Presidenza del Consiglio dei Ministri

PIANO NAZIONALE PER LA PROTEZIONE CIBERNETICA E LA SICUREZZA INFORMATICA

Marzo 2017

PIANO NAZIONALE
PER LA PROTEZIONE CIBERNETICA
E LA SICUREZZA INFORMATICA

Marzo 2017

INDICE

PREFAZIONE

Il presente Piano Nazionale, in linea di continuità con quello relativo al biennio 2014-2015 e alla luce dell'esperienza maturata nel corso dello stesso, 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 (QSN), alla luce degli indirizzi per la protezione cibernetica e la sicurezza informatica indicati dal Presidente del Consiglio dei Ministri nella sua qualità di Organo di vertice dell'architettura nazionale cyber.

Traendo spunto dalle riflessioni svolte in occasione delle attività di verifica dell'attuazione del precedente Piano Nazionale, sono state elaborate alcune misure di revisione del Decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013 – che ha finora costituito la cornice giuridica dell'architettura cibernetica del Paese – recepite nell'ambito del DPCM del 17 febbraio 2017 e delle quali il presente Piano tiene già conto.

L'attività di revisione – condotta congiuntamente dalle Amministrazioni che compongono l'architettura nazionale cyber – ha fatto tesoro sia dell'esperienza maturata nella fase di prima implementazione dell'architettura nazionale, sia delle scelte operate nel settore dai Paesi tecnologicamente più avanzati. Gli esiti di tali esercizi hanno consentito di affinare le riflessioni rispetto al contesto nazionale al fine di superare le criticità riscontrate e di rendere più agevole il compito degli attori, pubblici e privati, chiamati a concorrere all'attuazione del presente Piano Nazionale.

INTRODUZIONE

Il presente Piano Nazionale per la protezione cibernetica e la sicurezza informatica nazionali (PN) mira a sviluppare gli indirizzi individuati dal Quadro Strategico Nazionale (QSN).

Esso non costituisce un mero aggiornamento del precedente Piano, ma si pone l'obiettivo di imprimere un immediato impulso all'ulteriore fase di sviluppo dell'architettura nazionale *cyber*.

In continuità con l'attività svolta nel biennio 2014-2015, il Piano prevede undici indirizzi operativi (IIOO), con obiettivi specifici e conseguenti linee d'azione, così come esplicitato all'articolo 3, comma 1, *lit*. c), del Decreto del

QUADRO STRATEGICO NAZIONALE (QSN)

Indirizzi strategici

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

Presidente del Consiglio dei Ministri 17 febbraio 2017, recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale". Il Piano Nazionale stabilisce, dunque, la *roadmap* per l'adozione, da parte dei soggetti pubblici e privati di cui alla citata Direttiva, 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 terminologia impiegata nel presente Piano Nazionale è conforme a quella adottata in ambito internazionale (ONU, NATO e UE) in materia, oltre che al glossario, denominato "le parole del *cyber*", presente in calce al Documento di sicurezza nazionale, annesso quest'ultimo alla relazione annuale al Parlamento ed aggiornato annualmente ai sensi dell'art. 38, co. 1-*bis*, della legge 124/2007.

Il Piano Nazionale è stato rivisitato dai 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 all'epoca presso l'Ufficio del Consigliere Militare del Presidente del Consiglio).

Le **principali direttrici dell'intervento di revisione** hanno interessato:

- l'indirizzo operativo 5 (Operatività delle strutture nazionali di *incident prevention*, *response* e *remediation*), in cui sono state considerate le esigenze di potenziamento degli attuali CERT, la necessità di costituire le strutture previste dalla Direttiva NIS (CSIRT, punto

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 ed addestramento
4. Cooperazione internazionale ed esercitazioni
5. Operatività delle strutture nazionali di *incident prevention*, *response* e *remediation*
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 e operativa
10. Risorse
11. Implementazione di un sistema di *cyber risk management* nazionale

unico di contatto nazionale, Autorità nazionale) e le modalità di coordinamento tra i vari attori – attuali e futuri – dell'architettura (CERT e CSIRT, Comparto, CNAIPIC, Difesa, AgID, ecc.), in una prospettiva di progressiva unificazione dei CERT pubblici;

- l'indirizzo operativo 1 (Potenziamento delle capacità di intelligence, di polizia e di difesa civile e militare), che è stato allineato rispetto all'esperienza operativa maturata nell'ultimo biennio al fine di potenziare le capacità complessive di risposta integrata ad eventi cibernetici.

