

Ciclo di webinar in diretta
Sicurezza informatica & Protezione dei dati
negli enti locali

Gli obblighi di cybersecurity per le stazioni
appaltanti- le nuove modifiche previste
dall'articolo 108 comma 4 Dlgs 36/2023 14-12-
2023

Relatore: Dottor Antonio Guzzo Funzionario
Informatico Agenzia delle Entrate
Cyber security expert

DPO CERTIFIED ISO IEC 17024 e UNI 11697:2017

ASMEL - Associazione per la Sussidiarietà e la
Modernizzazione degli Enti Locali

Email info@dpointrete.it

Numero Verde 800.16.56.54 (int.3)

Web: www.dpointrete.it www.asmel.eu



Indice

- ▶ Normativa europea ed italiana cybersecurity
- ▶ Il nuovo codice degli appalti- articolo 108 comma 4 dlgs 36/2023
- ▶ I fattori abilitanti



Normativa

- ▶ Decreto legislativo 18 maggio 2018, n. 65, *"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"*;
- ▶ Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, *"relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»);*
- ▶ Decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre n. 133, recante *"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica"*;



Normativa

- ▶ Decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, recante "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";
- ▶ Decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"*;
- ▶ Decreto-legge 9 giugno 2021, n. 80, convertito, con modificazioni, dalla legge 6 agosto 2021, n. 113, recante *"Misure urgenti per il rafforzamento della capacità amministrativa delle pubbliche amministrazioni funzionale all'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per l'efficienza della giustizia"*, che definisce percorsi veloci, trasparenti e rigorosi per il reclutamento di profili tecnici e gestionali necessari alle finalità del PNRR, tra cui la cybersicurezza;



Normativa

- ▶ Decreto del Presidente del Consiglio dei ministri 9 dicembre 2021, n. 223, recante *"Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale"*;
- ▶ Decreto del Presidente del Consiglio dei ministri 15 giugno 2021, recante *"Individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, in attuazione dell'articolo 1, comma 6, lettera a), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133"*;
- ▶ Strategia Nazionale di Cybersicurezza 2022-2026 e il relativo Piano di Implementazione (di seguito anche "Piano") che definiscono come pianificare, coordinare e attuare misure tese al potenziamento del livello di maturità delle capacità cyber della Pubblica Amministrazione, assicurando una trasformazione digitale sicura e resiliente;



Gli elementi di cybersicurezza: normativa

- ▶ DLGS 31 Marzo 2023 n° 36 ARTICOLO 108 COMMA 4
- ▶ 4. I documenti di gara stabiliscono i criteri di aggiudicazione dell'offerta, pertinenti alla natura, all'oggetto e alle caratteristiche del contratto. In particolare, l'offerta economicamente più vantaggiosa, individuata sulla base del miglior rapporto qualità/prezzo, è valutata sulla base di criteri oggettivi, quali gli aspetti qualitativi, ambientali o sociali, connessi all'oggetto dell'appalto. La stazione appaltante, al fine di assicurare l'effettiva individuazione del miglior rapporto qualità/prezzo, valorizza gli elementi qualitativi dell'offerta e individua criteri tali da garantire un confronto concorrenziale effettivo sui profili tecnici.



Gli elementi di cybersicurezza: normativa

- ▶ DLGS 31 Marzo 2023 n° 36 ARTICOLO 108 COMMA 4
- ▶ Nelle attività di approvvigionamento di beni e servizi informatici per la pubblica amministrazione, le stazioni appaltanti, incluse le centrali di committenza, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione, tengono sempre in considerazione gli elementi di cybersicurezza, attribuendovi specifico e peculiare rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici. Nei casi di cui al quarto periodo, quando i beni e servizi informatici oggetto di appalto sono impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 10 per cento. Per i contratti ad alta intensità di manodopera, la stazione appaltante stabilisce un tetto massimo per il punteggio economico entro il limite del 30 per cento.



Gli elementi di cybersicurezza: normativa

► Cosa cambia per le stazioni appaltanti

- Da quanto riportato all'articolo 108 comma 4 è possibile, quindi, evincere la volontà del Governo in carica di attribuire un peso maggiore agli aspetti concernenti la cybersicurezza di prodotti e servizi acquistati, prediligendo una valutazione tecnico-qualitativa degli stessi, basata su aspetti "qualitativi, ambientali o sociali, connessi all'oggetto dell'appalto".
- La stazione appaltante è, infatti, tenuta alla valorizzazione di tali aspetti, per individuare il miglior rapporto qualità/prezzo e garantire "un confronto concorrenziale effettivo sui profili tecnici", compresi gli "elementi di cybersicurezza", ponendo sempre particolare attenzione nei casi in cui l'impiego dei beni o degli strumenti sia connesso alla tutela degli interessi nazionali strategici. **In questi casi, il legislatore ha stabilito che la stazione appaltante debba decretare un tetto massimo per il punteggio economico entro il limite del 10 per cento. Per i contratti ad alta intensità di manodopera, invece, questa dovrà stabilire un tetto massimo per il punteggio economico entro il limite del 30 per cento. Tale discrezionalità, concessa alle stazioni appaltanti, si ritiene possa rappresentare un vantaggio, in quanto il prezzo risulterebbe meno determinante a fronte di altri fattori correlati alla sicurezza cibernetica e digitale.**



Gli elementi di cybersicurezza: normativa

► Cosa cambia per le stazioni appaltanti

Il Nuovo Codice dei Contratti Pubblici non entra nel merito dei requisiti minimi che devono essere soddisfatti al riguardo. La ragione di tale scelta può essere spiegata con il fatto che tali requisiti possono variare anche notevolmente in considerazione delle dimensioni dell'operatore economico interessato, del suo ambito di operatività e del suo rischio specifico.



