Presidenza del Consiglio dei Ministri

PIANO NAZIONALE PER LA PROTEZIONE CIBERNETICA E LA SICUREZZA INFORMATICA

Dicembre 2013

Presidenza del Consiglio dei Ministri

PIANO NAZIONALE PER LA PROTEZIONE CIBERNETICA E LA SICUREZZA INFORMATICA

Dicembre 2013

INDICE

PREFAZIONE

Il presente Piano Nazionale individua gli indirizzi operativi, gli obiettivi da conseguire e le linee d'azione da porre in essere per dare concreta attuazione al Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico, in linea con quanto previsto dal Decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013 recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale".

Con questo ulteriore documento l'Italia si dota di una strategia organica, alla cui attuazione sono chiamati a concorrere non solo gli attori, pubblici e privati, richiamati nel Quadro Strategico Nazionale ma anche tutti coloro che, su base quotidiana, fanno uso delle moderne tecnologie informatiche, a partire dal singolo cittadino.

Tale strategia associa alla sua valenza organica un tratto di flessibilità, indispensabile a fronte delle rapide evoluzioni tecnologiche dello spazio cibernetico e delle relative sfide di sicurezza. La necessità, in sostanza, non è solo quella di essere "al passo con i tempi" ma anche di coglierne le "anticipazioni", così da prevenire le future minacce atte a minare lo sviluppo economico, sociale, scientifico e industriale, nonché la stabilità politico-militare del nostro Paese.

INTRODUZIONE

Nell'ambito del Quadro Strategico Nazionale (QSN), il presente Piano Nazionale per la protezione cibernetica e la sicurezza informatica nazionali (PN) mira a sviluppare, per il biennio 2014-2015, i sei indirizzi strategici ivi identificati. Al fine di dare concreta attuazione agli stessi, il Piano Nazionale dettaglia undici indirizzi operativi predefiniti nel Quadro Strategico, prevedendo obiettivi specifici e conseguenti linee d'azione, così come esplicitato all'articolo 3 comma 1 *lit.* b) del DPCM 24 gennaio 2013 Direttiva recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale".

QUADRO STRATEGICO NAZIONALE (QSN)

INDIRIZZI STRATEGICI

1. Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati
2. Potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese
3. Incentivazione della cooperazione tra istituzioni ed imprese nazionali
4. Promozione e diffusione della cultura della sicurezza cibernetica
5. Rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali *on-line*
6. Rafforzamento della cooperazione internazionale

Il Piano Nazionale stabilisce, dunque, la *roadmap* per l'adozione, da parte dei soggetti pubblici e privati di cui al citato DPCM, delle misure prioritarie per l'implementazione del Quadro Strategico, sulla base di un dialogo attivo e iterativo che vede nella protezione cibernetica e nella sicurezza informatica nazionali non solo un obiettivo ma, soprattutto, un processo che coinvolge tutti gli attori interessati, a vario titolo, alla tematica *cyber*.

La relazione tra il Quadro Strategico ed il Piano Nazionale è illustrata dalla seguente figura.

PIANO NAZIONALE (PN)

INDIRIZZI OPERATIVI

1. Potenziamento capacità di *intelligence*, di polizia e di difesa civile e militare
2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati
3. Promozione e diffusione della cultura della sicurezza informatica. Formazione e addestramento
4. Cooperazione internazionale ed esercitazioni
5. Operatività del CERT nazionale, del CERT-PA e dei CERT dicasteriali
6. Interventi legislativi e *compliance* con obblighi internazionali
7. *Compliance* a *standard* e protocolli di sicurezza
8. Supporto allo sviluppo industriale e tecnologico
9. Comunicazione strategica
10. Risorse
11. Implementazione di un sistema di *Information Risk Management* nazionale

La terminologia impiegata nel presente Piano Nazionale è conforme a quella adottata in ambito internazionale (ONU, NATO e UE) in materia, oltre che al Glossario *intelligence* pubblicato dal Dipartimento Informazioni per la Sicurezza (DIS).