L'attuazione delle linee d'azione indicate nel presente documento, il cui sviluppo va inteso in un'ottica incrementale, sarà misurata attraverso modalità idonee a consentire, ai sensi dell'articolo 5 comma 3 *lit.* c) della citata Direttiva presidenziale, 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*".

Da ultimo, l'esigenza di consentire un rapido ed efficace salto di qualità dell'architettura nazionale *cyber* ha reso necessario individuare un nucleo essenziale di iniziative, cui attribuire carattere di priorità ed urgenza, selezionate sulla base delle esigenze che hanno informato l'attività di revisione del QSN e del PN e a motivo dell'evoluzione del quadro normativo interno ed internazionale, cui è dedicato uno specifico piano d'azione, i cui elementi essenziali sono sintetizzati nella figura sottostante.

PIANO D'AZIONE

- Revisione del Nucleo per la Sicurezza Cibernetica
- Contrazione della catena di comando per la gestione delle crisi cibernetiche
- Riduzione della complessità dell'architettura nazionale, mediante soppressione/accorpamento di organi
- Progressiva unificazione dei CERT
- Istituzione di un centro di valutazione e certificazione nazionale ICT
- Fondazione o Fondo di *venture capital*
- Istituzione di un Centro nazionale di ricerca e sviluppo in *cybersecurity*
- Costituzione di un Centro nazionale di crittografia

PIANO D'AZIONE
MISURE DI POTENZIAMENTO DELLA ARCHITETTURA NAZIONALE CIBERNETICA

Il presente piano d'azione raccoglie le iniziative individuate per garantire il necessario ed effettivo cambio di passo in termini di innalzamento dei livelli di sicurezza dei sistemi e delle reti del nostro Paese, cui la recente approvazione del citato DPCM 17 febbraio 2017 intende fornire un deciso impulso.

Nonostante le iniziative assunte nel corso del biennio 2014-2015, hanno continuato a persistere differenti livelli di efficacia delle misure di protezione di reti e sistemi, che si osservano sia orizzontalmente, tra realtà pubblica e privata, sia verticalmente, all'interno degli stessi ambiti.

Occorre, inoltre, considerate che il patrimonio informativo sensibile ai fini della sicurezza nazionale non è pertinenza esclusiva del settore pubblico, ma è integrato anche da quegli *asset* detenuti da taluni soggetti privati operanti in settori strategici.

Ciò rende necessario un approccio di sistema che consenta un'armonica implementazione di *standard* minimi di sicurezza comuni, specie per i sistemi critici e strategici del Paese.

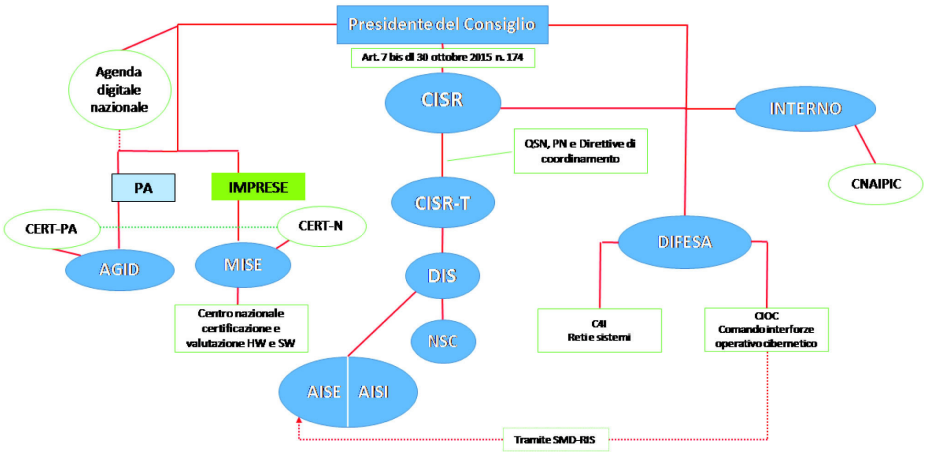
Sono queste, in sostanza, le riflessioni che hanno ispirato il nucleo delle iniziative inserite nel presente piano d'azione, che assumono valenza sistemica in quanto:

- fanno leva sulle competenze e sulle responsabilità dei diversi attori (pubblico, privato, ricerca) che costituiscono la struttura portante del tessuto *cyber* nazionale;
- riguardano le più significative attività di approntamento del sistema di difesa cibernetica, tra cui il perimetro di copertura degli assetti di difesa comuni (CERT), la certificazione di soluzioni SW/HW, l'identificazione delle funzioni manageriali/ professionali critiche, l'obbligo di condivisione degli eventi cibernetici significativi (al superamento di determinate soglie di gravità), etc.

Nelle more delle misure legislative che saranno adottate in occasione del recepimento della direttiva *Network and Information Systems* (NIS) della UE, è stata operata una razionalizzazione dell'architettura delineata nel 2013 improntata, ad invarianza del quadro normativo primario vigente, alla:

- semplificazione delle procedure ordinarie e straordinarie di gestione delle attività di mantenimento e di implementazione dell'architettura nazionale (*vds*. IIOO 1, 2 e 5);
- rimodulazione degli Organi che fanno parte del sistema di protezione cibernetica nazionale (soppressione nel NISP "*cyber*", revisione del ruolo del NSC, etc.) (*vds*. IO 1);
- complessiva contrazione della "catena di comando" deputata alla gestione delle crisi, al fine di rendere tempestiva ed efficace l'azione degli organi

ARCHITETTURA NAZIONALE *CYBER*



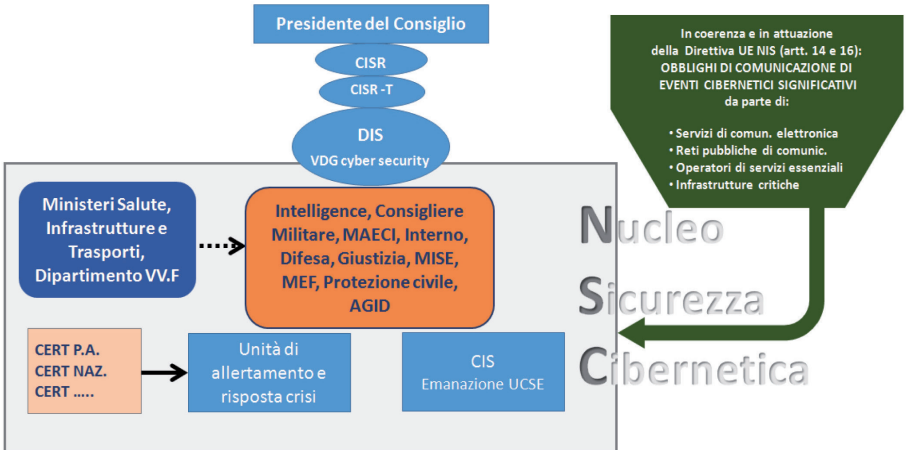
chiamati a svolgere compiti di *response* e *remediation* in caso di eventi cibernetici di rilievo (*vds*. IO 5).