Gli elementi di cybersicurezza

Tuttavia, possono essere individuati alcuni elementi comuni che possono costituire un elemento di analisi trasversale; in particolare, possono venire in rilievo a tale riguardo:

- ❑ la valutazione del rischio specifico a cui è esposto l'operatore economico;
- ❑ lo stato di conformità alla normativa in materia di protezione dei dati personali. A tal fine, è necessario un assessment sulla documentazione prodotta in materia di data protection e sui processi implementati, anche nell'ottica di poter soddisfare prontamente eventuali richieste documentali derivanti dalla partecipazione ai bandi di gara;
- ❑ valutazione della propria capacità di gestione dei rischi informatici.



Gli elementi di cybersicurezza: la gestione del rischio

A tal fine possono essere presi in considerazione i seguenti elementi:

- A. Fattore umano: è generalmente l'anello più debole della catena della cybersecurity. Per gestire questo fattore è necessario formare il personale dipendente affinché sia preparato a comprendere e prevenire i rischi che possono provenire dagli strumenti informatici;**
- B. Fattore tecnologico: è necessario analizzare le tecnologie implementate e comprendere come implementare e le best practice applicabili;**
- C. Processi: strettamente correlati al punto b., sono necessari al fine di garantire che l'operatore economico sia in grado di prevenire e gestire gli incidenti informatici]**



Gli elementi di cybersicurezza: quali sono

- Gli elementi per la cybersicurezza vengono evidenziati nella strategia nazionale sulla cybersicurezza 2022-2026 approvata nel 2022 dal Governo Draghi G.U. n° 127 del 01-06-2022



Gli elementi di cybersicurezza: quali sono

- ▶ la recente riforma dell'architettura nazionale cyber, che è stata attuata attraverso l'adozione del decreto-legge 14 giugno 2021, n. 82. Il decreto ha istituito l'Agenzia per la Cybersicurezza Nazionale (ACN), con l'obiettivo di razionalizzare e semplificare il frammentato sistema di competenze, esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.
- ▶ L'Agenzia, in qualità di Autorità nazionale per la cybersicurezza, ha tra i suoi compiti quello di predisporre la strategia nazionale di cybersicurezza. Inoltre, ai sensi del citato decreto-legge, l'ACN è designata quale Autorità nazionale competente in via esclusiva e punto di contatto unico (PoC) per le finalità di cui alla normativa sulla sicurezza delle reti e dei sistemi informativi (NIS), Autorità nazionale di certificazione della cybersicurezza, Centro Nazionale di Coordinamento (NCC) rispetto al Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca, ed elemento centrale del Perimetro di sicurezza nazionale cibernetica (PSNC).



Gli elementi di cybersicurezza: quali sono

- ▶ Ulteriore strumento strategico per affrontare le sfide è il Piano Nazionale di Ripresa e Resilienza (PNRR). Nell'ambito della Missione 1 "Digitalizzazione, Innovazione, Competitività, Cultura e Turismo", sono incluse le attività di transizione digitale della Pubblica Amministrazione, quali il progetto del Cloud Nazionale e la digitalizzazione dei processi e servizi per i cittadini, la cui realizzazione porterà al potenziamento delle capacità di resilienza delle infrastrutture e dei servizi digitali del Paese. Inoltre, lo specifico Investimento 1.5 "Cybersecurity" - pari a 623 milioni di euro - rimesso all'Agenzia per la Cybersicurezza Nazionale quale Soggetto Attuatore, prevede la realizzazione di specifiche progettualità per la creazione e lo sviluppo di servizi all'avanguardia per la gestione del rischio cyber, con strette connessioni, a livello nazionale e internazionale, con tutti i principali partner della Pubblica Amministrazione, dell'impresa e dei fornitori di tecnologia. Ciò, al fine di conseguire un'autonomia tecnologica nazionale ponendo la cybersicurezza e la resilienza a fondamento della trasformazione digitale della Pubblica Amministrazione.



Gli elementi di cybersicurezza: quali sono

- Per fronteggiare al meglio le sfide per il sistema-Paese sopra delineate, sono stati individuati tre obiettivi fondamentali - **protezione, risposta e sviluppo** - e relative misure, funzionali ad assicurare la concreta attuazione della strategia, raggruppate per aree tematiche e declinabili sia dal punto di vista organizzativo e di policy che prettamente operativo. Ciascuna misura è stata associata all'obiettivo maggiormente caratterizzante, per ognuna delle quali è indicato il novero degli attori responsabili dell'implementazione e tutti gli altri soggetti a vario titolo interessati, al netto di quelli direttamente beneficiari delle misure.



Protezione

La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.



