Deliberazione della Giunta Regionale 3 dicembre 2024, n. 3-474
Legge n. 90/2024 ''Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici''. Individuazione del Referente regionale per la cybersicurezza e disposizioni organizzative

Seduta N° **31** Adunanza 03 DICEMBRE 2024

Il giorno 03 del mese di dicembre duemilaventiquattro alle ore 18:10 si è svolta la seduta della Giunta regionale in via straordinaria, in modalità telematica, ai sensi della D.G.R. n. 1-8208 del 26 febbraio 2024 con l'intervento di Alberto Cirio Presidente , Elena Chiorino Vice Presidente e degli Assessori Paolo Bongioanni, Enrico Bussalino, Marina Chiarelli, Marco Gallo, Matteo Marnati, Maurizio Raffaello Marrone, Gian Luca Vignale con l'assistenza di Guido Odicino nelle funzioni di Segretario Verbalizzante.
Assenti, per giustificati motivi: gli Assessori Marco GABUSI - Federico RIBOLDI - Andrea TRONZANO

DGR 3-474/2024/XII

OGGETTO:
Legge n. 90/2024 “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici”. Individuazione del Referente regionale per la cybersicurezza e disposizioni organizzative

A relazione di: Marnati, Vignale

Premesso che in data 17 luglio 2024 è entrata in vigore la legge n. 90/2024 “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici” che, in particolare:
all’articolo 1, comma 1, individua le pubbliche amministrazioni, quali soggetti che devono applicare le sue disposizioni, includendo anche le Regioni;
al successivo comma 2, sancisce in capo ai suddetti soggetti l’obbligo di segnalazione e notifica degli incidenti informatici dettagliando che:
- essi segnalino, senza ritardo e comunque entro il termine massimo di ventiquattro ore dal momento in cui ne sono venuti a conoscenza a seguito delle evidenze comunque ottenute, qualunque incidente riconducibile a una delle tipologie individuate nella tassonomia di cui all'articolo 1, comma 3-bis, del decreto legge n. 105/2019, convertito, con modificazioni, dalla legge n. 133/2019, e come modificato dall'articolo 3 della stessa legge n. 90/2024, aventi impatto su reti, sistemi informativi e servizi informatici;
- entro settantadue ore a decorrere dal medesimo momento, sono tenuti ad effettuare la notifica completa di tutti gli elementi informativi disponibili;
- la segnalazione e la successiva notifica sono effettuate tramite le apposite procedure disponibili nel sito internet istituzionale dell'Agenzia per la cybersicurezza nazionale;
all’articolo 2, comma 1, impone che in caso di segnalazioni puntuali dell'Agenzia per la

cybersicurezza nazionale circa specifiche vulnerabilità cui le pubbliche amministrazioni risultino potenzialmente esposte, queste provvedono, senza ritardo e comunque non oltre quindici giorni dalla comunicazione, all'adozione degli interventi risolutivi indicati dalla stessa Agenzia;
al successivo comma 2, dettaglia le sanzioni previste nei casi di inosservanza degli obblighi di notifica e di mancato o ritardato adeguamento a seguito delle segnalazioni di specifiche vulnerabilità dell'Agenzia per la cybersicurezza nazionale;
all'articolo 8, dispone di individuare, ove non sia già presente, una struttura, anche tra quelle esistenti, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, che provveda allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni (lettera a); alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico (lettera b); alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione (lettera c); alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione (lettera d); alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d) (lettera e); alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale (lettera f); al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza (lettera g); all'articolo 8, comma 2, introduce la figura del referente per la cybersicurezza, definendolo come il soggetto che opera presso la citata struttura, individuato in ragione di specifiche e comprovate professionalità e competenze in materia di cybersicurezza e che svolge anche la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalla legge citata e dalle normative settoriali in materia di cybersicurezza cui sono soggette le amministrazioni, disponendo che, a tal fine, il suo nominativo sia formalmente comunicato all'Agenzia per la cybersicurezza nazionale; all'articolo 9, dispone che vengano effettuate le verifiche che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso, che utilizzano soluzioni crittografiche, rispettino le linee guida sulla crittografia nonché quelle sulla conservazione delle password adottate dall'Agenzia per la cybersicurezza nazionale e dal Garante per la protezione dei dati personali e non comportino vulnerabilità note, atte rendere disponibili e intellegibili a terzi i dati cifrati.
Premesso, inoltre, che:
in data 17 gennaio 2023 è entrata in vigore la direttiva (UE) 2022/2555 (NIS 2) del Parlamento Europeo e del Consiglio 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 (NIS), da recepire da parte di tutti gli Stati membri dell'Unione europea entro il 17 ottobre 2024;
tale direttiva stabilisce misure volte a garantire un livello comune elevato di cybersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno, definendo una serie di obblighi e misure da adottare da parte degli Stati membri;
in Italia la suddetta direttiva è stata recepita con decreto legislativo n. 138 del 4 settembre 2024, pubblicato in G.U. il 1° ottobre 2024.
Preso atto che:
l'ultima relazione annuale al Parlamento, predisposta, ai sensi del decreto legge n. 82/2021, dall'Agenzia nazionale per la cybersicurezza (ACN), evidenzia, in un contesto in cui le minacce informatiche sono in costante aumento e interessano e impattano le funzioni essenziali dello Stato, come la cybersicurezza sia diventata cruciale per garantire l'interesse del Paese;
la stessa Agenzia sta coordinando diverse progettualità dedicate principalmente al miglioramento della postura di sicurezza del sistema Paese nel suo insieme, a partire dalla pubblica amministrazione, nel quadro delle riforme per la digitalizzazione dell'Italia e del Piano nazionale di ripresa e resilienza (PNRR), il quale dedica risorse anche alle amministrazioni regionali al fine di