Il Piano Nazionale è stato elaborato dal Tavolo Tecnico Cyber (TTC) che – istituito il 3 aprile 2013 in seno all'organismo collegiale permanente (c.d. CISR "tecnico") dopo l'entrata in vigore del DPCM 24 gennaio 2013 – opera presso il Dipartimento Informazioni per la Sicurezza. Ai lavori del TTC partecipano i punti di contatto *cyber* dei Dicasteri CISR (Affari Esteri, Interno, Difesa, Giustizia, Economia e Finanze, Sviluppo Economico) dell'Agenzia per l'Italia Digitale e del Nucleo per la Sicurezza Cibernetica (operante presso l'Ufficio del Consigliere Militare del Presidente del Consiglio).

Tale sinergia dovrà essere sviluppata anche con una molteplicità di altri attori istituzionali tra cui il Ministero delle Infrastrutture e dei Trasporti ed il Ministero dell'Istruzione, Università e Ricerca, oltre ad enti pubblici nazionali.

Il Piano Nazionale, inoltre, dovrà essere condiviso con *stakeholder* privati, che costituiscono attori rilevanti nell'ottica di una *partnership* pubblico-privato e, in quanto tali, rappresentano *conditio sine qua non* per lo sviluppo di un'efficiente capacità di sicurezza e difesa cibernetica nazionale.

L'attuazione delle linee d'azione indicate nel presente documento, il cui sviluppo va inteso in un'ottica incrementale, sarà misurata attraverso una apposita matrice elaborata dall'organismo collegiale permanente (c.d. "CISR Tecnico") idonea a consentire allo stesso organismo, ai sensi dell'articolo 5 comma 3 lit. c) del DPCM 24 gennaio 2013, lo svolgimento delle attività necessarie a "*verificare l'attuazione degli interventi previsti dal Piano Nazionale per la sicurezza dello spazio cibernetico e l'efficacia delle procedure di coordinamento tra i diversi soggetti, pubblici e privati, chiamati ad attuarli*".

INDIRIZZO OPERATIVO 1

POTENZIAMENTO DELLE CAPACITÀ DI *INTELLIGENCE*, DI POLIZIA E DI DIFESA CIVILE E MILITARE

La protezione cibernetica e la sicurezza informatica nazionali, per essere efficacemente perseguite, presuppongono, in prima istanza, un'approfondita conoscenza delle vulnerabilità – non solo del fattore tecnologico ma anche di quello umano – e delle minacce cibernetiche che le sfruttano, al fine rendere le reti e i sistemi, in particolare nel caso delle infrastrutture critiche, più resilienti, assicurando, al contempo, l'efficacia del contrasto.

1.1 ***Analisi delle minacce e delle vulnerabilità***	**a.** Analizzare e valutare le minacce cibernetiche e le vulnerabilità su base periodica **b.** Monitorare le innovazioni tecnologiche in tutti i settori correlati all'impiego di sistemi e piattaforme ICT (industriale, infrastrutture critiche, telemedicina, *automotive, social network, data center, cloud computing*, ecc.), al fine di individuare precocemente eventuali profili di vulnerabilità **c.** Condividere le valutazioni effettuate con tutti i responsabili di infrastrutture critiche attraverso apposite piattaforme istituzionali **d.** Collaborare con università e centri di ricerca, anche privati, per l'elaborazione di metodologie e tecnologie innovative per la rilevazione e l'analisi delle minacce e delle vulnerabilità

1.2	*Sviluppo delle capacità di raccolta, elaborazione e disseminazione delle informazioni (*cyber intelligence*), nonché della gestione della conoscenza che ne deriva (*knowledge management*)*	a. Potenziare le capacità di *cyber intelligence* b. Sviluppare capacità e procedure per il monitoraggio dei volumi di traffico e per la correlazione degli eventi ai fini della tempestiva rilevazione di anomalie associate a stati della minaccia c. Implementare procedure di *early warning* d. Sviluppare capacità informative integrate (interministeriali, *multi-sources*)
1.3	*Sviluppo delle capacità di contrasto alla minaccia cibernetica*	a. Migliorare le capacità di attribuzione di un attacco *cyber* b. *Cyber Situational Awareness* c. Favorire accordi per scambi informativi tra le Autorità competenti in materia ed il settore privato, secondo le modalità già previste dalla normativa vigente d. Potenziare le capacità di risposta ad incidenti informatici e di contrasto ad ogni forma di crimine informatico
1.4	*Sviluppo delle capacità operative fondamentali, secondo le Direttive della Difesa sull'ambiente cibernetico*	a. Implementare l'operatività delle strutture preposte alla difesa dello spazio cibernetico, predisponendo gli assetti, individuati dalle linee di comando, attraverso la preparazione, l'addestramento, la *leadership*, la protezione, il sostegno ed il dispiegamento degli stessi b. Sviluppare strutture di Comando e Controllo in grado di pianificare e condurre operazioni militari nello spazio cibernetico in maniera efficace, veloce e distribuita (Centro Operativo Cibernetico Interforze – COCI)