In particolare, in base al piano d'azione attuativo del presente PN:

- sarà attribuito al Direttore Generale del DIS un ruolo attivo e centrale nell'ambito degli organi deputati alla gestione ordinaria e straordinaria della sicurezza cibernetica nazionale;
- sarà ridotta la complessità dell'architettura con l'abolizione del NISP "*cyber*" e il riposizionamento presso il DIS del NSC, organo, quest'ultimo, cui sarà demandato il coordinamento della gestione delle crisi cibernetiche e che sarà guidato da un Vice Direttore Generale del medesimo Dipartimento;
- sarà garantita una stretta ed efficace interazione dei due CERT (Nazionale e della Pubblica Amministrazione), così da consentire il necessario allineamento operativo degli stessi, rivedendo regole e responsabilità per la PA (Agenda digitale e AgID) ed i privati (MiSE), al fine di assicurare una capacità unitaria di rilevazione, allarme e prima analisi degli incidenti cibernetici (*vds*. IIOO 5, 6 e 7);

- sarà istituito, presso il MiSE, un centro di valutazione e certificazione nazionale per la verifica dell'affidabilità della componentistica ICT destinata ad infrastrutture critiche e strategiche (*vds*. IO 7);
- sarà ampliato e definito il perimetro dei soggetti che operano nei settori d'interesse per la sicurezza nazionale (operatori di servizi essenziali e fornitori di servizi digitali), per i quali sarà previsto un obbligo di notifica – al superamento di determinate soglie di gravità – degli incidenti informatici

NUOVO SISTEMA DI GESTIONE DELLE CRISI



di rilievo, con conseguenti sanzioni in caso di omissioni (*vds*. IIOO 2, 5 e 6).

Un effettivo cambio di passo nel settore in parola non può prescindere dal contributo delle varie componenti pubbliche, private e della ricerca, che costituiscono la struttura portante del tessuto *cyber* nazionale. Motivo, questo, per il quale è necessario lo sviluppo di iniziative che coinvolgano le principali imprese nazionali impegnate nel settore, il tessuto accademico e la ricerca scientifica (*vds*. IO 8).

A tal fine, la componente legata al mondo accademico e della ricerca dovrà trovare adeguato impulso attraverso l'avvio di iniziative volte – anche mediante l'eventuale costituzione di un soggetto giuridico dedicato (es. fondazione) – a realizzare (*vds*. IIOO 2, 6 e 7):

- il finanziamento di *start-up* e/o la partecipazione al capitale societario di realtà imprenditoriali d'interesse (*venture capital*);
- un "Centro nazionale di Ricerca e Sviluppo in *Cybersecurity*", il cui ambito di azione potrebbe dispiegarsi, tra l'altro, nei settori della *malware analysis*, della *security governance*, della protezione delle infrastrutture critiche e della *threat analysis systems*, etc.;

- un "Centro nazionale di crittografia", impegnato nella progettazione di cifrari, nella realizzazione di un algoritmo e di una *blockchain* nazionali e in valutazioni di sicurezza.

Nel quadro di un intervento di sistema, coerente e definito, occorre poi fare leva sulle competenze e sulle responsabilità degli attori pubblici titolari di competenze primarie a livello nazionale nel settore *cyber*.

In tale contesto, il rinnovato NSC, potenziato e collocato al centro dell'architettura, mira a semplificarne la *governance*, attraverso l'accorciamento della catena decisionale e la razionalizzazione dei processi di lavoro, sia di carattere ordinario, sia per la risposta emergenziale ad eventi cibernetici, ponendosi altresì quale fulcro della cooperazione tra le amministrazioni che compongono lo stesso Nucleo.

In tale ambito, il Ministero dell'Interno riveste un ruolo centrale per la protezione delle infrastrutture critiche informatizzate (in particolare attraverso il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – CNAIPIC), grazie alle sue specifiche competenze investigative e forensi.

Altrettanto rilevanti sono le funzioni di AgID, chiamata a dettare indirizzi, regole tecniche e linee guida in materia di sicurezza informatica e di omogeneità degli *standard*, ad assicurare la qualità tecnica e la sicurezza dei sistemi informativi pubblici e della loro rete di interconnessione e a monitorare i piani ICT delle amministrazioni pubbliche.