incrementare la sicurezza cibernetica nazionale;
con determinazione del 18 gennaio 2023 del Direttore Generale dell'Agenzia di Cybersicurezza Nazionale è stata approvata la graduatoria definitiva dei progetti presentati da Regioni, Città metropolitane e province autonome a valere sull'Avviso 3/2022 "Avviso Pubblico n. 03/2022 per la presentazione di proposte di interventi di potenziamento della resilienza cyber delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane e delle Province autonome a valere sul Piano Nazionale di Ripresa e Resilienza, Missione 1, Componente 1, Investimento 1.5 "Cybersecurity", Codice d'investimento M1C1I1.5";
la suddetta determinazione ha finanziato, tra l'altro, due progetti presentati da parte della Regione Piemonte in data 27 settembre 2022.
Dato atto che tali progetti, di seguito descritti e che sono stati ultimati il 30 novembre 2024, hanno come obiettivo la messa in sicurezza e il rafforzamento di servizi e infrastrutture che negli anni sono stati sviluppati dalla Direzione regionale Competitività del Sistema regionale a favore della Regione Piemonte e delle altre pubbliche amministrazioni presenti nel territorio regionale:

- il primo progetto, denominato "Postazioni di lavoro e rete regionale: l'evoluzione in sicurezza", ha ottenuto un finanziamento di euro 984.400, e si articola in due tranche: una riguarda la verifica dello stato della sicurezza della rete informatica interna, la capacità di organizzare le difese e l'efficienza nel rispondere ad eventuali attacchi; l'altra prevede lo sviluppo e l'evoluzione della rete regionale per l'accesso delle amministrazioni locali alla piattaforma Cloud regionale;
- il secondo progetto, denominato "Transizione digitale e servizi sicuri", conta su un finanziamento di euro 995.100 e riguarda principalmente il rafforzamento delle competenze del personale in relazione all'aumento del livello di consapevolezza dei rischi di sicurezza cui sono esposti gli utenti della pubblica amministrazione, l'analisi della "cybersecurity posture", ovvero l'insieme dei dati che riguardano lo stato di sicurezza del software e dei servizi, la capacità di organizzarne le difese e l'efficienza nel rispondere ad eventuali attacchi e la realizzazione di strumenti di analisi vulnerabilità per evidenziare eventuali problemi di sicurezza e di conseguenza pianificare interventi di mitigazione.

