTO TECNICO DI ACCOMPAGNAMENTO AL BILANCIO DI PREVISIONE 2023-2025 E AGGIORNAMENTO DEI PROSPETTI PER IL CONSOLIDAMENTO DEI CONTI DEL BILANCIO REGIONALE E DEGLI ENTI DIPENDENTI, DEI PROGRAMMI PLURIENNALI DELLE ATTIVITÀ DEGLI ENTI E DELLE SOCIETÀ IN HOUSE, DEL PIANO DI STUDI E RICERCA, DELL'ELENCO RIPORTANTE GLI APPALTI AFFIDATI AD ARIA SPA E DEI PROSPETTI DELLA PROGRAMMAZIONE GARE PER L'ACQUISIZIONE DI BENI E SERVIZI PER L'ANNO 2023 IN RACCORDO CON LE DISPONIBILITÀ DI BILANCIO DI CUI ALLA DGR XII/248/2023, A SEGUITO DELLA L.C.R N. 2 DEL 27/07/2023 "ASSESTAMENTO AL BILANCIO DI PREVISIONE 2023-2025 CON MODIFICHE DI

LEGGI REGIONALI" rimodulando le seguenti Attività sul capitolo 13.01.103.8380 sulle annualità 2024 e 2025 senza incremento della spesa:

- PPA2023_129 Evoluzione del Sistema Informativo Regionale per il Welfare
- PPA2023_133 Attività per la gestione e la manutenzione del Sistema Informativo Regionale per il Welfare
- PPA2023_138 Network Provider e Service Provider
- PPA2023_141 Piattaforma Regionale di Integrazione
- PPA2023_144 Rete Regionale di Prenotazione
- PPA2023_154 Supporto alla campagna vaccinale
- PPA2023_177 Infrastruttura Tecnologica Facility Welfare;

6. di procedere alla pubblicazione del presente atto nella Sezione "Amministrazione trasparente" del sito istituzionale di Regione Lombardia, ai sensi dell'art. 37, comma 1, lett. b) del D. Lgs. 33/2013 e degli artt. 29, comma 1 e 192 comma 3, del D. Lgs. 50/2016.

IL SEGRETARIO

RICCARDO PERINI

Atto firmato digitalmente ai sensi delle vigenti disposizioni di legge

Task Force Cybersecurity per gli Enti Sanitari

Relazione sulle attività svolte nel 2022 e programmazione degli interventi per il triennio 2023-2025

Indice

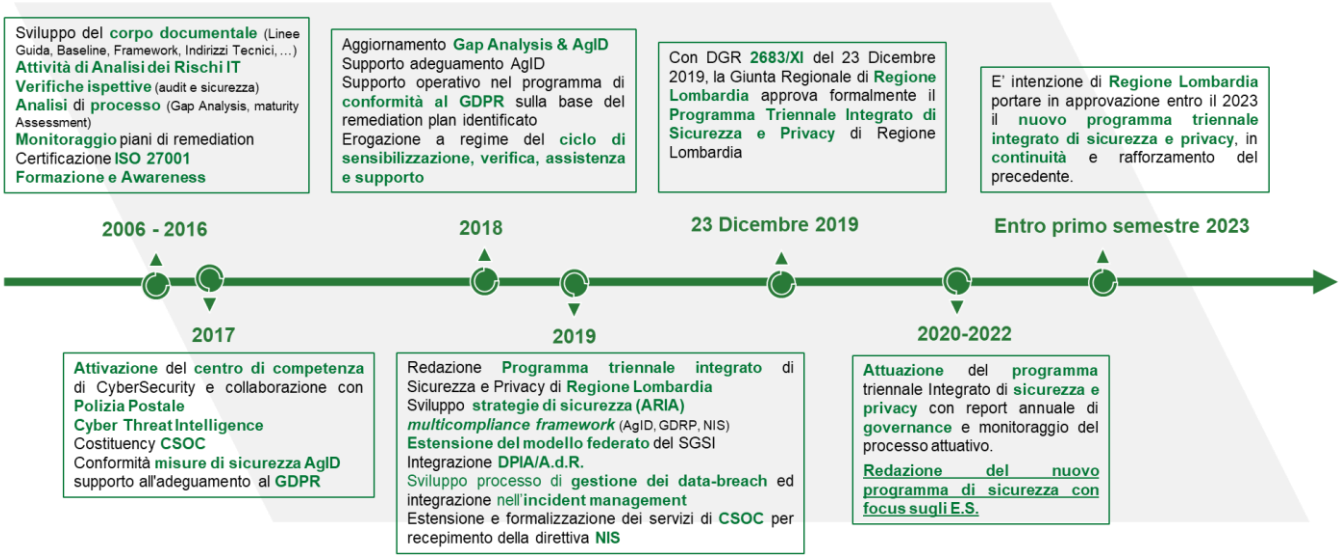
1. Introduzione e contesto

Questo documento ha lo scopo di illustrare le attività svolte da Regione Lombardia ed ARIA al fine di migliorare la postura di sicurezza degli Enti del Welfare Territoriale e permettere loro di raggiungere un livello di sicurezza omogeneo e adeguato.