1.5	***Sviluppo delle capacità di analisi forense digitale***	**a.** Accrescere e diffondere le capacità di acquisizione dei dati con tecniche di *digital forensics* **b.** Incrementare le capacità di *live digital forensics* **c.** Potenziare le capacità di *data analysis* **d.** Sviluppare le capacità di analisi digitale *post-mortem*
1.6	***Processo delle lezioni apprese***	**a.** Creare un insieme di procedure e strumenti che permettano di registrare, analizzare, valorizzare e condividere le lezioni apprese nella gestione di incidenti informatici

INDIRIZZO OPERATIVO 2

POTENZIAMENTO DELL'ORGANIZZAZIONE E DELLE MODALITÀ DI COORDINAMENTO E DI INTERAZIONE A LIVELLO NAZIONALE TRA SOGGETTI PUBBLICI E PRIVATI

Tale indirizzo si pone l'obiettivo di potenziare il coordinamento e la cooperazione non solo tra i diversi soggetti pubblici, ma anche tra questi e i soggetti privati, considerato che questi ultimi gestiscono le infrastrutture critiche nazionali. Da qui discende l'esigenza di assicurare l'interoperabilità tra i vari attori, anche a livello internazionale.

2.1 ***Integrazione***	a. Sviluppare sistemi di collaborazione e di relazioni fiduciarie tra i settori pubblico e privato (inclusi i fornitori di servizi), anche per l'individuazione e la riduzione delle vulnerabilità b. Favorire l'attività di tavoli istituzionali, tavoli tecnici ed organismi competenti che prevedono la partecipazione di operatori di reti/fornitori di servizi di comunicazioni elettroniche, con particolare riguardo alla definizione di accordi e di procedure condivise per l'operatività del CERT nazionale c. Potenziare il sistema di *info-sharing*

2.2	*Infrastrutture*	a. Elaborare una metodologia per l'identificazione dei sistemi cibernetici e informatici che supportano funzioni critiche b. Sviluppare iniziative, soluzioni e prodotti per la gestione delle crisi a carattere cibernetico attraverso il contributo sinergico delle Autorità competenti in materia di protezione delle infrastrutture critiche, delle strutture dei diversi Dicasteri, del settore privato e di Paesi *partner*, per creare un sistema sicuro e resiliente c. Definire specifici *standard* di valutazione e *format* di comunicazione delle analisi interne relative alle infrastrutture gestite ed alle vulnerabilità individuate d. Elaborare strategie per la mitigazione delle vulnerabilità e. Stabilire i requisiti minimi di *cyber defence*, in termini sia strumentali che procedurali, per la protezione delle infrastrutture critiche
2.3	*Interoperabilità*	a. Assicurare l'interoperabilità organizzativa e semantica al fine di avere una comune descrizione e comprensione dei fenomeni e delle procedure per la protezione e la reazione, integrabili tra la Pubblica Amministrazione, il settore privato, la UE e la NATO

2.4	*Partecipazione degli operatori privati ad eventi di sicurezza cibernetica anche internazionali, a livello bilaterale e multilaterale*	a. Rafforzare gli specifici canali di dialogo e consultazione tra le istituzioni ed il settore privato, nell'ottica dell'approccio "Sistema Paese" b. Predisporre missioni congiunte di settore in contesti bilaterali e multilaterali c. Favorire la partecipazione del settore privato ad esercitazioni internazionali sulle tematiche della protezione delle infrastrutture critiche informatizzate
2.5	*Coordinamento nazionale dei lavori svolti dal Consiglio dell'Unione Europea relativi alla proposta di Direttiva in materia di sicurezza cibernetica*	a. Definire la posizione nazionale in merito alla proposta di Direttiva COM(2013) 48 finale del 7 febbraio 2013, sulla base dei contributi delle Istituzioni interessate