Risposta

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.



Sviluppo

Lo sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

Gli elementi di cybersicurezza: quali sono

► **OBIETTIVO PROTEZIONE**

La protezione degli asset strategici nazionali, attraverso un approccio sistemico orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli che possono abilitare una transizione digitale resiliente del Paese. Di particolare importanza è lo sviluppo di strategie e iniziative per la verifica e valutazione della sicurezza delle infrastrutture ICT, ivi inclusi gli aspetti di approvvigionamento e supply-chain a impatto nazionale.

Per poter assicurare un livello di protezione efficace e duraturo è, infatti, indispensabile:

A. il potenziamento delle capacità del Centro di Valutazione e Certificazione Nazionale (CVCN) dell'Agenzia per la Cybersicurezza Nazionale e, negli ambiti di competenza, dei Centri di Valutazione (CV) del Ministero dell'Interno e della Difesa, nonché l'integrazione con una rete di Laboratori Accreditati di Prova, permetterà di sviluppare capacità nazionali di valutazione delle vulnerabilità di tecnologie avanzate a servizio degli asset più critici del Paese;



Protezione

La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.

Gli elementi di cybersicurezza: quali sono

► OBIETTIVO PROTEZIONE

B. la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente in materia di cybersicurezza, che tenga conto degli orientamenti e degli sviluppi in ambito europeo ed internazionale. Tale impianto non ricomprende solamente il livello normativo, quanto anche l'insieme di linee guida, schemi di certificazione e policy settoriali rivolte ai soggetti pubblici e agli operatori privati. In tale contesto, assume rilevanza primaria:

- il supporto allo sviluppo di schemi di certificazione e standard europei e internazionali in materia di cyber-sicurezza;
- la promozione dell'utilizzo di schemi di certificazione europea in materia di cybersicurezza, da parte delle imprese italiane specializzate, al fine di conseguire un vantaggio competitivo sul mercato;
- l'adozione di linee guida per le amministrazioni pubbliche, basate su di un approccio "zero trust" quale cambiamento di paradigma nella gestione del rischio cyber, affinché le relative reti, sistemi e servizi soddisfino elevati standard di cybersicurezza;



Protezione

La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.

Gli elementi di cybersicurezza: quali sono

► **OBIETTIVO PROTEZIONE**

B. ■ la valorizzazione dell'inclusione di elementi di sicurezza cibernetica nelle attività di procurement ICT della Pubblica Amministrazione;

■ la definizione di una politica nazionale sulla divulgazione coordinata di vulnerabilità, così da porre il Paese al passo con altre nazioni e con quanto richiesto dalla comunità internazionale;



Protezione

La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.

Gli elementi di cybersicurezza: quali sono

► **OBIETTIVO PROTEZIONE**

■ C. la conoscenza approfondita del quadro della minaccia cibernetica e il possesso di adeguati strumenti tecnici, competenze specialistiche e capacità operative, in capo agli attori a vario titolo coinvolti. L'ulteriore rafforzamento della situational awareness mediante il monitoraggio continuo degli eventi cibernetici e la tempestiva condivisione delle connesse risultanze, secondo gli specifici ambiti di competenza, costituisce, infatti, condizione necessaria ai fini dell'incremento delle capacità nazionali di difesa, resilienza, contrasto al crimine informatico e cyber intelligence. A tal fine, appare essenziale il costante scambio informativo pubblico-privato e pubblico-pubblico, anche mediante l'introduzione di canali di comunicazione protetti e di un sistema integrato di gestione del rischio cyber per identificare e analizzare vulnerabilità, minacce e rischi in chiave previsionale e programmatica;



Protezione

La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.

Gli elementi di cybersicurezza: quali sono

► **OBIETTIVO PROTEZIONE**

■ D. il potenziamento del livello di maturità delle capacità cyber della Pubblica Amministrazione, assicurando una trasformazione digitale sicura e resiliente. A tal fine, la transizione verso il Cloud della Pubblica Amministrazione, sia verso tecnologie di Public Cloud che mediante la creazione di un Polo Strategico Nazionale (PSN), rappresenta un elemento fondante per garantire adeguate garanzie di autonomia tecnologica del Paese.



Protezione

La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.

Gli elementi di cybersicurezza: quali sono

► OBIETTIVO PROTEZIONE

- E. lo sviluppo di capacità di protezione per le infrastrutture nazionali, realizzate anche mediante programmi con i privati, tra cui:
 - il monitoraggio delle configurazioni Border Gateway Protocol (BGP) mediante lo sviluppo di procedure, processi e strumenti in cooperazione con gli Internet Exchange Point (IXP) nazionali, al fine di aumentare la resilienza delle infrastrutture BGP nazionali;
 - un'infrastruttura di risoluzione Domain Name System (DNS) nazionale, con servizi di protezione della navigazione web a uso della PA, per un utilizzo più sicuro della rete Internet;
 - il monitoraggio di vulnerabilità e configurazioni erranee dei servizi digitali della PA, sia a livello applicativo che di configurazioni DNS, al fine di ridurre in modo proattivo potenziali superfici di attacco;
 - il monitoraggio delle configurazioni dei domini di posta elettronica della PA, supportando e facilitando l'applicazione delle migliori configurazioni di sicurezza contro eventi di phishing o abusi collegati;



Protezione

La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.