Da ultimo, le capacità cibernetiche che l'Amministrazione della Difesa ha sviluppato a protezione delle proprie reti in territorio nazionale e in teatro operativo costituiscono una risorsa utile ai fini del potenziamento del NSC e, per il suo tramite, dell'intero Sistema-Paese.

Nell'ambito della cornice sopra delineata, si prevede anche un supporto alle iniziative del Ministero della Difesa volte a:

- istituire un Comando Interforze Operazioni Cibernetiche (CIOC), deputato alla protezione dei sistemi e delle reti di quel Dicastero nonché all'effettuazione delle operazioni in campo cibernetico;
- realizzare, presso la Scuola Telecomunicazioni delle Forze Armate di Chiavari (GE), un poligono virtuale nazionale.

Da collegare a tali iniziative, infine, la definizione, all'esito di articolate interlocuzioni, di un apposito protocollo d'intesa attraverso il quale il Comparto *intelligence* e lo Stato Maggiore della Difesa hanno elaborato un quadro strategico e tattico allineato, tale da permettere il miglior posizionamento del costituendo CIOC con riguardo all'operatività nel dominio digitale anche alla luce dell'esperienze in corso di sedimentazione nell'Alleanza Atlantica.

La visione sistematica che informa il presente piano d'azione è volta ad assicurare la messa in sicurezza degli assetti nazionali secondo una progressione dettata da una scala di criticità:

- *1° livello* – sicurezza nazionale dello Stato [Comparto *Intelligence*, Difesa, Interno, altre amministrazioni CISR];
- *2° livello* – le infrastrutture critiche nazionali [TLC, *utilities*, settore finanziario, trasporto] altre amministrazioni pubbliche sensibili [Sanità, etc.];
- *3° livello* – tessuto produttivo nazionale, cittadinanza.

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 in modo continuativo le minacce cibernetiche e le vulnerabilità b. Monitorare le innovazioni tecnologiche che hanno impatto su tutti i settori strategici e le infrastrutture critiche, correlati all'impiego di sistemi e piattaforme ICT, al fine di individuare precocemente eventuali profili di vulnerabilità c. Condividere le valutazioni effettuate con tutti i gestori di servizi essenziali e 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 l'analisi di contesto 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. Sviluppare un'adeguata *Cyber Situational Awareness*, che incentivi la conoscenza e la comprensione della situazione corrente, attraverso valutazioni puntuali, pertinenti ed accurate delle attività che si svolgono nello spazio cibernetico, al fine di facilitare l'opera di prevenzione e di contrasto della minaccia c. Favorire accordi per scambi informativi tra le Autorità competenti in materia ed il settore privato d. Potenziare le capacità di risposta integrata, secondo protocolli e regole d'ingaggio prestabiliti, ad incidenti informatici e di contrasto ad ogni forma di crimine informatico, adeguando il quadro normativo alla possibilità di creare *pool* d'intervento tecnici in supporto, in caso di gravi eventi cibernetici, alle amministrazioni centrali e ai gestori di servizi essenziali e di infrastrutture critiche (OS 5.1.c)

1.4	***Sviluppo delle capacità operative fondamentali, idonee ad espletare i compiti della Difesa nell'ambiente cibernetico***	a. Potenziare le strutture preposte alla difesa dello spazio cibernetico ed avere cura che gli assetti che le compongono raggiungano e mantengano nel tempo i necessari livelli di efficacia ed efficienza b. Sviluppare strutture di Comando e Controllo in grado di pianificare e condurre operazioni militari nello spazio cibernetico in maniera efficace
1.5	***Processo delle lezioni apprese***	a. Creare un insieme di procedure e strumenti che permettano, possibilmente in modo automatizzato, di registrare, analizzare, valorizzare e condividere le lezioni apprese nella gestione di incidenti informatici tra tutti i vari attori, anche privati, in funzione del *need to know* e del *need to share*