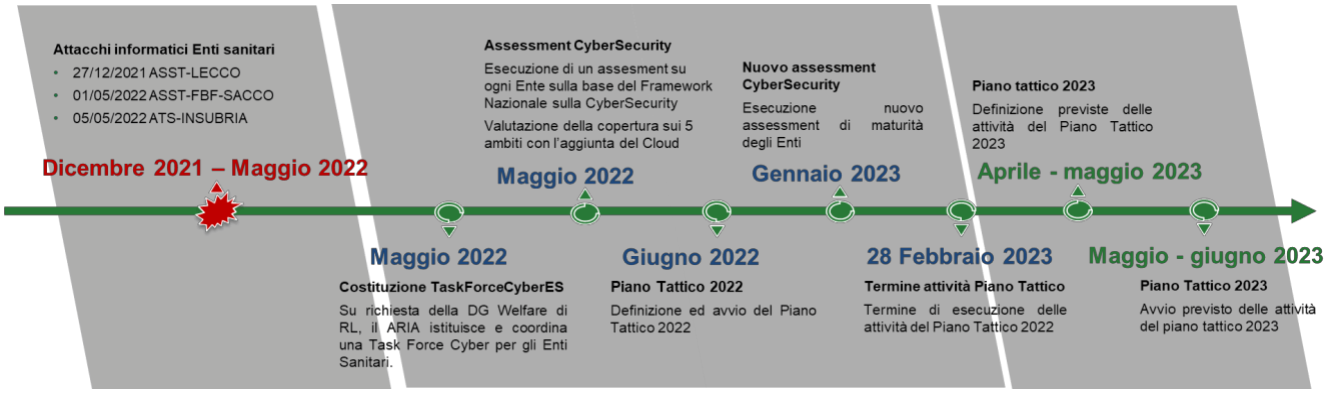
In particolare, si sofferma sulla descrizione delle attività svolte nel corso del 2022 e sulle attività programmate per il triennio 2023-2025.

Regione Lombardia ed ARIA, nell'ambito delle loro competenze, già da tempo affrontano i temi relativi alla cybersecurity e alla sicurezza, sia dal punto di vista strategico, sia dal punto di vista tattico.

La seguente immagine sintetizza la timeline della programmazione strategica degli ultimi anni.



Gli attacchi informatici verificatisi tra il dicembre 2021 e il maggio 2022 di cui sono state vittime alcuni Enti Sanitari della Regione Lombardia, hanno innescato una serie di successive contromisure tattiche necessarie a migliorare la postura di sicurezza degli Enti Sanitari, sintetizzate nella seguente timeline.



In seguito a tali attacchi è stato infatti necessario programmare, in modalità coordinata da ARIA e condivisa con tutti gli Enti, interventi per il progressivo e continuo innalzamento del livello di sicurezza informatica dell'intera architettura dei sistemi informativi regionali, in particolare:

- Attivazione della Task Force Regionale di Cybersecurity (di seguito Task Force) ed esecuzione di un assessment per la valutazione dello stato di protezione delle infrastrutture dei singoli Enti, oltre che la programmazione di interventi mirati;
- Attivazione di azioni verticali per ogni Ente previste dal piano tattico;

- Introduzione e attivazione presso tutti gli Enti di un servizio di Cyber Threat Intelligence;
- Attivazione del nuovo servizio regionale MDA per la gestione centralizzata dei “Security Incidents” rilevati dalle piattaforme EDR/XDR;
- Erogazione di attività formative su temi di cybersecurity rivolti al personale degli Enti.

La descrizione di questi interventi e di quelli previsti nel 2023 sono l’oggetto di questo documento, interventi che vengono descritti più in dettaglio nei seguenti paragrafi.

2. Modello per la valutazione della maturità degli Enti

La prima azione messa in campo dalla Task Force è stata la predisposizione di un framework per l'esecuzione di un security maturity assessment su 38 Enti del welfare territoriale (non è stato eseguito su ATS Insubria e ASST Fatebenefratelli/Sacco). Il framework è basato su una checklist di 236 punti suddivisa su diversi ambiti di indagine:

- Asset Management
- Sicurezza degli Endpoint
- Posta Elettronica
- Sicurezza Perimetrale
- Sicurezza della Rete
- Data Center
- Cloud Security
- Sicurezza dei sistemi
- Sicurezza dei database
- Sicurezza dei dati non strutturati
- Sicurezza applicativa
- Identità e gestione accessi
- Vulnerability Management
- Operation Technology Security
- Monitoraggio sicurezza
- Business Continuity e Disaster Recovery
- Sicurezza fisica
- Incident Management
- Active Directory
- Cybersecurity awareness

Le risposte ai punti della checklist sono state raccolte nel mese di maggio 2022 attraverso interviste on-site ai Referenti IT degli Enti e a verifiche congiunte sulla situazione del livello di sicurezza informatica presso ciascuna realtà locale. Al fine di coordinare l'assessment ed elaborare i risultati è stata istituita una Cabina di Regia.

I controlli corrispondenti alle domande incluse nella checklist utilizzata nel corso delle visite on-site, sono stati referenziati gli standard NIST, Cyber Security Framework e CSA con riferimento alla sezione Cloud («framework di riferimento»).
I livelli di maturità per ciascuna category relativa al «framework di riferimento» sono strutturati su un modello CMMI a 6 livelli da «Non Adeguato» (Livello 0) fino a «Stabile e Flessibile» (Livello 5), secondo la seguente nomenclatura.