Gli elementi di cybersicurezza: quali sono

F. la promozione dell'uso della crittografia come strumento di cybersicurezza, favorendo l'impiego di crittografia commerciale lungo l'intero ciclo di vita dei sistemi e servizi ICT, in conformità ai principi della sicurezza e della tutela della privacy, nel rispetto dei principi stabiliti dalla normativa nazionale ed europea. In tale contesto e in settori specifici, l'ACN, anche in sinergia con le altre Amministrazioni, intende sviluppare tecnologie/sistemi di cifratura nazionale, il che ha come prerequisito la creazione di un apposito ecosistema nazionale per il suo mantenimento ed evoluzione;

G. l'implementazione di un'azione di coordinamento nazionale, coerente con le iniziative adottate a livello europeo e in sinergia con i Paesi like-minded, per prevenire e contrastare la disinformazione online, che sfruttando le caratteristiche del dominio cibernetico, mira a condizionare/influenzare processi politici, economici e sociali del Paese.



Protezione

La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO RISPOSTA

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso l'impiego di elevate capacità nazionali di monitoraggio, rilevamento, analisi e risposta e l'attivazione di processi che coinvolgano tutti gli attori facenti parte dell'ecosistema di cybersicurezza nazionale. Una risposta quanto più tempestiva e risolutiva deve, infatti, necessariamente basarsi su:

A. un sistema di gestione crisi cibernetica nazionale - assicurato dal Nucleo per la Cybersicurezza (NCS) - e transnazionale, che sia fondato su procedure di collaborazione consolidate supportate da costanti flussi informativi ed elementi di conoscenza condivisi anche grazie a reti e infrastrutture nazionali e transnazionali, con il coinvolgimento delle Amministrazioni e degli operatori privati interessati.



Risposta

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO RISPOSTA

In tale ambito dovranno altresì essere assicurati:

- lo sviluppo di un sistema di coordinamento continuativo di tutte le Amministrazioni che compongono il NCS, che garantisca una tempestiva e sinergica gestione dei vari possibili scenari di crisi cibernetica, nonché una immediata implementazione delle misure di risposta;
- il periodico aggiornamento delle procedure operative relative alle misure di risposta connesse ai vari scenari della minaccia cyber per le determinazioni del Presidente del Consiglio, ai sensi della vigente normativa nazionale, e per la conseguente corretta implementazione da parte dei soggetti interessati;
- una pronta attività di comunicazione istituzionale in caso di incidenti cyber rilevanti o di crisi cibernetica, nonché ogni qual volta si renda necessario svolgere azioni di sensibilizzazione nei confronti della popolazione civile;



Risposta

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO RISPOSTA

B. l'integrazione degli attuali servizi cyber nazionali nei seguenti ambiti:

- identificazione della minaccia realizzando un "Hyper SOC" ovvero un sistema di raccolta, correlazione e analisi di eventi di interesse da Security Operation Center (SOC), nonché dagli Internet Service Provider (ISP) mediante apposite convenzioni, al fine di individuare precocemente eventuali "pattern" di attacco complessi che potrebbero rappresentare minacce emergenti di interesse;
- assicurare e facilitare modalità di notifica unitaria degli incidenti di sicurezza cibernetica al Computer Security Incident Response Team (CSIRT), così da rendere più efficace la capacità di risposta e allarme tempestivo;



Risposta

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO RISPOSTA

B. l'integrazione degli attuali servizi cyber nazionali nei seguenti ambiti:

- risposta agli incidenti realizzando una rete di CSIRT/Computer Emergency Response Team (CERT) settoriali federati con lo CSIRT Italia per la condivisione di procedure, informazioni e supporto nella risposta alle minacce emergenti e agli incidenti;
- condivisione di informazioni realizzando un Information Sharing and Analysis Center (ISAC) centrale presso l'Agenzia, integrabile con una rete di ISAC settoriali sviluppati mediante iniziative pubblico-private, che possa potenziare la diffusione e l'applicazione di informazioni a maggior valore aggiunto per l'innalzamento del livello di cyber resilience del Paese, quali ad esempio best-practice di settore, linee guida, avvisi di sicurezza e raccomandazioni;
- qualificazione di aziende in materia di incident response, in grado di fornire supporto allo CSIRT Italia nel caso in cui dovesse verificarsi una moltitudine di incidenti cyber di natura sistemica.



Risposta

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO RISPOSTA

Queste capacità sono pienamente in linea con l'iniziativa lanciata dalla Strategia di cybersecurity dell'Unione europea di realizzazione di uno "EU CyberShield" e si avvarranno delle più recenti tecnologie di intelligenza artificiale (IA) e machine learning messe a disposizione da un centro di "High Performance Computing" (HPC) realizzato ad hoc, nonché da sistemi integrati di monitoraggio e analisi del rischio cyber nazionale. L'Italia si porrà alla guida, in Europa, del processo di sviluppo e di integrazione con i diversi Stati membri di questi nuovi strumenti tecnologici.