INDIRIZZO OPERATIVO 3

PROMOZIONE E DIFFUSIONE DELLA CULTURA DELLA SICUREZZA INFORMATICA. FORMAZIONE E ADDESTRAMENTO

La formazione e l'addestramento nel settore della sicurezza informatica sono stati, fino ad oggi, orientati prevalentemente al personale specialistico che opera o che è destinato ad operare nel settore. Si pone, pertanto, l'esigenza di un'attività di promozione della cultura della sicurezza informatica diretta ad un ampio pubblico, che includa privati cittadini e personale, sia delle imprese che della Pubblica Amministrazione.

3.1	***Sviluppo concetti e dottrina***	a. Analizzare l'evoluzione del quadro strategico internazionale, aggiornare i concetti e sviluppare le dottrine sulle attività cibernetiche anche attraverso l'individuazione delle *best practices* internazionali b. Migliorare la comprensione degli effetti della dissuasione e della deterrenza sul controllo della *escalation* di crisi nello spazio cibernetico in ambito nazionale, NATO e UE
3.2	***Promozione e diffusione della cultura della sicurezza informatica***	a. Organizzare mirate iniziative differenziate per cittadini, studenti, imprese e personale della Pubblica Amministrazione
3.3	***Educazione, formazione e addestramento***	a. Partecipare alle iniziative di sensibilizzazione coordinate dall'*European Union Agency for Network and Information Security* (ENISA) b. Sensibilizzare e formare i *decision makers* sugli effetti e sull'evoluzione della minaccia cibernetica

c. Formare ed addestrare il personale. Specifica formazione deve essere dedicata al personale assegnato alle operazioni cibernetiche ed a quello delle diverse Amministrazioni preposto alla messa in opera, gestione e protezione dei sistemi informatici
d. Sviluppare, sperimentare e validare attività operative nel *cyber*-spazio con l'ausilio di strumenti di simulazione, con addestramento collettivo e *training on the job*
e. Accentrare in un unico polo interforze in ambito Difesa le funzioni di formazione ed addestramento rendendo disponibile l'accesso al personale di altri Dicasteri, imprese pubbliche e private (nazionali e internazionali), dei membri della NATO e dell'UE e di Paesi *partner*
f. Organizzare, da parte della Scuola Superiore di Specializzazione in Telecomunicazioni (SSST), corsi specialistici, seminari e convegni, su materie che riguardano la sicurezza delle reti e delle informazioni con riferimento anche agli aspetti di certificazione della sicurezza informatica e all'analisi delle vulnerabilità
g. Sviluppare programmi di formazione specifici in cooperazione tra la Scuola Superiore della Magistratura e le Scuole di formazione del personale amministrativo e penitenziario
h. Sviluppare sinergie con enti universitari e di ricerca nella definizione di percorsi formativi *ad hoc* a favore di personale della Pubblica Amministrazione e delle imprese
i. Mappare i centri di eccellenza in materia

INDIRIZZO OPERATIVO 4

COOPERAZIONE INTERNAZIONALE ED ESERCITAZIONI

Il carattere per definizione transnazionale della minaccia cibernetica e la sua pervasività richiedono un approccio internazionale alla tematica, posto che i singoli Stati devono necessariamente agire sinergicamente per far fronte alla stessa. Ciò presuppone, necessariamente, un comune livello di preparazione e di interoperabilità.

4.1 ***Rafforzamento della cooperazione bilaterale e multilaterale***

a. Instaurare rapporti strutturati di cooperazione con i Paesi membri della NATO, della UE e con le nazioni *partner*
b. Assicurare la massima integrazione e interoperabilità dei processi di pianificazione e condotta delle operazioni cibernetiche attraverso attività congiunte a livello Difesa, interministeriale, NATO, UE e multinazionale
c. Garantire la massima integrazione e interoperabilità dei processi di gestione delle attività nel settore cibernetico ai fini della condivisione di informazioni e di iniziative congiunte a livello bilaterale, multilaterale e in seno ai principali consessi internazionali (UE, NATO e OCSE) anche sotto il profilo normativo e formativo
d. Partecipare ai consessi multilaterali (NATO, UE, ONU, OCSE, ecc.) al fine di garantire una visione integrale e assicurare la coerenza degli indirizzi nazionali in materia