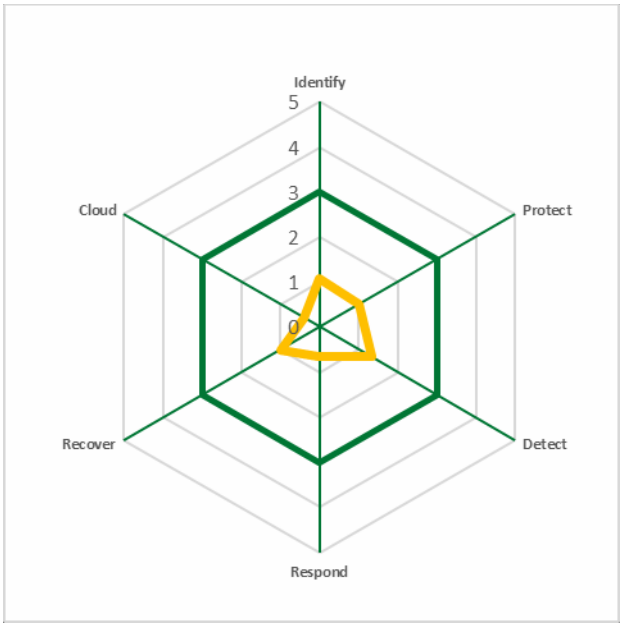
4,1 – 5,0	**Stabile e Flessibile**. Le attività volte alla copertura del controllo e dei rischi inerenti rispettano gli standard del livello precedente, integrando l'uso di strumenti dedicati alla misurazione dei risultati ai fini del miglioramento continuo e dell'aggiornamento dei processi
3,1 – 4,0	**Approccio Misurato e Controllato**. Le attività volte alla copertura del controllo e dei rischi inerenti prevedono la presenza di standard di sicurezza aggiuntivi rispetto ai requisiti minimi identificati
2,1 – 3,0	**Approccio Proattivo e Soddisfacimento dei requisiti minimi**. Le attività volte alla copertura del controllo e dei rischi inerenti avvengono secondo un processo standardizzato che prevede il soddisfacimento dei requisiti minimi di sicurezza identificati.
1,1 – 2,0	**Approccio Destrutturato**. Le attività volte alla copertura del controllo e dei rischi inerenti avvengono secondo un processo ripetibile ma non sono presenti processi formali diffusi su tutto il perimetro in oggetto
0,6 – 1,0	**Approccio Reattivo**. Le attività volte alla copertura del controllo e dei rischi inerenti sono implementate occasionalmente, in base alla necessità o

	all'iniziativa dei singoli
0 – 0,5	**Non adeguato**. Non sono rilevati un numero sufficiente di elementi atti alla copertura dei requisiti oggetto del controllo

È stato individuato il Livello 3 «Approccio Proattivo» quale livello target a cui tendere. Tale Livello target corrisponde alla copertura di 66 requisiti di sicurezza identificati come minimi in termini di postura Cyber degli Enti. Tali requisiti di sicurezza rappresentano un sottoinsieme dei controlli corrispondenti alle 236 domande incluse nella checklist. Il livello di aderenza degli Enti a ciascun requisito minimo è stato valutato su 3 livelli («Coperto», «Parzialmente coperto», «Non coperto») sulla base delle risposte relative alle domande del questionario.
Il livello di maturità AS-IS e target è stato valutato per ogni Ente sulle Function e sulle Category del NIST e del CSA, di seguito descritte.

Functions	Category	ID
Identify	Asset management	ID.AM
	Governance	ID.GV
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes and Procedures	PR.IP
	Protective Technology	PR.PT
Detect	Anomalies and events	DE.AE
	Detection Processes	DE.DP
	Security Continuous Monitoring	DE.CM
Respond	Analysis	RS.AN
	Communications	RS.CO
	Mitigations	RS.MI
	Response Planning	RS.RP
	Improvement	RS.IM
Recover	Improvement	RC.IM
	Recovery planning	RC.RP
Cloud	Cloud Security Alliance Controls Matrix	CSA.CM

A ciascun Ente è stato condivisa una rappresentazione del proprio livello di maturità simile a quella esemplificativa di seguito riportata.



Figurina 1: Esempio di livello di maturità Function NIST e CSA

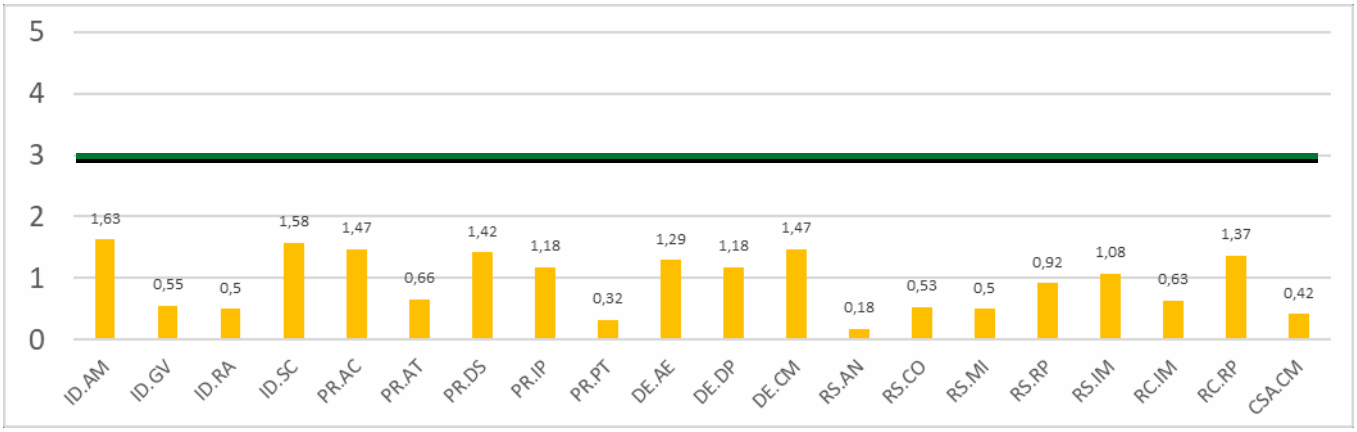


Figura 2: Esempio di livello di maturità Category NIST e CSA

Con riferimento ai 66 requisiti minimi, sono state identificate le seguenti 25 azioni tattiche allo scopo di attivare un piano immediato e sostenibile di rafforzamento della postura di sicurezza degli Enti; tali azioni e la loro immediatamente successiva evoluzione (e.g. l'implementazione di specifiche tecnologie di sicurezza individuate nella fase tattica) avrebbero permesso il raggiungimento del Livello 3 (target).