C. l'organizzazione di periodiche esercitazioni di sicurezza cibernetica e resilienza, anche nell'ambito del Perimetro di sicurezza nazionale cibernetica, nonché la promozione e il coordinamento della partecipazione a quelle europee e internazionali;



Risposta

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO RISPOSTA

D. la definizione del posizionamento e della procedura nazionale in materia di attribuzione di attività cibernetiche ostili, che specifichi anche i diversi attori coinvolti e il relativo contributo. Il nostro Paese, infatti, quale membro dell'UE e della NATO, è sovente chiamato ad apportare il proprio contributo nei rispettivi consessi, per l'applicazione delle misure di risposta ad attività cyber ostili - incluso il rilascio di dichiarazioni congiunte - contemplate nell'EU Cyber Diplomacy Toolbox e nella NATO Guide for Response Options to Malicious Cyber Activities. È importante evidenziare al riguardo come l'attribuzione costituisca prerogativa nazionale dei singoli Paesi membri, come riconosciuto nei documenti di policy delle citate organizzazioni;



Risposta

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO RISPOSTA

E. il contrasto al cybercrime, declinato nella prevenzione e nel contrasto delle attività criminali di matrice comune, organizzata e terroristica rivolte all'integrità delle infrastrutture critiche informatizzate, erogatori dei servizi pubblici essenziali; nella prevenzione e nel contrasto ai financial cybercrime ed alle attività illecite dirette a colpire le infrastrutture finanziarie; nell'attività info investigativa condotta, in collaborazione con i competenti Uffici della PS, in materia di tutela dell'ordine pubblico e di contrasto al terrorismo, colti nella loro proiezione cibernetica; nella tutela della persona, con particolare riguardo alla protezione dei minori, dalle aggressioni alla libertà personale e sessuale, alla sicurezza, all'incolumità, alla riservatezza, all'onore ed alla reputazione che si realizzano nella dimensione virtuale, ovvero mediante l'utilizzo di strumenti informatici o telematici;

F. Il rafforzamento delle capacità di deterrenza in ambito cibernetico



Risposta

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO SVILUPPO

Lo sviluppo consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale, in grado di rispondere alle esigenze del mercato. La costellazione di centri di eccellenza e imprese che compongono, assieme all'accademia, il tessuto della ricerca e dello sviluppo è infatti un patrimonio essenziale per il nostro Paese con importanti potenzialità di espansione. Numerosi sono gli strumenti e le iniziative avviate negli ultimi anni per supportare lo sviluppo delle capacità del sistema nazionale di ricerca, la trasformazione digitale e l'innovazione tecnologica, tra cui si annoverano, in particolare, quelli previsti dal PNRR, dalle ultime leggi di bilancio, e dal Piano Nazionale Impresa 4.0. Per accrescere ulteriormente tale impegno, è pertanto fondamentale:



Sviluppo

Lo sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO SVILUPPO

A. il ruolo del Centro Nazionale di Coordinamento (NCC) che, in stretto raccordo con il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca (ECCC), è chiamato a supportare lo sviluppo e il potenziamento dell'autonomia strategico-tecnologica e digitale dell'Unione europea e del nostro Paese. Ciò, coordinando le attività di ricerca e sviluppo, favorendo l'osmosi con il mondo industriale, accademico e della ricerca per l'avvio di progetti e partnership pubblico-private in cybersicurezza, mediante l'eccesso a finanziamenti nazionali ed europei. In questo senso, risultano fondamentali le sinergie con i Centri di competenza ad alta specializzazione e i Digital Innovation Hub (DIH) attivi sul territorio nazionale;



Sviluppo

Lo sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO SVILUPPO

B. lo sviluppo di tecnologia nazionale ed europea, così da ridurre la dipendenza da tecnologie extra-UE, attraverso l'avvio di dedicate progettualità che saranno realizzate - grazie a specifici stanziamenti utilizzando sia fondi nazionali che europei - nell'ambito di un "parco nazionale della cybersicurezza" destinato, a tendere, ad inglobare i Cluster tecnologici che svolgono attività in materia. Tale tecnologia consentirà di sviluppare un'industria nazionale ed europea competitiva, anche attraverso una specializzazione virtuosa di startup e piccole e medie imprese (PMI) innovative, in grado di fornire tecnologie e servizi abilitanti ad elevato grado di sicurezza, con particolare riguardo alle infrastrutture critiche digitali;



Sviluppo

Lo sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO SVILUPPO

C. la realizzazione di un "parco nazionale della cybersicurezza" che, mettendo a sistema competenze e risorse provenienti dalla Pubblica Amministrazione, dall'industria e dal mondo accademico e della ricerca, fornisca tutte le infrastrutture tecnologiche necessarie allo svolgimento di attività di ricerca e sviluppo nell'ambito della cybersecurity e delle tecnologie digitali quali, a titolo di esempio, l'intelligenza artificiale, il quantum computing & cryptography e la robotica. Con la sua creazione si intende conseguire nel tempo una maggiore autonomia strategica nazionale sulle tecnologie cyber, sostenendo lo sviluppo e la produzione di software e hardware nazionali da impiegare nelle reti e nei sistemi di maggiore rilevanza strategica. Il parco è concepito come un incubatore di capacità e tecnologie, al cui interno giovani talenti e startup possano entrare in contatto con le grandi aziende e con le diverse realtà nazionali che, a vario titolo, operano nel settore. Per tale motivo, il parco deve poter disporre di una struttura "diffusa" nella quale, accanto ad un "hub" centrale, sussistono ramificazioni distribuite sull'intero territorio nazionale;



Sviluppo

Lo sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO SVILUPPO

D. l'introduzione di nuovi meccanismi e soluzioni incentivanti per continuare a supportare lo sviluppo industriale, tecnologico e della ricerca, con particolare riferimento allo sviluppo di competenze e al trasferimento tecnologico (specie nei settori avanzati della cybersicurezza).