		e. Supportare la piena partecipazione del sistema della giustizia italiana al tavolo della Giustizia Elettronica Europea (*European e-Justice*) ai fini dello sviluppo dei relativi sistemi informativi e la messa a disposizione dei conseguenti servizi, quando disponibili
4.2	***Esercitazioni***	a. Organizzare, su base periodica, esercitazioni nazionali di sicurezza informatica (*Cyber Italy*) b. Coordinare la partecipazione nazionale, nella componente pubblica e privata, alle esercitazioni pan-europee (*Cyber Europe*), con gli Stati Uniti (*Cyber Atlantic)* ed in ambito NATO (*Cyber Coalition*)
4.3	***Progetti comunitari***	a. Promuovere e diffondere, anche a beneficio del settore privato, l'informazione relativa alle iniziative ed alle modalità per la partecipazione ai fondi resi disponibili dall'Unione Europea b. Ottimizzare l'accesso ai fondi comunitari c. Partecipare a progetti finanziati dall'Unione Europea, tra cui quello denominato *Advanced Cyber Defence Centre* (ACDC)

INDIRIZZO OPERATIVO 5

OPERATIVITÀ DEL CERT NAZIONALE, DEL CERT-PA E DEI CERT DICASTERIALI

L'approntamento di capacità di prevenzione e reazione ad eventi cibernetici richiede lo sviluppo di Computer Emergency Response Team *(CERT) quali soggetti erogatori di servizi di assistenza tecnica, ricerca e sviluppo, formazione e informazione per i rispettivi utenti, pubblici e/o privati, operando sulla base di un approccio sia proattivo che reattivo.*

5.1	*Sviluppo del CERT-PA e dei CERT dicasteriali*	a. Integrare la struttura del CERT-SPC trasformandola nel CERT-PA, individuando le risorse umane necessarie ed attivando opportune procedure di reperimento del personale, nonché adeguando le infrastrutture tecniche, strumentali e logistiche, per garantire la sua piena operatività b. Stabilire il sistema di cooperazione delle strutture di gestione della sicurezza ICT della PA, in particolare Unità Locali di Sicurezza (ULS) e Security Operations Center (SOC), promuovendone, ove possibile, la trasformazione in CERT dicasteriali c. Favorire la creazione di CERT Regionali con il compito di supportare le Pubbliche Amministrazioni Locali (PAL) del territorio e di implementare regole e modelli organizzativi nazionali d. Adottare le procedure definite dall'Agenzia per l'Italia Digitale (AgID) e. Perseguire uniformi livelli di sicurezza dei *Data Center* e degli ambienti di lavoro delle Amministrazioni e dei gestori delle infrastrutture critiche nazionali
5.2	*Avvio del CERT nazionale*	a. Individuare le risorse umane e strumentali per l'operatività del CERT nazionale con attivazione di procedure di reperimento di personale nella Pubblica Amministrazione

		b. Definire accordi con istituzioni e settore privato per implementare forme di cooperazione e di scambi di informazioni, tramite specifiche audizioni c. Dare avvio ad una fase di sperimentazione ed ai servizi di base d. Adeguare le infrastrutture tecniche e logistiche del CERT nazionale per garantire la piena operatività dello stesso
5.3	*Sviluppo di una* Computer Incident Response Capability *(CIRC) nazionale integrata*	a. Perseguire il coinvolgimento e la cooperazione tra i CERT Dicasteriali ed il CERT-PA, al fine di mitigare gli effetti di possibili eventi cibernetici b. Fornire supporto ai CERT dicasteriali nella rapida ed efficace risoluzione delle problematiche derivanti da incidenti informatici c. Minimizzare l'impatto di incidenti informatici che hanno comportato la perdita o la sottrazione di informazioni (classificate e non) o la distruzione di sistemi e risorse di supporto informatico d. Sviluppare un approccio proattivo integrato al fine di limitare e ridurre i rischi per la sicurezza informatica che preveda l'adozione di un database integrato per la raccolta delle segnalazioni di incidente e delle contromisure intraprese; sistema integrato per la rilevazione degli allarmi, *online incident/intrusion detection, strong authentication,* ecc. e. Sviluppare un approccio reattivo integrato (concetto di resilienza), seguendo procedure testate, proiettate a garantire la disponibilità dei servizi erogati (*business continuity e disaster recovery*) f. Sviluppare capacità di *incident response* g. Sostenere le evoluzioni tecnico-funzionali e procedurali a similitudine e in armonia con il NATO *Computer Incident Response Capability – Technical Centre* (CIRC-TC)