DESCRIZIONE AZIONI TATTICHE	
IDENTIFY	**ID.1 Identificare il perimetro degli asset critici (in termini di disponibilità, integrità e riservatezza dei dati), incluse dipendenze e priorità di recovery, e selezionare una soluzione di Asset Management da implementare [ALTA PRIORITÀ]**
	ID.2 Identificare il set minimo di informazioni da censire e la frequenza degli aggiornamenti
PROTECT	PR.1 Rafforzare i meccanismi di gestione sicura degli accessi remoti da parte di personale terze parti
	PR.2 Implementare la segmentazione di rete e controllare i flussi tra i vari segmenti
	PR.3 Eseguire una review di tutti gli accessi privilegiati, disabilitando quelli non necessari, e selezionare una soluzione di Privileged Access Management (PAM) da implementare [ALTA PRIORITÀ]
	PR.4 Implementare meccanismo di Multi Factor Authentication (MFA) per l'accesso ad asset critici

	[ALTA PRIORITÀ]
	PR.5 Rafforzare i meccanismi di controlli accessi e password policy
	PR.6 Sviluppare un piano di formazione/awareness su temi di cybersecurity per tutto il personale [ALTA PRIORITÀ]
	PR.7 Implementare soluzioni di analisi del traffico email per filtrare le comunicazioni a rischio rispetto a parametri personalizzabili (e.g. IP, Blacklist, etc.), incluse funzionalità di sandboxing
	PR.8 Implementare i certificati digitali necessari all'autenticazione dell'identità dei siti-web per ottenere una connessione crittografata e sicura
	PR.9 Identificare i dati sensibili che necessitano di essere crittografati ai fini del soddisfacimento dei requisiti normativi (e.g. GDPR) e i rispettivi sistemi sui quali risiedono allo scopo di implementare processi di crittografia at rest e in transit
	PR.10 Identificare un subset di sistemi di fileshare sicuri (e.g. Citrix) e comunicare agli utenti l'obbligo di utilizzare solamente le soluzioni identificate nel subset
	PR.11 Implementazione soluzione EDR/XDR [ALTA PRIORITÀ]
	PR.12 Analisi delle attuali politiche e configurazioni di logging/auditing degli asset critici al fine di avviare un percorso di integrazione con sistemi di log monitoring [ALTA PRIORITÀ]
	DE.1 Esecuzione VA/PT (Vulnerability Assessment e Penetration Test) e relativa Remediation per le vulnerabilità «High»
	DE.2 Implementare un meccanismo che permetta agli utenti di segnalare potenziali email malevole
DETECT	**DE.3 Avviare tutte le analisi necessarie per dotarsi di un servizio SOC/MDR per il monitoraggio degli allarmi di sicurezza [ALTA PRIORITÀ]**
	DE.4 Implementare un sistema di Intrusion Detection
	DE.5 Attivazione immediata di un processo per la revisione regolare delle regole firewall
RESPOND	**RS.1 Definire ruoli/responsabilità e processo per la gestione degli incidenti di sicurezza (e.g. Isolamento LAN interna e scollegamento macchine dalla rete; tempestiva comunicazione verso il CyberSOC ARIA) [ALTA PRIORITÀ]**
	RC.1 Esecuzione test di ripristino dai backup
RECOVER	RC.2 Implementazione di sistemi di backup per sistemi e dati on-prem e in cloud
	RC.3 Implementare mezzi di conservazione off-line della golden copy [ALTA PRIORITÀ]
	CSA.1 Definire ruoli e responsabilità nell'ambito dei servizi Cloud (e.g. RACI)
CLOUD	CSA.2 Implementazioni di soluzioni di log monitoring ed ingestion per gli accessi ai dati

Sul totale delle azioni tattiche sono inoltre state individuate 9 azioni ad alta priorità.

In base ai risultati dell'assessment sono state individuate, per ognuno degli Enti, le azioni tattiche necessarie per raggiungere il livello Target, sia quelle ad alta priorità che quelle a priorità standard.

Regione Lombardia ha deciso di finanziare l'implementazione di due azioni ad alta priorità per tutti gli Enti:

- PR.6 Formazione e awareness: sviluppare un piano di formazione/awareness su temi di cybersecurity per tutto il personale;

- PR.11 EDR/XDR: implementazione soluzione EDR/XDR e altre 5 azioni tra quelle ad alta priorità per ogni Ente, a propria scelta in base alle necessità.

Ogni Ente ha avuto la possibilità di implementare su propria iniziativa e con proprie risorse le azioni tattiche indicate come necessarie in seguito all'assessment.