Ciò, anche con l'obiettivo di:

- continuare a favorire la competitività del sistema produttivo del Paese, sostenendo le imprese nella loro transizione digitale ed ecologica, agevolandone l'internazionalizzazione e l'attrazione di investimenti;



Sviluppo

Lo sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

Gli elementi di cybersicurezza: quali sono

OBIETTIVO SVILUPPO

- realizzare prodotti e servizi ICT ad alta affidabilità, anche incoraggiando la creazione di Product Security Incident Response Team (PSIRT) da parte degli operatori privati, per accrescere le loro capacità di gestire le vulnerabilità di prodotti ICT;

il continuo impulso all'innovazione tecnologica e alla digitalizzazione della Pubblica Amministrazione e del tessuto produttivo del Paese, assicurando una costante rispondenza ai principi di cybersicurezza e facendo ricorso alle risorse messe a disposizione dal PNRR. Ciò va di pari passo con la promozione di iniziative volte a rafforzare l'autonomia industriale e tecnologica dell'Italia.



Sviluppo

Lo sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

I fattori abilitanti

FATTORI ABILITANTI

Al fin di realizzare gli obiettivi descritti, è indispensabile fare riferimento a una serie di fattori abilitanti - **formazione, promozione della cultura della sicurezza cibernetica e cooperazione** - i quali, data la loro trasversalità, sono necessariamente correlati a tutti e tre gli obiettivi sopra delineati, quali elementi imprescindibili per la loro piena attuazione.

1. In primo luogo, la formazione in ambito cyber, con particolare focus sulle nuove tecnologie. Questo deve realizzarsi tramite:
 - meccanismi incentivanti che favoriscano la progressiva familiarizzazione degli studenti con le nuove tecnologie informatiche, con approccio formativo e di respiro culturale, prima ancora che tecnico e pratico.



Protezione

La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.



Risposta

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.



Sviluppo

Lo sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

Gli elementi di cybersicurezza: i fattori abilitanti

FATTORI ABILITANTI

- ▶ meccanismi incentivanti che promuovano l'inserimento in carriere tecnico-scientifiche (cercando anche di colmare il divario di genere presente in esse), con particolare riferimento agli aspetti di cybersicurezza;
- ▶ il continuo aggiornamento della didattica e della preparazione del corpo docente, a tutti i livelli di istruzione scolastica e universitaria, affinché l'offerta educativa sia al passo con lo sviluppo delle conoscenze e delle tecnologie e con le esigenze dettate dal mercato del lavoro, secondo un approccio fondato sul binomio, ormai inscindibile, sviluppo e sicurezza;
- ▶ il dispiegamento di fondi per la formazione specialistica e l'aggiornamento professionale nei settori pubblico e privato, da realizzarsi in modo continuo e multilivello così da favorire la crescita e la qualificazione delle risorse umane operanti nel campo della cybersicurezza e di conseguire una sovranità nazionale digitale delle competenze



Protezione

La protezione degli asset strategici nazionali, attraverso un approccio orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli per abilitare una transizione digitale resiliente del Paese.



Risposta

La risposta alle minacce, agli incidenti e alle crisi cyber nazionali, attraverso sistemi di monitoraggio, rilevamento, analisi e attivazione di processi che coinvolgano l'intero ecosistema di cybersicurezza nazionale.



Sviluppo

Lo sviluppo sicuro delle tecnologie digitali, per rispondere alle esigenze del mercato, attraverso strumenti e iniziative volti a supportare i centri di eccellenza, le attività di ricerca e le imprese.

Gli elementi di cybersicurezza: i fattori abilitanti

FATTORI ABILITANTI

- la realizzazione di un sistema nazionale di certificazione di tali professionalità (sia in ambito scolastico/accademico che lavorativo), mediante l'attivazione di percorsi di formazione ad hoc approvati dall'ACN;
- percorsi di formazione specifici per i non specialisti della materia, rivolti ai dipendenti di Pubbliche Amministrazioni e soggetti privati, incluse le PMI, ad iniziare dai top manager, così da sensibilizzare gli stessi in merito all'importanza di concepire la cybersicurezza più come un investimento che come un costo;
- il potenziamento delle capacità di cyber diplomacy, attraverso percorsi mirati per il personale diplomatico da dispiegare nei principali consessi internazionali sulla tematica e mettersi così al passo con altri Paesi, europei e non.



