



Regione Lombardia

LA GIUNTA

DELIBERAZIONE N° XII / 1542

Seduta del 18/12/2023

Presidente

ATTILIO FONTANA

Assessori regionali MARCO ALPARONE *Vicepresidente*

ALESSANDRO BEDUSCHI

GUIDO BERTOLASO

FRANCESCA CARUSO

GIANLUCA COMAZZI

ALESSANDRO FERMI

PAOLO FRANCO

GUIDO GUIDESI

ROMANO MARIA LA RUSSA

ELENA LUCCHINI

FRANCO LUCENTE

GIORGIO MAIONE

BARBARA MAZZALI

MASSIMO SERTORI

CLAUDIA MARIA TERZI

SIMONA TIRONI

Con l'assistenza del Segretario Riccardo Perini

Su proposta del Presidente Attilio Fontana di concerto con l'Assessore Guido Bertolaso

Oggetto

APPROVAZIONE DEL PROGRAMMA DELLA XII LEGISLATURA PER LA SICUREZZA DEI DATI E DEI SERVIZI - (DI CONCERTO CON L'ASSESSORE BERTOLASO)

Il Segretario Generale Antonello Turturiello

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

Il Direttore Centrale Aldo Colombo

Il Direttore Generale Giovanni Pavesi

La Dirigente Chiara Penello

Il Dirigente Giovanni Delgrossi

L'atto si compone di 114 pagine

di cui 109 pagine di allegati

parte integrante

PREMESSO CHE:

- la tecnologia è diventata ormai parte integrante della quotidianità, modificando in particolare le relazioni fra le persone, le modalità di lavoro, di comunicazione, di spostamento;
- lo scenario è in continua evoluzione e ha conosciuto un'accelerazione durante la pandemia da Covid-19 quando sono stati attivati in emergenza numerosi servizi basati su nuove tecnologie e si sono rapidamente diffuse nuove forme di lavoro in mobilità senza la necessaria pianificazione e attuazione di misure di sicurezza compensative;
- gli scenari sociopolitico e del cybercrime, costantemente in evoluzione negli ultimi anni, hanno evidenziato ed enfatizzato i rischi per l'erogazione dei servizi al cittadino da parte delle PA;
- la diffusione dei servizi cloud spesso spinge le organizzazioni a delegare al Cloud Service Provider anche aspetti di sicurezza che secondo il modello di responsabilità condiviso dovrebbero essere in carico all'organizzazione;

RICHIAMATI:

- il Regolamento Europeo in materia di protezione dei dati personali ("GDPR") e Decreto Legislativo 10 agosto 2018, n. 101, che hanno completamente cambiato il paradigma di conformità alla normativa privacy e che pertanto richiedono un grosso lavoro di analisi e di adeguamento;
- la Direttiva NIS 2 che si configura quale aggiornamento a miglioramento della Direttiva NIS n. 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (approfondimento par. 1.3.1 "Direttiva NIS e NIS2");
- le Misure di Sicurezza AGID che prevedono il recepimento dei livelli di sicurezza previsti dall'Agenzia per l'Italia Digitale (AGID);
- la strategia nazionale di cybersicurezza 2022 – 2026 pubblicata dall'Agenzia Nazionale per la Cybersicurezza (ACN) che ha lo scopo di pianificare, coordinare e attuare misure tese a rendere il Paese più sicuro e resiliente;
- la Strategia Cloud Italia che prevede nuovi livelli di adeguamento per le infrastrutture digitali e per i servizi Cloud per la pubblica amministrazione, fino al completamento della migrazione dei servizi presso il PSN (Polo Strategico Nazionale) o altro Cloud Provider qualificato entro il 30 Giugno 2026;
- il Piano Nazionale di Ripresa e Resilienza (PNRR) ed in particolare la Componente 1 della Missione 1, che interessa il Programma per la sicurezza dei dati e dei servizi e ha l'obiettivo di trasformare la Pubblica Amministrazione attraverso una strategia centrata sulla digitalizzazione;

RICHIAMATO, altresì, il Programma Regionale di Sviluppo Sostenibile della XII

Legislatura (PRSS) ed in particolare l'obiettivo strategico 7.5.3 che mira al 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 (cyber-security);

ATTESO CHE:

- con Deliberazione della Giunta Regionale n. 2683/2019 Regione si è dotata di un Programma di sicurezza e privacy triennale per tutto il Sistema federato, che ha consentito di rispondere alle esigenze, alle minacce e alle opportunità che si sono manifestate nel corso dell'ultimo triennio;
- il Sistema federato è composto da Regione Lombardia, dagli Enti e dalle Società del Sistema Regionale (ex L.r. 30/2006), dal Territorio Sanitario composto da Aziende Sanitarie pubbliche (ASST e ATS) ed Enti Erogatori Privati Accreditati (EEPA) della Socio Sanità e dal Consiglio regionale;