3. Azioni svolte con il supporto della Task Force

In base ai criteri sopra descritti, da settembre 2022 a febbraio 2023 sono state erogate le seguenti attività:

ID azione	Titolo azione	N° Enti su cui è stata erogata dalla Task Force
ID.1	Identificazione e gestione degli asset critici	19
PR.2	Segmentazione di rete	3
PR.3	Review e gestione degli accessi privilegiati	36
PR.4	Multi-Factor Authentication (MFA)	20
PR.6	Formazione e awareness	Azioni proposte come prioritarie e rivolte a tutti gli Enti (coperte da RL)
PR.11	EDR/XDR	
PR.12	Politiche e configurazioni di logging/auditing	31
DE.3	Servizio SOC/MDR	28
RS.1	Gestione degli incidenti di sicurezza	29
RC.3	Conservazione off-line della golden copy	10

ID.1 Identificazione e gestione degli asset critici

L'attività è stata svolta con l'obiettivo di assegnare un livello di criticità agli asset IT sulla base della rilevanza dei dati conservati e processati in termini di riservatezza, integrità e disponibilità, oltre che di raccogliere requisiti per la definizione di un processo e di uno strumento di asset management.

PR.2 Segmentazione di rete

È stata analizzata la configurazione di rete dell'Ente, individuate le potenziali debolezze e vulnerabilità, e predisposto un piano di segmentazione della rete al fine di limitare la possibilità di movimenti laterali in caso di attacco e aumentare la protezione degli asset critici.

PR.3 Review e gestione degli accessi privilegiati

Attività svolta con l'obiettivo di aumentare la consapevolezza rispetto gli attuali rischi a cui sono esposti gli account privilegiati, effettuare una review degli stessi per disabilitare quelli non necessari, individuare raccomandazioni e best practices rispetto allo stato corrente e definire una roadmap implementativa di una soluzione PAM.

PR.4 Multi-Factor Authentication (MFA)

È stato analizzato lo stato attuale (as-is) dell'Ente in termini di asset critici, tecnologie, procedure di accesso, policy, processi, licenze, e identificato lo stato futuro (to-be), con la definizione di una strategia di adozione MFA e di una roadmap progettuale per la transizione dal «as-is» al «to-be».

PR.6 Formazione e awareness

Le attività formative e di awareness sono state erogate centralmente da ARIA secondo due differenti modalità rivolte a interlocutori diversi.

La prima modalità di erogazione è quella della formazione in aula su temi cyber governance e tech, rivolta al personale degli Enti che in maniera particolare tratta questi temi, ovvero:

- Responsabili e amministratori IT (personale SIA e IC),
- Responsabili Sicurezza IT,
- Referenti NIS,
- Referenti applicativi/Key user,
- Responsabili trattamenti,
- Risk manager.

Nel corso del 2022 sono stati erogati ad ognuno dei partecipanti due moduli formativi della durata di 4 ore l'uno. Hanno partecipato all'iniziativa tutti i 40 Enti, per un totale di 577 persone partecipanti.

La seconda modalità di erogazione è quella della formazione a distanza su temi di cybersecurity awareness, rivolta a tutto il personale dell'Ente. Il piano di awareness prevede un corso svolto in modalità e-learning con quiz interattivi di sicurezza informatica con focus specifico sui seguenti scenari:

- In ufficio
- A casa
- In viaggio e mobilità
- In ospedale

L'attività di cybersecurity awareness è stata avviata durante il mese di maggio 2023 e, rispetto ai dati registrati, in data 13/09/2023 risulta essere stata completata da 10.267 persone.

PR.11 EDR/XDR

L'attività di implementazione di un sistema di EDR/XDR è stata considerata fondamentale per innalzare il livello di maturità degli Enti ed è quindi stata erogata su tutti i 40 Enti. L'attività ha previsto l'implementazione di un sistema di Endpoint/eXtended Detection Response (EDR/XDR) per consentire la protezione e il monitoraggio della sicurezza di tutti i server e i client dell'Ente, attraverso il rilevamento e la reazione ad eventi significativi di sicurezza che abbiano come oggetto gli Endpoint.

La Task Force ha individuato 3 diversi strumenti tecnologiche che dessero la possibilità di essere erogati come servizi gestiti. Al momento sono stati installati 70.051 agenti EDR, distribuiti su 33 enti.

PR.12 Politiche e configurazioni di logging/auditing

L'attività ha previsto l'analisi e valutazione delle politiche di logging presenti per ciascuno degli asset ritenuti critici dall'organizzazione e la definizione di specifiche linee guida per la collezione dei log prodotti dagli elementi analizzati con l'obiettivo di migliorare il processo di monitoraggio di sicurezza.

DE.3 Servizio SOC/MDR

L'attività è stata svolta con l'obiettivo di raccogliere i dati necessari per dimensionare correttamene un servizio di Security Operation Center (SOC) e definire i requisiti di processo e funzionali per la gestione degli incidenti di sicurezza da parte del SOC.

RS.1 Gestione degli incidenti di sicurezza

Definizione di ruoli e responsabilità da attribuire all'interno dell'Ente per una tempestiva ed efficace presa in carico deli incidenti di sicurezza. L'attività ha inoltre previsto la definizione dei processi da seguire per la rilevazione, classificazione, escalation e gestione degli incidenti di sicurezza al fine di minimizzarne gli impatti, predisponendo una procedura per la gestione degli incidenti di sicurezza e un runbook di dettaglio per la gestione tecnica di determinate casistiche.

RC.3 Conservazione off-line della golden copy

Attività svolta con l'obiettivo di garantire l'integrità dei backup dei dati critici e le capacità di ripristino, attraverso l'individuazione delle applicazioni in golden copy e la definizione di strategie e procedure di ripristino.

Cyber Threat Intelligence

Oltre alle attività verticali svolte dalla Task Force, è stato attivato presso tutti gli Enti Sanitari un servizio di monitoraggio di Cyber Threat Intelligence (CTI). Tale attività si basa sui risultati di un assessment preliminare svolto per individuare il

perimetro di ciascun Ente, e, attraverso analisi automatiche e manuali, mira ad identificare informazioni esposte pubblicamente, evidenziando potenziali rischi collegati alla loro presenza al di fuori del perimetro aziendale.