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. Favorire l'operatività dei già esistenti sistemi di collaborazione e di relazioni fiduciarie tra settore pubblico e privato, per l'individuazione precoce delle minacce, la riduzione delle vulnerabilità e per la risposta coordinata ad attacchi informatici b. Favorire l'attività di tavoli istituzionali, tavoli tecnici ed organismi competenti che prevedono la partecipazione di gestori di servizi essenziali, di operatori di infrastrutture critiche informatizzate nazionali ed altri soggetti rilevanti nei settori strategici e dell'ICT

2.2	*Strumenti di cooperazione tra il settore Pubblico ed il settore Privato*	a. Elaborare una metodologia per l'identificazione dei sistemi cibernetici e informatici che supportano funzioni critiche, anche in relazione all'erogazione di servizi essenziali b. Potenziare il sistema di *info-sharing*, anche attraverso l'adozione di linguaggi strutturati e comuni c. 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 dei Paesi *partner*, per creare un sistema sicuro e resiliente d. Definire specifici *standard* di valutazione e *format* di comunicazione delle analisi interne relative alle infrastrutture gestite ed alle vulnerabilità individuate
2.3	*Partecipazione degli operatori privati ad eventi di sicurezza cibernetica anche internazionali, a livello bilaterale e multilaterale*	a. Consolidare gli specifici canali di dialogo e consultazione tra le istituzioni ed il settore privato, nell'ottica dell'approccio "Sistema Paese" b. Favorire la partecipazione del settore privato ad esercitazioni internazionali sulle tematiche della protezione delle infrastrutture critiche informatizzate

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
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'UE, dalla NATO ed altre Organizzazioni Internazionali **b.** Sensibilizzare e formare i *decision makers* sugli effetti e sull'evoluzione della minaccia cibernetica

c. Formare e addestrare il personale, con un *focus* specifico sulla tematica della *cyber security* per quello assegnato alle operazioni cibernetiche e quello 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. Concentrare in poli d'eccellenza, valorizzando quelli esistenti, le funzioni di formazione ed addestramento nel settore pubblico, rendendo disponibile l'accesso anche al personale di imprese pubbliche e private (nazionali ed internazionali), dei membri della NATO e dell'UE e di Paesi *partner*
f. 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
g. 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. Partecipare ai consessi multilaterali al fine di garantire una visione integrale e assicurare la coerenza degli indirizzi nazionali in materia
4.2	***Esercitazioni***	a. Organizzare, su base periodica, esercitazioni nazionali di sicurezza informatica (es. *Cyber Italy*), stimolando la partecipazione dei principali operatori di servizi essenziali e dei gestori di infrastrutture critiche e/o i settori strategici nazionali

		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 dell'Unione Europea e di organizzazioni internazionali***	a. Promuovere e diffondere, anche a beneficio del settore privato, l'informazione relativa alle iniziative ed alle modalità di partecipazione ai fondi resi disponibili dall'Unione Europea b. Ottimizzare l'accesso ai fondi dell'Unione Europea c. Partecipare a progetti finanziati dall'Unione Europea d. Partecipare a progetti NATO e di altre organizzazioni internazionali

INDIRIZZO OPERATIVO 5

OPERATIVITÀ DELLE STRUTTURE NAZIONALI DI *INCIDENT PREVENTION*, *RESPONSE* E *REMEDIATION*

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. La Direttiva NIS prevede, quantomeno a favore dei gestori di servizi essenziali, la costituzione dei Computer Security Incident Response Team (CSIRT), una nuova tipologia di organismo intesa quale evoluzione dei CERT in grado di assicurare una effettiva capacità di assistenza e supporto attivo alla propria constituency in caso di evento cibernetico. Nel contesto del recepimento delle novità introdotte dalla Direttiva NIS, occorre ridefinire il ruolo rivestito dagli attori presenti nell'attuale architettura nazionale (i vari CERT) e quelli che vi faranno ingresso (oltre a CSIRT, Autorità nazionale/i e punto unico di contatto). Nelle more del recepimento della direttiva NIS, sarà avviato un processo di progressiva unificazione dei CERT pubblici per sancire, nei settori di interesse strategico, la competenza esclusiva di un CERT nazionale unico, ovvero per creare una rete nazionale di CERT individuando un soggetto con poteri di coordinamento.