INDIRIZZO OPERATIVO 6

INTERVENTI LEGISLATIVI E *COMPLIANCE* CON OBBLIGHI INTERNAZIONALI

La rapida evoluzione tecnologico-informatica comporta un'altrettanto veloce obsolescenza delle norme che disciplinano materie correlate alle tecnologie dell'informazione e della comunicazione. Pertanto, esse necessitano di periodiche revisioni e aggiornamenti, oltre che di integrazioni, anche per creare un substrato giuridico alle attività condotte ai fini della protezione cibernetica e della sicurezza informatica e per responsabilizzare gli amministratori e gli utenti delle operazioni da questi compiute sui sistemi loro assegnati.

6.1	***Revisione e consolidamento della legislazione in materia di sicurezza informatica***	a. Mettere a sistema conoscenze giuridiche specialistiche in materia di *cybersecurity*, presenti nelle strutture delle diverse Amministrazioni sia di *staff* che di *line* b. Valutare l'allineamento tra l'attuale assetto giuridico interno e le dinamiche di sviluppo legate all'innovazione tecnologica, esaminando l'eventualità di interventi normativi e tenendo conto delle *best practices* internazionali c. Finalizzare il quadro normativo relativo alle infrastrutture critiche nazionali informatizzate, pubbliche e private, volto alla definizione dei criteri per la loro individuazione d. Riformulare la normativa in materia di informatica giudiziaria

6.2	*Definizione di un quadro giuridico adeguato per supportare attività di sicurezza in materia* cyber *e, in particolare, operazioni cibernetiche*	a. Individuare, alla luce del contesto normativo internazionale di riferimento, la disciplina giuridica nazionale atta a regolamentare – in una logica di anticipazione dei presìdi – le attività di sicurezza in materia *cyber*, incluse le operazioni cibernetiche
6.3	*Attribuzione di responsabilità e sanzione delle violazioni*	a. Elaborare un quadro legale ed una metodologia di riferimento al fine di identificare gli strumenti tecnici, inclusi quelli relativi all'indirizzamento, necessari all'attribuzione di responsabilità in caso di violazioni di sicurezza (e delle relative sanzioni) da parte di amministratori ed utenti delle reti di interesse
6.4	*Proposte di attuazione della Direttiva del Parlamento Europeo e del Consiglio recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione*	a. Promuovere il confronto con Istituzioni e settore privato al fine di elaborare proposte per il recepimento della Direttiva in materia di *cyber security*, con particolare riguardo all'individuazione di misure tecnico-organizzative volte all'incremento della sicurezza nei settori individuati dalla medesima Direttiva

INDIRIZZO OPERATIVO 7

COMPLIANCE A *STANDARD* E PROTOCOLLI DI SICUREZZA

La compliance *a* standard *e protocolli di sicurezza, elaborati sia a livello nazionale che internazionale, consente di garantire un comune ed elevato livello qualitativo nell'assicurare la protezione cibernetica e la sicurezza informatica dei sistemi e delle reti.*

7.1	***Standardizzazione***	**a.** Aggiornare il quadro nazionale di riferimento agli *standard* e ai protocolli di sicurezza secondo le normative ratificate NATO e UE **b.** Adottare *standard* di riferimento per l'autenticazione ed autorizzazione degli accessi alle reti di interesse **c.** Elaborare indirizzi vincolanti ai fini dell'adozione dell'indirizzamento IPv6
7.2	***Documenti di riferimento***	**a.** Elaborare e pubblicare documenti di riferimento quali manuali, elenchi di procedure *standard* e raccomandazioni (*best practices* di settore), tassonomia e lessico uniforme da utilizzare per lo scambio di informazioni
7.3	***Revisione documenti di gestione***	**a.** Sottoporre a revisione ed aggiornamento periodico la documentazione (norme, procedure, ecc.) relativa alla gestione delle infrastrutture critiche