Il servizio prevede che, una volta identificate, tali informazioni vengono segnalati agli Enti coinvolti; le tipologie di segnalazioni oggetto del servizio di CTI sono le seguenti:

- Esfiltrazione dati;
- Credenziali esposte;
- Campagne malevole in corso che hanno come target l'Ente;
- Account compromessi.

Le attività verticali (o stream), coordinate e monitorate a livello centrale dalla Cabina di Regia, sono state erogate dalle aziende coinvolte dalla Task Force. A livello locale è stato assegnato ad ogni Ente un Service Manager che ha avuto il ruolo di interfaccia tra i singoli Enti e le aziende della Task Force che hanno eseguito le attività verticali, oltre che tra i singoli Enti e la Cabina di Regia. Tale modello organizzativo è riassunto nello schema di seguito rappresentato.

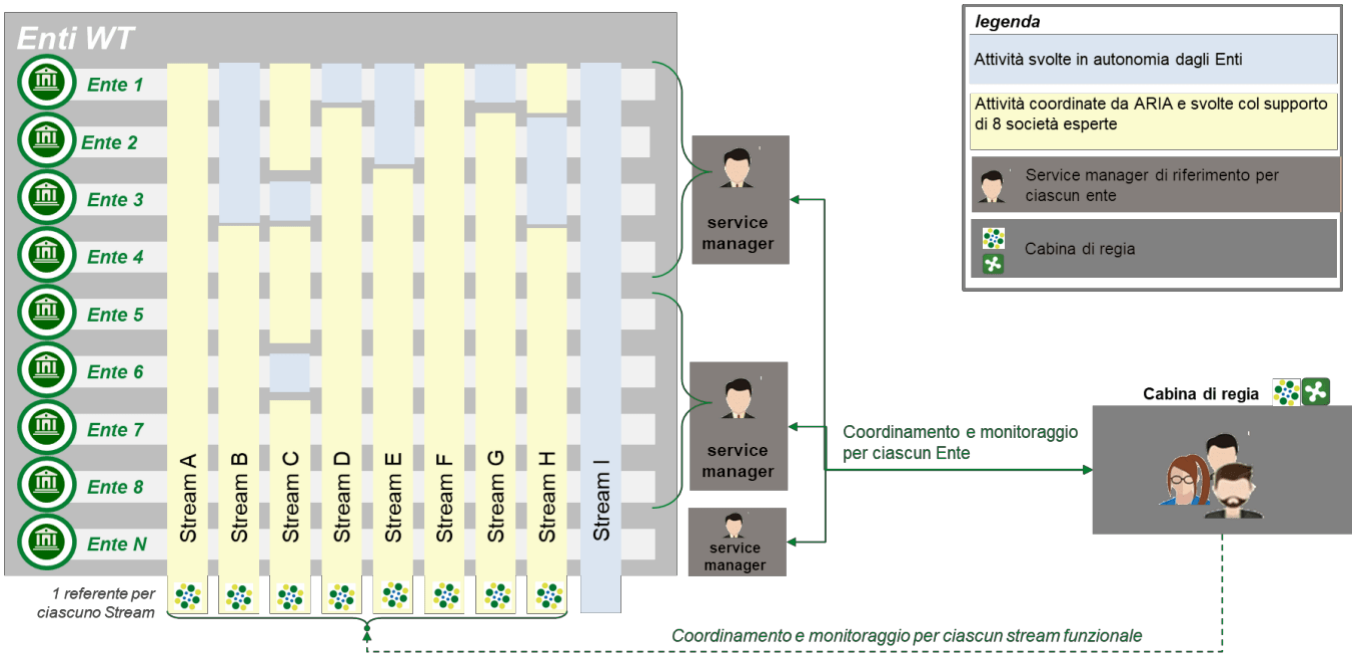


Figura 3: Schema del modello organizzativo adottato dalla Task Force

4. Nuova valutazione del livello di maturità degli Enti

Con l'obiettivo di individuare il livello di maturità raggiunto dagli Enti a fronte delle iniziative puntuali svolte nel corso dell'anno precedente, durante il mese di gennaio 2023 è stato nuovamente eseguito l'assessment presso gli Enti, utilizzando lo stesso framework predisposto a maggio 2022.

L'assessment è stato eseguito in modalità self-assessment da parte dell'Ente, pertanto, come nel 2022, non sono state richieste e verificate le evidenze a supporto delle risposte fornite dai singoli referenti al proprio Service Manager che ha supportato lo svolgimento dell'attività.

Si precisa che l'ambito di analisi "Cloud" è stato parzialmente coinvolto nelle attività programmate dagli Enti Sanitari nel primo anno di attuazione del modello di miglioramento in quanto saranno oggetto di iniziative specifiche, anche con il supporto di risorse finanziate dal Piano nazionale di Ripresa e Resilienza, che hanno l'obiettivo di migrare progressivamente l'intera infrastruttura tecnologica degli Enti in Cloud entro il primo semestre del 2025.

Nonostante sia necessario programmare diversi ulteriori interventi tecnici e organizzativi per il raggiungimento del livello obiettivo, la metodologia adottata e la modalità di coordinamento e conduzione delle diverse attività svolte centralmente e localmente nel corso del 2022 hanno dimostrato una buona efficacia in termini di miglioramento continuo del livello di maturità della sicurezza informatica del sistema sociosanitario e di progressiva diffusione e allineamento su tutti gli Enti coinvolti.