5.1 ***Sviluppo di una capacità nazionale integrata di incident prevention, response e remediation***

- **a.** Istituire un punto unico di contatto e uno o più CSIRT dotati di adeguate capacità di *incident response* (Direttiva NIS)
- **b.** Rendere operativa una (o più) Autorità nazionale (Direttiva NIS)
- **c.** Implementare il quadro normativo di riferimento per le strutture di sicurezza cibernetica, in particolare CSIRT/CERT, SOC, ULS e pool d'intervento tecnico (OS 1.3.d)

	d. Adeguare il ruolo delle attuali strutture tecnico-operative nazionali di sicurezza cibernetica (CERT-N, CERT-PA, CERT-Difesa, CNAIPIC, Comparto intelligence, ecc.), anche alla luce dei nuovi attori e delle nuove disposizioni della Direttiva NIS, definendo chiaramente i rapporti intercorrenti tra di esse ed individuando il relativo modello di cooperazione e. Sviluppare un modello standardizzato di gestione degli eventi cibernetici, in particolare per la fase di *triage*, con specifica attenzione alle esigenze di automazione delle attività f. 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. g. 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. h. Sviluppare un approccio reattivo integrato (concetto di resilienza), seguendo procedure testate, proiettate a garantire la disponibilità dei servizi erogati (*business continuity* e *disaster recovery*)
5.2 ***Sviluppo dei CERT***	a. Sviluppo delle infrastrutture e dei servizi dei CERT, prevedendo l'eventuale adeguamento dei rispettivi compiti e dotazioni alla luce delle modalità con le quali sarà implementa l'architettura nazionale al fine di recepire la Direttiva NIS (Autorità nazionale, CSIRT, ecc.).

		b. Incrementare l'efficacia dell'azione dei CERT verso le rispettive *constituency*, con particolare riferimento, per il CERT-N, al sistema delle imprese, incluse le PMI, e, per il CERT-PA, allo sviluppo di livelli superiori di accreditamento da parte delle pubbliche amministrazioni c. Valutare le modalità più opportune per supportare le Pubbliche Amministrazioni Locali (PAL) nell'adozione di regole e modelli organizzativi nazionali d. Rafforzare la cooperazione con i CERT a livello internazionale ed europeo, anche attraverso la partecipazione alla rete dei CSIRTs, di cui alla direttiva NIS, e la partecipazione a progetti tecnologici comuni (LA 4.3)
5.3	***Procedure per l'acquisizione di beni e servizi***	a. Definire modalità ordinarie di acquisizione di beni e servizi da parte delle P.A., anche mediante l'utilizzo delle centrali d'acquisto pubbliche (CONSIP), per approntare adeguate misure di sicurezza a protezione dei rispettivi assetti cibernetici b. Individuare, a cura degli attori pubblici coinvolti nel relativo processo (AgID, ANAC, Corte dei Conti, Consip, ecc.), strumenti idonei per l'acquisizione dei beni e servizi da parte della P.A. necessari a fronteggiare le emergenze cibernetiche

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 tenendo conto anche di quelli stabiliti per i settori rientranti nel campo di applicazione della Direttiva NIS

		d. Semplificare e armonizzare gli adempimenti e gli obblighi gravanti su amministrazioni e imprese in materia, al fine di incrementare l'efficacia delle comunicazioni in tema di data breach e incident notification nonché l'effettività e l'efficienza di politiche e di misure di sicurezza e. Stimolare in ambito europeo l'avvio di una riflessione in merito alle modalità per procedere, attraverso specifiche disposizioni normative, ad un processo di semplificazione e armonizzazione di adempimenti e obblighi, analogo a quello di cui alla LA 6.1.d.
6.2	*Definizione di un quadro giuridico adeguato per supportare attività di sicurezza in materia cyber*	a. Individuare, alla luce del contesto normativo dell'Unione europea e 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 b. Introdurre nuove disposizioni per disciplinare l'impiego di strumenti di rilevazione e contrasto alle minacce *cyber*
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	***Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione***	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 b. Valutare l'impatto della Direttiva sull'architettura nazionale per la sicurezza dello spazio cibernetico per eventuali revisioni dell'attuale assetto normativo c. Recepire la Direttiva nell'ordinamento nazionale e definire i relativi provvedimenti attuativi, armonizzando le nuove disposizioni con quelle relative alle infrastrutture critiche e strategiche (Direttiva 2008/114/CE e D.Lgs. n. 61/2011)

