DETERMINAZIONE n. 181 del 13 luglio 2023

OGGETTO: Costituzione del "Comitato di Crisi per la Continuità Operativa"

IL DIRETTORE GENERALE

Visto il D.P.R. 30 aprile 1970, n. 639;

Vista la Legge 9 marzo 1989, n. 88;

Visto il Decreto Legislativo del 30 giugno 1994, n. 479 e successive modifiche ed integrazioni;

Visto il D.P.R. 24 settembre 1997, n. 366;

Visto il decreto-legge 10 maggio 2023, n. 51 "*Disposizioni urgenti in materia di amministrazione di enti pubblici, di termini legislativi e di iniziative di solidarietà sociale*" e in particolare l'art. 1, comma 2, dello stesso;

Visto il Decreto del Ministro del lavoro e delle politiche sociali dell'11 febbraio 2022, con il quale il dott. Vincenzo Caridi è stato nominato Direttore generale dell'Istituto Nazionale della Previdenza Sociale;

Visto il Regolamento di Organizzazione dell'Istituto, adottato con deliberazione del Consiglio di Amministrazione n. 4 del 6 maggio 2020, successivamente modificato con deliberazione del Consiglio di Amministrazione n. 108 del 21 dicembre 2020;

Visto l'Ordinamento delle funzioni centrali e territoriali dell'INPS, adottato con deliberazione del Consiglio di Amministrazione n. 137 del 7 settembre 2022;

Visto il D.P.C.M. del 17 febbraio 2017 "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*";

Visto il D.P.C.M. del 31 marzo 2017 di adozione del "*Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali*";

Visto il D.Lgs. 18 maggio 2018, n. 65 di "*Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione"* il quale all'art. 12, tra l'altro, prevede che: "*Gli operatori di servizi essenziali adottano misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano nelle loro operazioni*";

Visto l'articolo 1, comma 1, del D.L. 21 settembre 2019, n. 105, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133, il quale prevede che "*Al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, è istituito il perimetro di sicurezza nazionale cibernetica*";

Visto l'art. 1, comma 2, lett. *a)*, del suindicato D.L. il quale prevede che, con il D.P.C.M. adottato su proposta del Comitato interministeriale per la cybersicurezza (CIC) "*sono definiti modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati di cui al comma 1 aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo*";

Visto il D.P.C.M. 30 luglio 2020, n. 131, di adozione del "*Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*";

Vista la nota n. 0187771 del 21 dicembre 2020, con cui la Presidenza del Consiglio dei Ministri – Dipartimento Informazioni per la Sicurezza – ha comunicato l'avvenuta iscrizione dell'INPS nell'elenco dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica;

Visto il D.P.R. 5 febbraio 2021, n. 54 che individua procedure, modalità e termini da seguire ai fini delle valutazioni da parte del CVCN in ordine all'acquisizione in fornitura, da parte dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, di beni, sistemi e servizi ICT rientranti nelle categorie individuate secondo i criteri stabiliti all'art. 13, comma 1;

Visto il D.P.C.M. 14 aprile 2021 n. 81 che individua le categorie di incidenti aventi impatto sui beni ICT e la tempistica della comunicazione al CSIRT;

Visto il D.L. 14 giugno 2021, n. 82, convertito con modificazioni dalla Legge 4 agosto 2021, n. 109, avente ad oggetto: "*Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*";

Vista la determinazione dell'Agenzia per l'Italia Digitale (AgID) n. 628/2021 del 15 dicembre 2021 - Adozione del "*Regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica*

amministrazione, le modalità di migrazione, nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione";

Viste le determinazioni n. 306/2022 e n. 307/2022 del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale (ACN);

Visto il Decreto Direttoriale n. 29 del 2 gennaio 2023 del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, d'intesa con il Dipartimento per la trasformazione digitale, che definisce il passaggio verso il nuovo sistema di qualificazione dei servizi cloud per la Pubblica Amministrazione, attualmente di competenza dell'Agenzia per la Cybersicurezza Nazionale che subentra all'AgID;

Visto il Decreto Direttoriale n. 5489 dell'8 febbraio 2023 del Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, che determina tempi e modi per la transizione delle infrastrutture e servizi digitali gestiti dalle Pubbliche Amministrazioni o dalle Società a controllo pubblico al nuovo quadro regolatorio relativo alla valutazione e verifica di rispondenza ai requisiti di qualità e sicurezza;

Vista la determinazione dell'Agenzia per la Cybersicurezza Nazionale del 3 gennaio 2023, pubblicata in Gazzetta Ufficiale n. 7 del 10 gennaio 2023, concernente la *"tassonomia degli incidenti che debbono essere oggetto di notifica"* con *"impatto su reti, sistemi informativi e servizi informatici diversi dai beni ICT di pertinenza dei soggetti inclusi nel perimetro, che i soggetti medesimi sono tenuti a notificare ai sensi dell'art. 1, comma 3-bis, del decreto-legge" n. 105 del 2019* convertito con modificazioni dalla Legge 18 novembre 2019, n. 133*";*

Vista la circolare dell'AgID n. 01 del 14 giugno 2019 avente ad oggetto "*Censimento del patrimonio ICT delle Pubbliche Amministrazioni e classificazione delle infrastrutture idonee all'uso da parte dei Poli Strategici Nazionali*";

Vista la comunicazione PEC del 10 febbraio 2020 con la quale AgID ha comunicato, a conclusione della procedura di Censimento del Patrimonio ICT delle PA, l'idoneità delle infrastrutture digitali dell'INPS per la candidatura quali Poli Strategici Nazionali a supporto degli Enti Pubblici per l'erogazione dei servizi digitali;