Proprio in considerazione del buon esito delle attività svolte nel corso del 2022, il modello per la valutazione della maturità della gestione della sicurezza informatica applicato dagli Enti Sanitari pubblici è stato presentato anche gli Enti Sanitari Privati accreditati allo scopo di valutare la possibile adozione da parte loro. In tale caso Regione Lombardia disporrebbe di uno strumento condiviso che consentirebbe di conoscere il livello complessivo di sicurezza del sistema sociosanitario e di evidenziare eventuali punti di debolezza sui quali indirizzare gli investimenti al fine di perseguire il continuo miglioramento nell'ambito della sicurezza informatica e della protezione dei dati.

5. Programma di interventi proposti per gli anni successivi

Con riferimento ai piani di miglioramento della sicurezza degli Enti Sanitari richiesti attraverso la Deliberazione n°XI/7758 del 28/12/2022 "DETERMINAZIONI IN ORDINE AGLI INDIRIZZI DI PROGRAMMAZIONE PER L'ANNO 2023" sono state individuate alcune attività in ambito cybersecurity ritenute prioritarie per gli Enti.

La prioritizzazione delle attività è stata guidata centralmente dalla Cabina di Regia ma effettuata direttamente dagli Enti, col supporto dei Service Manager, ognuno secondo le proprie necessità.

5.1 Identificazione delle azioni

5.1.1 Proposta delle azioni da svolgere

In continuità con il programma di interventi dello scorso anno è stato deciso di proseguire con la fase implementativa delle azioni propedeutiche che ogni Ente ha svolto nel corso del 2022 col supporto della Task Force. Per ciascuna di tali azioni è stata quindi individuata la rispettiva azione implementativa come riportato nella tabella sottostante.

ID azione	Azione svolta nel 2022	Attività implementativa
ID.1	Identificazione e gestione degli asset critici	Implementazione di uno strumento di asset management
PR.2	Segmentazione di rete	Supporto tecnico per l'implementazione della segmentazione della rete
PR.3	Review e gestione degli accessi privilegiati	Implementazione di uno strumento di Privileged Access Management (PAM)
PR.4	Multi-Factor Authentication (MFA)	Implementazione dei meccanismi di Multi-Factor Authentication (MFA)
PR.12	Politiche e configurazioni di logging/auditing	Implementazione di uno strumento di Log Collector
DE.3	Servizio SOC/MDR	Attivazione del servizio SOC di ARIA
RS.1	Gestione degli incidenti di sicurezza	Declinazione del processo rispetto agli attori specifici dell'Ente, personalizzazione e test dei playbook rispetto alle infrastrutture e alle tecnologie
RC.3	Conservazione off-line delle golden copy	Implementazione mezzi di conservazione off-line delle golden copy

5.1.2 Prioritizzazione delle attività

Nei primi mesi del 2023 è stato chiesto ad ogni Ente di esprimere la propria priorità rispetto alle attività implementative sulla base delle proprie necessità operative e strategiche. Ogni Ente ha potuto inserire in una propria classifica solamente le attività implementative facenti riferimento ad azioni propedeutiche completate nel corso del 2022.

Al termine della mappatura è stato possibile identificare sia le attività implementative prioritarie per ciascun Ente sia le esigenze strategiche di tutti gli Enti al fine di poter definire un piano di lavori personalizzato.

È stato inoltre richiesto agli Enti di definire le priorità sulle attività tattiche propedeutiche e individuate come prioritarie nel 2022 che non ha potuto svolgere con il supporto della Task Force, in quanto inserite lo scorso anno come priorità maggiore di 5. Tale classificazione mira a garantire a tutti gli Enti la possibilità raggiungere la medesima postura di sicurezza e sbloccare nuove attività implementative.

5.1.3 Selezione delle attività

Si riportano di seguito i risultati della prioritizzazione delle attività effettuata dagli Enti, sulla base della quale le attività implementative proposte sono state inserite in una classifica.

Attività implementativa	Punti[1]	n° Enti che hanno messo l'azione come priorità 1	n° Enti che hanno messo l'azione come priorità 2	n° Enti che hanno messo l'azione come priorità 3	n° Enti che hanno messo l'azione come priorità 4	n° Enti che hanno messo l'azione come priorità 5
Implementazione di uno strumento di Privileged Access Management (PAM)	139	11	15	6	3	0
Attivazione del servizio SOC di ARIA	104	15	3	2	5	1
Implementazione di uno strumento di Log Collector	95	2	8	12	8	1
Implementazione dei meccanismi di Multi-Factor Authentication (MFA)	71	6	6	4	1	3
Declinazione del processo rispetto agli attori specifici	66	4	4	6	4	4

[1] I *punti ad ogni azione sono stati calcolati assegnando 5 punti per ogni volta che questa viene inserita come priorità 1, 4 punti per priorità 2, 3 punti priorità 3, 2 punti priorità 4 e 1 punto priorità 5.*

dell'Ente, personalizzazione e test dei playbook rispetto alle infrastrutture e alle tecnologie						
Implementazione di uno strumento di asset management	41	1	1	4	7	6
Implementazione mezzi di conservazione off-line della golden copy	20	0	2	2	1	4
Supporto tecnico per l'implementazione della segmentazione della rete	9	0	1	1	0	2

Rispetto alla classifica finale emerge chiaramente come l'implementazione di strumenti Privileged Access Management (PAM) e l'attivazione del servizio SOC di ARIA siano le azioni maggiormente richieste dagli Enti.