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 e compliance***	**a.** Aggiornare il quadro nazionale di riferimento agli *standard* e alle *best practices* secondo le normative ratificate NATO e UE, ed internazionali **b.** Identificare e aggiornare le misure minime di sicurezza da implementare sulle reti e i sistemi della PA e delle infrastrutture critiche **c.** Adottare *standard* di riferimento, *best practices* e requisiti minimi per la sicurezza delle reti e dei sistemi (tra cui quelli indicati in 7.1.a e 7.1.b) **d.** Costituire un sistema per l'accreditamento e l'auditing degli Enti responsabili dell'emissione di certificati digitali per l'autenticazione e per le altre certificazioni di sicurezza informatica

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 della sicurezza dei sistemi e delle reti
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 di dati non classificati) attraverso l'Organismo di Certificazione della Sicurezza Informatica (OCSI) b. Mantenere aggiornato uno schema nazionale per la certificazione dei processi utilizzati dai sistemi informativi 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 e. Ampliare lo spettro d'azione del DIS-UCSe ai fini del rilascio delle certificazioni di sicurezza e omologazioni di apparati e sistemi che gestiscono informazioni classificate, prevedendo procedure di verifica estese anche agli ambiti non classificati onde valutare la sicurezza complessiva dei sistemi in uso (classificati e non)

7.5	*Verifica delle misure cyber defence applicate a gestori di servizi essenziali e 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)

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 ***Produzione, Innovazione e Cooperazione Tecnologica***	**a.** Favorire la realizzazione di 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, valutando anche l'introduzione di meccanismi incentivanti, per lo sviluppo di un adeguato tessuto industriale competitivo nel panorama nazionale e internazionale, favorendo la costituzione di *supply-chain* verticali, a livello di Unione europea e nazionale, in cui la produzione sia basata su metodologie di progettazione orientate alla "*security by design*" **c.** Potenziare programmi di cooperazione multilaterali e bilaterali per favorire le funzioni di ricerca e sviluppo nazionali nel contesto europeo e 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 ed i soggetti privati gestori di servizi essenziali devono essere in grado di fornire, ove necessario o opportuno, 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 e operativa***	**a.** Sviluppare un coordinamento sulla *Situation Awareness* dei contenuti e delle informazioni, allo scopo di rendere efficaci i flussi comunicativi anche in funzione delle relative azioni di risposta e ripristino, individuando le circostanze in cui può rendersi necessaria la diffusione al pubblico delle informazioni e relativi canali di comunicazione

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.** Sviluppare 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 *CYBER 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.** Adottare il piano di valutazione dei rischi previsto nell'ambito delle attività strumentali all'implementazione della strategia nazionale, di cui alla Direttiva NIS **b.** Individuare una metodologia di *cyber risk management* univoca e condivisa a livello strategico, adottando modelli per i gestori di servizi essenziali, le infrastrutture critiche e i settori strategici nazionali **c.** Coinvolgere centri di ricerca e università per consentire l'adozione di aggiornati strumenti di gestione del rischio

Prot. n. 0053289 Reg. U
Data: 2017-04-11
D002/01310/2.1.1(66 - UGLG)12

Il Presidente del Consiglio dei Ministri

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'articolo 1, comma 3-*bis*;

VISTO il decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, recante "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" e, in particolare, gli articoli 3 e 4;

VISTA la deliberazione del Comitato interministeriale per la sicurezza della Repubblica formulata nella seduta del 24 marzo 2017;

DISPONE

Articolo 1

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

Roma, 31 MAR. 2017