7.4	*Certificazioni e valutazioni di sicurezza*	a. Gestire lo Schema Nazionale di Certificazione della Sicurezza Informatica per Prodotti e Sistemi ICT commerciali (che trattano dati non classificati) attraverso l'Organismo di Certificazione della Sicurezza Informatica (OCSI), che opera in accordo con lo *standard* internazionale *Common Criteria* (ISO/IEC 15408) b. Mantenere aggiornato uno schema nazionale per la certificazione dei processi utilizzati dai sistemi informativi, in accordo con lo *standard* UNI ISO/IEC 27001:2006 c. Garantire l'operatività del CE.VA – Centro Valutazione – quale laboratorio di sicurezza informatica che opera nella valutazione tecnica di prodotti e sistemi ICT che trattano dati classificati d. Partecipare ai lavori degli organi di indirizzo degli accordi di mutuo riconoscimento internazionale nel settore delle certificazioni, segnatamente: il *Common Criteria Recognition Arrangement* (CCRA), che opera a livello mondiale, e il *Senior Official Group for Information Systems Security – Mutual Recognition Arrangement* (SOGIS – MRA), che opera a livello europeo
7.5	*Verifica delle misure di* cyber defence *applicate alle infrastrutture critiche*	a. Effettuare test periodici dei sistemi di protezione attraverso verifiche tecniche e procedurali b. Definire un sistema di verifica indipendente (es. *audit* esterno)
7.6	Compliance	a. Costituire un sistema per l'accreditamento e l'*auditing* degli Enti responsabili dell'emissione di certificati digitali di autenticazione

INDIRIZZO OPERATIVO 8

SUPPORTO ALLO SVILUPPO INDUSTRIALE E TECNOLOGICO

La garanzia dell'affidabilità e della sicurezza di componenti hardware *e* software *prodotte nell'Unione Europea e nei Paesi terzi, specie di quelle impiegate da infrastrutture critiche e da soggetti che svolgono attività di rilevanza strategica per il Paese, rappresenta un obiettivo conseguibile solo se tutti gli attori della catena del valore (produttori di componenti* hardware*, sviluppatori di* software*, fornitori di servizi della società dell'informazione) faranno della sicurezza una priorità.*

8.1 ***Logistica***	**a.** Garantire una catena di approvvigionamento di componenti sicure e resilienti dal punto di vista della sicurezza cibernetica, supportata da un processo flessibile e veloce di validazione, verifica e certificazione **b.** Promuovere l'innovazione ICT per lo sviluppo di un adeguato tessuto industriale competitivo nel panorama internazionale, favorendo la costituzione di *supply-chain* verticali a livello nazionale e comunitario **c.** Potenziare programmi di cooperazione multilaterali e bilaterali per favorire le funzioni di ricerca e sviluppo nazionali nel contesto europeo ed internazionale
8.2 ***Implementazione di un laboratorio governativo di analisi comparativa***	**a.** Favorire la costituzione di un laboratorio governativo di verifica che sottoponga ad analisi comparativa i sistemi ICT di interesse delle Amministrazioni e delle Infrastrutture Critiche di interesse nazionale

INDIRIZZO OPERATIVO 9

COMUNICAZIONE STRATEGICA

La comunicazione circa un evento cibernetico occorso e le relative conseguenze assume un'importanza strategica, in quanto le singole Amministrazioni interessate devono essere in grado di fornire un'informazione completa, corretta, veritiera e trasparente, senza con ciò creare inutili allarmismi che verrebbero ad amplificare l'impatto economico e sociale dell'evento stesso.