CONSIDERATO CHE:

- Regione intende proseguire nel solco di quanto realizzato grazie al Programma sopra citato rafforzando il governo e la maturità di Sicurezza e Privacy di tutto il Sistema Federato, ossia garantire Riservatezza, Integrità e Disponibilità del patrimonio informativo, con particolare riferimento ai dati personali adottando un Programma per la sicurezza dei dati e dei servizi che abbraccia tutta la XII legislatura e si sviluppa sulle linee programmatiche contenute nel Programma Regionale di Sviluppo Sostenibile (PRSS) avendo come priorità l'obiettivo strategico 7.5.3 sopra richiamato;
- Regione sta realizzando i progetti "Programma sicurezza e protezione dei dati" e "Potenziamento CSIRT Regione Lombardia" finanziati con fondi PNRR, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity";

VISTO il Programma allegato alla presente deliberazione come parte integrante e sostanziale, che definisce la strategia e le priorità di intervento in tema di sicurezza delle informazioni, dei dati, delle infrastrutture e di conformità alle normative e standard ricostruendo un quadro organico delle diverse linee di sviluppo in corso;

ATTESO che il Programma prevede un modello di Governance del Sistema Federato allo scopo di promuovere un'azione comune sulle tematiche di Sicurezza e Privacy a livello sia centrale che territoriale e sviluppare le sinergie tra i diversi ambiti di intervento per garantire:

- una chiara ed efficiente attribuzione delle responsabilità, sia nella gestione che nell'operatività;

-
- la collaborazione e comunicazione tra le parti, la condivisione delle informazioni e la formalizzazione di linee guida e procedure comuni con l'obiettivo di ottimizzare le risorse e le competenze a disposizione e generare valore aggiunto sia in termini di contenuti che di efficacia degli interventi;

ATTESO che le modalità di attuazione del programma saranno oggetto di una pianificazione da parte di Regione Lombardia con il supporto di ARIA, sulla base del modello di Governance del Sistema Federato. Con specifico riferimento alle attività portate avanti da Regione Lombardia, la programmazione operativa delle stesse ha luogo in concomitanza alla formalizzazione degli incarichi;

RITENUTA la realizzazione coerente con il modello di attuazione per il Governo della Sicurezza delle Informazioni e Privacy che Regione Lombardia ha definito al fine di valorizzare e sfruttare tutte le possibili sinergie all'interno del Sistema Federato;

CONSIDERATA la DGR XII/1224 del 30/10/2023 "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", che approva il "Modello di Sicurezza Informatica degli Enti Sanitari basato sugli ambiti di intervento Identify, Protect, Detect, Recover e Cloud";

VERIFICATO che con DGR XII/1224 la Direzione Generale Welfare ha stanziato le risorse economiche per il triennio 2023-2025 necessarie per proseguire nel percorso tecnico e organizzativo condiviso con tutti gli Enti Sanitari Pubblici e coordinato centralmente che porti ad un graduale e costante miglioramento del livello di sicurezza informatica dell'intero sistema sociosanitario regionale attraverso interventi specifici sia a livello centrale che locale;

RICHIAMATA la convenzione quadro approvata con DGR n. 7409 del 30/11/2022 e registrata nel RCCC il 13.12.2022 con n. 13200 che regola i rapporti tra Regione Lombardia e l'Azienda Regionale per l'Innovazione e gli Acquisti spa (ARIA);

STABILITO che le attività saranno svolte da ARIA spa sulla base del Piano delle attività e del Prospetto di raccordo della società approvato annualmente dalla Giunta regionale;

A voti unanimi, resi nelle forme di legge;

DELIBERA

1. di approvare, sulla base di quanto riportato in premessa, il Programma della XII Legislatura per la sicurezza dei dati e dei servizi allegato alla presente deliberazione come parte integrante e sostanziale (Allegato 1);
2. di stabilire che le attività saranno svolte da ARIA spa sulla base del Piano delle attività e del Prospetto di raccordo della società approvato annualmente dalla Giunta regionale;
3. di procedere alla pubblicazione del presente atto nella sezione Amministrazione Trasparente del sito istituzionale di Regione Lombardia, ai sensi dell'art. 37 del D.lgs 33/2013.

IL SEGRETARIO
RICCARDO PERINI

Atto firmato digitalmente ai sensi delle vigenti disposizioni di legge