Considerato che l'allegato A alla predetta circolare AgID n. 01 del 14 giugno 2019, denominato "*Requisiti preliminari delle infrastrutture della PA per l'utilizzo da parte di un Polo Strategico Nazionale*", prevede, nell'ambito degli "Aspetti Organizzativi e Gestionali" - ID 3 - che "*L'Ente deve aver formalmente adottato procedure per la gestione della sicurezza IT, ad esempio ISO/IEC 27002 oppure essere certificate ISO/IEC 27001*";

Tenuto conto che INPS ha intrapreso il percorso di certificazione dei Sistemi di Gestione ottenendo la certificazione ISO 22301 in data 01/09/2022 con certificato n. 76326 e la certificazione ISO/IEC 20000-1 in data 01/09/2022 con certificato n. 76325;

Considerato che l'Istituto ha avviato il percorso per la certificazione dei Sistemi di Gestione quali – a titolo esemplificativo ma non esaustivo – ISO 9001 e ISO/IEC 22237;

Considerato che i diversi standard ISO prevedono requisiti specifici inerenti all'ambito dei ruoli e delle responsabilità, tali per cui l'alta direzione deve definire e comunicare i ruoli dell'organizzazione assegnando a ciascun ruolo responsabilità e poteri;

Visto il Codice dell'Amministrazione Digitale adottato con D.Lgs. 7 marzo 2005, n. 82, e successivamente modificato e integrato con i D.Lgs. 26 agosto 2016 n. 179, 13 dicembre 2017 n. 217, il D.L. n. 36/2022, convertito, con modificazioni, dalla Legge n. 79/2022 e da ultimo dal D.L. 24 febbraio 2023, n. 13, convertito, con modificazioni, dalla legge n. 41/2023;

Visto, in particolare, l'art. 50 del citato Codice, rubricato "*Disponibilità dei dati delle pubbliche amministrazioni*", il quale stabilisce che i dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati;

Visto, inoltre, l'art. 51, comma 1, del medesimo Codice, il quale prevede che con le regole tecniche contenute nelle Linee guida adottate da AgID "*sono individuate le soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture*";

Viste le "*Linee Guida per il Disaster Recovery delle Pubbliche amministrazioni*" adottate dall'AgID;

Visto il comma 2-*quater* dell'art. 51 del suindicato Codice, il quale stabilisce che: *"I soggetti di cui articolo 2, comma 2, predispongono, nel rispetto delle Linee guida adottate dall'AgID, piani di emergenza in grado di assicurare la continuità operativa delle operazioni indispensabili per i servizi erogati e il ritorno alla normale operatività"*;

Rilevato che le suddette Linee Guida di AgID prevedono, tra le Strutture per la gestione dell'emergenza, il "Comitato di Crisi" definendolo come: "*l'organismo di vertice a cui spettano le principali decisioni e la supervisione delle attività delle risorse coinvolte è l'organo di direzione strategica dell'intera struttura in occasione dell'apertura dello stato di emergenza ICT e, inoltre, condivide con il responsabile della Continuità Operativa (CO) la responsabilità di garanzia e controllo sulla continuità operativa di un Ente o Amministrazione*";

Considerato che la soluzione tecnologica di continuità operativa e *disaster recovery* dell'Istituto è costituita da n. 3 "Datacenter" di cui due allocati presso il Campus metropolitano di Roma e uno presso il Sito di DR di Casamassima di Bari;

Tenuto conto del punto 8.4 "*Piani e procedure per la Continuità Operativa*" dello standard ISO 22301 "*Sicurezza e resilienza – Sistemi di gestione per la continuità operativa - Requisiti*";

Ritenuto che la gestione della continuità operativa dei sistemi ICT rappresenta un impegno inderogabile per l'INPS che deve operare in modo da limitare al massimo gli effetti negativi di possibili fermi prolungati dei servizi che possano impattare la continuità operativa compromettendo la corretta erogazione di prestazioni e servizi a favore della collettività;

Ravvisata la necessità, pertanto, di procedere alla costituzione del "Comitato di Crisi per la Continuità Operativa" e all'individuazione dei suoi componenti;

Vista la relazione predisposta sull'argomento dalla competente Direzione centrale Tecnologia, Informatica e Innovazione;

DETERMINA

la costituzione del **Comitato di Crisi per la Continuità Operativa** presieduto dal Direttore Generale *pro-tempore* e composto dai titolari *pro-tempore* delle Direzioni Centrali di livello dirigenziale generale, dei Coordinamenti Generali nonché delle Direzioni Regionali di Puglia e Lazio e della Direzione di Coordinamento Metropolitano di Roma, dal Data Protection Officer, secondo il vigente Ordinamento delle Funzioni.

In considerazione delle peculiarità degli scenari da fronteggiare, il Comitato di crisi potrà anche essere costituito, in composizione ristretta, dal Direttore Generale *pro-tempore*, dal Direttore centrale Tecnologia, Informatica e Innovazione e dai suoi delegati, dai Direttori Centrali delle Direzioni centrali interessate dalla situazione emergenziale, dai Coordinamenti Generali nonché dai Direttori regionali Puglia e Lazio e del Coordinamento Metropolitano di Roma, dal Data Protection Officer, secondo il vigente Ordinamento delle Funzioni.

Il Comitato di Crisi per la Continuità Operativa svolge i compiti e le attività previste dalle "Linee Guida per il Disaster Recovery delle Pubbliche amministrazioni" adottate dall'AgID".

Vincenzo Caridi
Firmato digitalmente da
Vincenzo Caridi
C = IT
Data e ora della firma: 13/07/2023 18:00:03