Gli elementi di cybersicurezza: i fattori abilitanti

FATTORI ABILITANTI

1. Altro fattore abilitante, che si muove in parallelo con le esigenze di formazione, è la promozione della cultura della sicurezza cibernetica, al fine di aumentare la consapevolezza del settore pubblico e privato e della società civile sui rischi e le minacce cyber, le quali includono non solo gli attacchi cibernetici propriamente intesi, ma anche la diffusione di contenuti fake e il fenomeno del cyberbullismo, che, ancorché non nuovo, non cessa di creare allarme sociale.

Al riguardo, è quindi importante che i soggetti pubblici, gli operatori privati e la società civile nel suo complesso, percepiscano il proprio ruolo quale parte attiva e responsabile all'interno del sistema-Paese, attuando comportamenti sicuri e virtuosi nello spazio cibernetico. Ciò deve avvenire:

- attraverso la previsione di un programma capillare di educazione digitale - da sviluppare anche online - a beneficio della collettività e diretto all'adozione di buone prassi e all'acquisizione di capacità di verificare i contenuti e le informazioni reperite online avendo contezza di quegli indicatori che consentono di identificare le c.d. "fake news";



Gli elementi di cybersicurezza: i fattori abilitanti

FATTORI ABILITANTI

- all'interno delle organizzazioni pubbliche e private, mediante una forte sensibilizzazione delle risorse - ad iniziare dai livelli apicali per poi coinvolgere l'intera linea - non soltanto per promuovere una "cyber hygiene" interna, quanto per accrescere la percezione delle esigenze di sicurezza dell'organizzazione e delle minacce a cui questa è esposta, nonché per mettere in campo le azioni di prevenzione più efficaci;
- promuovendo la gestione consapevole del cd. "rischio residuo", anche prevedendo l'adozione di strumenti di autovalutazione basati su specifici "cyber index", che consentono alle organizzazioni una gestione autonoma del livello di esposizione.



Gli elementi di cybersicurezza: i fattori abilitanti

FATTORI ABILITANTI

1. Da ultimo vi è la cooperazione, da incrementare:

- sul fronte nazionale, a livello governativo, nel rapporto pubblico-privato, pubblico-pubblico, nonché con accademia e ricerca. In tale contesto, è prevista la creazione di tavoli operativi permanenti con i soggetti Perimetro suddivisi per settore, a seconda delle trattazioni ed esigenze contingenti, per creare maggiori sinergie tra le Pubbliche Amministrazioni e l'industria;
- in ambito internazionale, partecipando in modo proattivo alle iniziative europee e internazionali e promuovendo collaborazioni bilaterali.



Gli elementi di cybersicurezza: i fattori abilitanti

FATTORI ABILITANTI

Trasversale ai citati obiettivi di protezione, risposta e sviluppo, nonché ai richiamati fattori abilitanti della formazione, della promozione della cultura della cybersicurezza e della cooperazione, è la Partnership Pubblico-Privato (PPP), la quale permea interamente la presente strategia, improntata come già detto ad un approccio "whole-of-society", che vede il settore pubblico agire sinergicamente con quello privato, il mondo accademico e della ricerca, i media, le famiglie e gli individui per rafforzare la resilienza cibernetica della nazione e della società nel suo insieme. Lo spazio cibernetico è, peraltro, costituito da prodotti e servizi ICT realizzati ovvero erogati principalmente da soggetti privati.



Gli elementi di cybersicurezza previsti da ACN

L'Agenzia per la Cybersicurezza Nazionale, in qualità di Soggetto attuatore dell'Investimento 1.5 “Cybersecurity” - Missione 1 ha lo scopo di individuare delle proposte progettuali finalizzate al potenziamento del livello di maturità delle capacità cyber dei sistemi informativi delle Regioni, dei Comuni capoluogo facenti parte di Città metropolitane, delle Province autonome.

Il fine ultimo degli interventi è quello di potenziare il livello di resilienza cyber dei sistemi informativi per la messa in sicurezza dei dati e dei servizi dei cittadini. Questi interventi, nonché il complesso degli interventi dell'Investimento 1.5, rappresentano un elemento fondante per la transizione digitale sicura della PA. Pertanto, **l'investimento 1.5 rappresenta una opportunità imprescindibile per la PA, e nel complesso per il Paese, per irrobustire le infrastrutture e i servizi digitali, nonché le competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza per il paese.**

Nel perseguimento degli obiettivi sopra indicati, l'Agenzia per la Cybersicurezza Nazionale, in accordo con il DTD, intende attuare per l'individuazione dei Soggetti attuatori, mediante una selezione di progetti cd. “a regia”, volti al potenziamento della resilienza cyber dei sistemi informativi.