Per questo motivo, e in un'ottica di contenimento dei costi sfruttando il fenomeno di economia di scala, è stato scelto di circoscrivere a queste due azioni il supporto della Task Force proponendo ad ogni Ente l'azione che tra le due ha posizionato a un livello più alto di priorità.

Tale scelta corrisponde alle esigenze di Regione Lombardia e ARIA di programmare ed attuare in modalità coordinata e controllata interventi su ambiti di rilevante miglioramento del livello di sicurezza informatica di ciascun singolo Ente e del sistema sociosanitario complessivo.

A queste si aggiunge, per alcuni Enti che lo necessitano, l'implementazione di uno strumento di Log Collector, strumento necessario alla corretta attivazione dei servizi erogati dal SOC.

5.2 Programma degli interventi

Il programma di interventi la cui implementazione deve essere avviata nel corso del 2023 e deve proseguire negli anni successivi è stato predisposto con lo scopo di migliorare l'attuale livello di sicurezza di ciascun Ente e di tutto il Sistema Federato di Regione Lombardia.

È bene notare che i costi relativi a queste attività rappresentano una nuova voce di spesa per il Sistema Regionale in quanto mai sostenute negli anni precedenti. Tale mancanza ha portato ad una situazione non sostenibile per la sicurezza delle informazioni in termini di maturità delle misure di protezione poste in essere e, pertanto, pericolosa rispetto all'attuale scenario cyber.

Si evidenzia, inoltre, che la gestione di queste iniziative non può prescindere da un modello federato in cui l'entità centrale, Regione Lombardia, ne indirizza e guida l'applicazione. Una gestione decentralizzata e completamente autonoma a livello dei singoli Enti da un lato ostacolerebbe il controllo e la comprensione da parte di Regione Lombardia del livello di maturità dell'intero sistema e delle misure necessarie di innalzamento di tale livello, dall'altro graverebbe sugli Enti anche in considerazione della mancanza di cultura rispetto ai temi di cybersecurity al loro interno: le risorse IT, per la maggior parte dei casi già di piccole dimensioni, non hanno competenze e figure professionali dedicate alla gestione degli aspetti di sicurezza informatica.

Il programma di interventi è diviso in due macro-aree:

- Attività implementative: strumenti Privileged Access Management (PAM) e servizio SOC di ARIA con l'implementazione di uno strumento di Log Collector, selezionate come prioritarie dagli Enti rispetto alle attività proposte dalla Cabina di Regia per l'evoluzione del piano tattico 2023. Queste attività saranno svolte con il supporto della Task Force presso ciascun Ente secondo la divisione riportata sopra.
- Attività continuative rispetto a quelle già avviate nel 2022: Servizio di Cyber Threat Intelligence, Servizio di EDR/XDR, Supporto Formazione & Awareness in modalità e-learning e il supporto dato a ogni Ente dai Service Manager coordinato dalla Cabina di Regia.

A queste si aggiungono:

- attività di Simulazione di un incident in modalità Table Top: l'obbiettivo principale dell'esercitazione è quello di rafforzare l'awareness e la resilience dell'Ente. Grazie a questa attività è possibile:
  - Verificare se l'organizzazione risponde in modo coerente e tempestivo ad un incident con ulteriore fuga dei dati attraverso il disegno e la simulazione di scenari realistici;
  - Riscontrare il livello di efficienza ed efficacia delle comunicazioni interne fra gli stakeholder nella risoluzione dell'evento;
  - Verificare l'aderenza ai processi di gestione dell'incident a livello organizzativo e tecnico;
  - Sviluppare una maggiore consapevolezza sulle minacce legate ai dati personali trattati in ambito ospedaliero;
  - Stressare l'importanza di una corretta gestione della privacy a tutti i livelli ed in modo trasversale all'azienda.
- attività di VAPT: Vulnerability Assessment & Penetration Test finalizzati a verificare l'efficacia delle misure di sicurezza dei sistemi poste in essere da ciascun Ente ed individuare le eventuali vulnerabilità presenti in modo da consigliare un piano di risoluzione volto a sanarle.

La tabella sottostante riassume le iniziative previste dal programma per l'anno 2023 e per gli anni successivi, mostrando anche i costi relativi a ciascuna attività.

Attività implementativa	Totale 2023	Totale 2024	Totale 2025
Implementazione di uno strumento di **Privileged Access Management (PAM)**	329.400,00 €	1.000.000,00 €	1.000.000,00 €
Attivazione e gestione del **servizio SOC di ARIA**	1.529.880,00 €	5.770.600,00 €	5.770.600,00 €
Implementazione di uno **strumento di Log Collector**	536.800,00 €	-	-
	2.396.080,00 €	**6.770.600,00 €**	**6.770.600,00 €**
Chiusura attività 2022	724.800,00 €	-	-
CTI	1.464.000,00 €	1.464.000,00 €	1.464.000,00 €
EDR/XDR	1.750.000,00 €	2.650.000,00 €	2.650.000,00 €
Formazione - Awareness	57.340,00 €	57.340,00 €	57.340,00 €
Formazione – Simulazione Table Top	97.600,00 €	195.200,00 €	195.200,00 €
Predisposizione Strumento AdR in Self Assessment e Tool per Security Maturity Assessment	107.360,00 €	-	-
Service manager	317.700,00 €	317.700,00 €	317.700,00 €
Cabina di regia	205.000,00 €	205.000,00 €	205.000,00 €
VAPT	655.200,00 €	218.400,00 €	218.400,00 €
	5.379.000,00 €	**5.107.640,00 €**	**5.107.640,00 €**
Totale	**7.775.080,00 €**	**11.878.240,00 €**	**11.878.240,00 €**