9.1	***Comunicazione strategica***	a. Sviluppare una *Situation Awareness* dei contenuti e delle informazioni, allo scopo di rendere efficaci i flussi comunicativi b. Stabilire un protocollo di comunicazione pubblica volto a dare un corretto e trasparente inquadramento degli eventi cibernetici (di natura sia volontaria od accidentale), anche in funzione delle relative azioni di risposta e ripristino

INDIRIZZO OPERATIVO 10

RISORSE

Punto di partenza per un'oculata pianificazione finanziaria e per la ripartizione delle risorse è l'analisi dei costi di eventi cibernetici occorsi o potenziali, in quanto la rilevanza del rischio è direttamente proporzionale alla probabilità ed all'entità del danno. Parimenti, l'opportunità e la priorità d'intervento su una specifica vulnerabilità potrebbero essere meglio supportate a livello decisionale qualora corredate degli opportuni elementi di valutazione economica. Quest'ultima potrebbe meglio bilanciare l'analisi dei costi correlata alle esigenze di investimento nel settore pubblico quanto in quello privato.

10.1	***Pianificazione finanziaria e aspetti economici***	**a.** Definire le priorità e i costi associati alle misure di *cyber-security* e di *cyber-defence* per la protezione delle infrastrutture critiche e per lo sviluppo delle capacità operative fondamentali, sia per le componenti materiali e strumentali che per quelle relative al personale
10.2	***Misurazione dei costi riconducibili ad eventi di natura cibernetica***	**a.** Determinare metriche per la valutazione dell'entità del danno economico diretto ed indiretto di eventi cibernetici accaduti o potenziali (attività di *detect, remediation*, danno di immagine, perdita di clienti/credibilità/affidabilità/competitività, costi dei disservizi, eventuali perdite umane, ecc.) **b.** Analizzare le interdipendenze tra infrastrutture critiche/strategiche anche ai fini della valutazione puntuale del danno economico complessivo derivante da un eventuale "effetto domino" **c.** Effettuare una mappatura economica degli incidenti ed un'analisi di scenari potenziali

10.3	*Efficientamento della spesa*	a. Definire strumenti normativi e finanziari per l'ottimizzazione e l'eventuale condivisione delle spese, collegati a misure di *cyber defence* tra Dicasteri, tra comparto pubblico e privato, ed eventualmente tra Paesi per programmi di cooperazione internazionale
10.4	*Personale*	a. Agevolare la condivisione interministeriale al fine di favorire approcci integrati per il reclutamento di personale specializzato, tenendo anche conto delle *best practices* internazionali

INDIRIZZO OPERATIVO 11

IMPLEMENTAZIONE DI UN SISTEMA DI *INFORMATION RISK MANAGEMENT* NAZIONALE

La protezione dei dati da minacce che ne pregiudicano l'autenticità, l'integrità, la riservatezza e la disponibilità è parte integrante del presente Piano Nazionale in quanto le informazioni costituiscono un valore intrinseco all'organizzazione, pubblica o privata, e imprescindibile obiettivo di ogni attacco cibernetico.

11.1	***Metodologia***	**a.** Individuare una metodologia di *Information Risk Management* univoca e condivisa a livello strategico, adottando un modello per le infrastrutture critiche nazionali informatizzate, in accordo con la UNI EN ISO 27005:2011 **b.** Coinvolgere centri di ricerca e università per consentire l'adozione di aggiornati strumenti di gestione del rischio

Il Presidente del Consiglio dei Ministri

N.0012959/2.1.1.(36) GAB.UGLG
del 30/01/2014 D002 I

VISTA la legge 3 agosto 2007, n. 124, recante "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto", come modificata e integrata dalla legge 7 agosto 2012, n. 133, e, in particolare, l'art. 1, comma 3-*bis*;

VISTO il decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013, recante "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale" e, in particolare, gli artt. 3 e 4;

VISTA la deliberazione del Comitato interministeriale per la sicurezza della Repubblica assunta nella seduta del 17 dicembre 2013;

DISPONE

Articolo 1

1. È adottato il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali, di cui all'art. 3, comma 1, lett. *b*), della Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, allegato al presente decreto.

Roma, 27 GEN. 2014

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
SEGRETARIATO GENERALE
UFFICIO DEL BILANCIO E PER IL RISCONTRO
DI REGOLARITA' AMMINISTRATIVO-CONTABILE
VISTO E ANNOTATO AL N. 232/2014
Roma, 4.2.2014
IL REVISORE
IL DIRIGENTE

Reg.to ALLA CORTE DEI CONTI
Addì 7 FEB. 2014
Fg. 317