Ritenuto, pertanto, in ottemperanza all'articolo 8 della legge n. 90/2024, di individuare quale Referente regionale per la cybersicurezza, per la Giunta regionale e le sue strutture, il Responsabile pro-tempore del Settore "Sistema Informativo regionale" della Direzione regionale Competitività del Sistema regionale, in considerazione delle specifiche materie di competenza, per rispondere sin d'ora a quando disposto dalla normativa, quale soluzione temporanea, nelle more delle procedure di riorganizzazione volte ad assicurare un assetto strutturato e specifico per lo svolgimento delle funzioni in materia di "cybersicurezza", in considerazione della particolare complessità quali-quantitaviva delle funzioni medesime.
Ritenuto, altresì, di demandare alla Direzione regionale Competitività del Sistema regionale la comunicazione all'Agenzia per la cybersicurezza nazionale relativa all'individuazione del Referente per la cybersicurezza, come previsto dell'articolo 8, comma 2, della legge n. 90/2024;
Ritenuto, inoltre, di disporre, quale soluzione organizzativa che, recependo quanto previsto dalle legge n. 90/2024, possano porre tempestivamente l'amministrazione regionale nelle condizioni di assolvere agli obblighi di segnalazione e notifica degli incidenti informatici verso l'Agenzia per la cybersicurezza nazionale, prendere in carico le segnalazioni di vulnerabilità e intervenire secondo i tempi e le disposizioni stabilite dalla norma e provvedere al rafforzamento delle misure di sicurezza dei dati attraverso la crittografia, secondo le linee guida e le indicazioni della stessa Agenzia, l'istituzione di un gruppo di lavoro interdirezionale per l'attuazione della normativa in materia di "cybersicurezza", con il coinvolgimento di tutte le Direzioni regionali, coordinato dal predetto Referente per la cybersicurezza**,** per la condivisione e il raccordo stabile rispetto alle funzioni specifiche in capo a tutte le strutture regionali, nonché le funzioni che necessitino di un coinvolgimento diretto delle strutture regionali.
Richiamata la DGR n. 10-9336 del 1° agosto 2008, ai sensi della quale, il gruppo di lavoro è

istituito dal Direttore regionale competente in materia di organizzazione per i casi in cui lo svolgimento delle attività interessi le attribuzioni di più direzioni.
Ritenuto, pertanto, di demandare al Direttore della Direzione della Giunta regionale l'istituzione del sopra riportato Gruppo di Lavoro.

Attestato che, ai sensi della DGR n. 8-8111 del 25 gennaio 2024 ed in esito all'istruttoria sopra richiamata, il presente provvedimento non comporta effetti contabili diretti né effetti prospettici sulla gestione finanziaria, economica e patrimoniale della Regione Piemonte, in quanto le disposizioni organizzative dal medesimo adottate sono ad invarianza di spesa.

Visti:
il decreto legislativo 7 marzo 2005 n. 82 - Codice dell'Amministrazione Digitale;
il decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali;
la legge 6 novembre 2012, n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione";
la deliberazione della Giunta regionale n. 4 – 8114 del 31 gennaio 2024 "Approvazione del Piano integrato di attività e organizzazione (PIAO) della Giunta regionale del Piemonte per gli anni 2024-2026 e della tabella di assegnazione dei pesi degli obiettivi dei Direttori del ruolo della Giunta regionale per l'anno 2024";
il regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR);
la legge 18 novembre 2019, n. 133 conversione in legge, con modificazioni, del Decreto legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica;
la legge regionale 28 luglio 2008, n. 23 "Disciplina dell'organizzazione degli uffici regionali e disposizioni concernenti la dirigenza ed il personale.

Attestata la regolarità amministrativa del presente provvedimento ai sensi della D.G.R. n. 8-8111 del 25 gennaio 2024.
La Giunta regionale per le motivazioni espresse in premessa, unanime,

delibera

di individuare, in ottemperanza all'articolo 8 della legge n. 90/2024, il Responsabile pro-tempore del Settore "Sistema Informativo regionale" della Direzione regionale Competitività del Sistema regionale, quale Referente regionale per la cybersicurezza, per la Giunta regionale e le sue strutture;

di demandare alla Direzione regionale Competitività del Sistema regionale la comunicazione all'Agenzia per la cybersicurezza nazionale relativa all'individuazione del Referente per la cybersicurezza, come previsto dell'articolo 8, comma 2, della legge n. 90/2024;

di disporre l'istituzione di un gruppo di lavoro interdirezionale per l'attuazione della normativa in materia di "cybersicurezza", con il coinvolgimento di tutte le Direzioni regionali, coordinato dal predetto Referente per la cybersicurezza, per la condivisione e il raccordo stabile rispetto alle funzioni specifiche in capo a tutte le strutture regionali, nonché le funzioni che necessitino di un coinvolgimento diretto delle strutture regionali;

di demandare, ai sensi della DGR n. 10-9336 del 1° agosto 2008 al Direttore della Direzione della Giunta regionale l'istituzione del sopra riportato Gruppo di Lavoro;
che il presente provvedimento non comporta effetti contabili diretti né effetti prospettici sulla

gestione finanziaria, economica e patrimoniale della Regione Piemonte, come in premessa attestato.

La presente deliberazione sarà pubblicata sul B.U. della Regione Piemonte ai sensi dell’art. 61 dello Statuto e dell’art. 5 della L.R. 22/2010.