Il modello della postura informatica previsti da ACN per gli enti locali

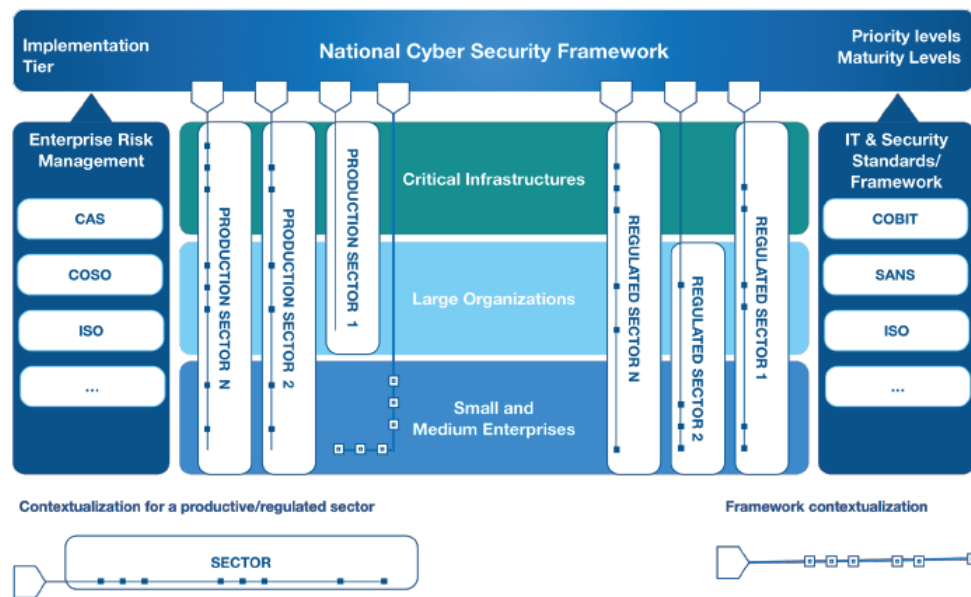
Il modello di analisi della postura di sicurezza è definito in linea con il "Framework nazionale per la cybersicurezza e la data protection" ed ha l'obiettivo di uniformare i risultati del censimento dei livelli di resilienza cyber della PA, introducendo concetti quali la rilevanza e i livelli di maturità delle prassi di sicurezza. La compilazione, nonché eventuale contestualizzazione del modello alle specificità del Soggetto attuatore dell'intervento, sarà responsabilità dello stesso in accordo alle modalità prescelte, quali ad esempio conduzione di interviste, compilazione di check-list di autovalutazione o la conduzione di verifiche tecniche o documentali. Pertanto, il Soggetto attuatore dell'intervento sarà responsabile dei livelli di maturità identificati e, quindi, degli eventuali rischi e criticità annesse.

Il modello di piano di potenziamento strategico ha l'obiettivo di tracciare le attività di rientro dalle scoperture eventualmente identificate in fase di analisi. Il piano ha l'obiettivo di tracciare una vista organica degli investimenti da realizzare in ambito cyber per la PA, sia a breve che a medio-lungo termine.



Il National Cybersecurity Framework

Contextualization



Il modello della postura informatica previsti da ACN per gli enti locali

- Le proposte intendono realizzare opportune progettualità per la risoluzione di criticità delle capacità di gestione del rischio cyber nei sistemi informativi del Soggetto richiedente. Le stesse dovranno essere documentate mediante opportune schede progetto e potranno interessare una o più delle seguenti tipologie di intervento:

1) analisi della postura di sicurezza e piano di potenziamento: progetti volti all'individuazione del livello di maturità delle capacità cyber dei servizi informativi al fine di effettuare una pianificazione strategica di un piano di potenziamento delle capacità cyber, quali, a titolo esemplificativo:

- attività di analisi di dettaglio delle procedure, processi e organizzazione delle capacità cyber;
- analisi delle capacità dei sistemi e strumenti di sicurezza in essere;
- analisi dei processi e strumenti di gestione delle identità digitali;



Il modello della postura informatica previsti da ACN per gli enti locali

2) miglioramento dei processi e dell'organizzazione di gestione della cybersecurity: progetti volti all'analisi, miglioramento e potenziamento dei processi di gestione del rischio cyber attualmente in uso, quali, a titolo esemplificativo:

- definizione di procedure di risposta ad attacchi ransomware, o incidenti di natura cyber;
- revisione e potenziamento dei processi e metodologie di security-by-design e sviluppo sicuro;
- revisione e potenziamento dei processi a supporto della continuità operativa;
- revisione e potenziamento dei processi di gestione delle vulnerabilità;



Il modello della postura informatica previsti da ACN per gli enti locali

3) miglioramento della consapevolezza delle persone: progetti volti al rafforzamento delle competenze, pratiche e attitudini del personale del Soggetto attuatore dell'intervento nella gestione del rischio cyber, quali, a titolo esemplificativo:

- servizi di formazione per l'identificazione e gestione di mail di phishing;
- servizi di formazione per la preparazione del personale, sia tecnico che manageriale, coinvolto durante incidenti di natura cyber;



Il modello della postura informatica previsti da ACN per gli enti locali

4) progettazione e sviluppo di nuovi sistemi per la mitigazione del rischio cyber: progetti volti al potenziamento dei sistemi di mitigazione del rischio cyber, quali, a titolo esemplificativo:

- attività di verifica e rafforzamento delle configurazioni di sicurezza perimetrale e monitoraggio;
- acquisizione di nuovi servizi o strumenti di sicurezza;
- potenziamento delle piattaforme di gestione delle identità e degli accessi interni e da remoto;
- potenziamento mediante nuovi strumenti delle capacità di monitoraggio del rischio cyber (SOC);
- potenziamento mediante nuovi strumenti delle capacità di risposta a incidenti di sicurezza (CERT/CSIRT).

Gli interventi dovranno essere implementati, in via preferenziale, nei settori dell'assistenza sanitaria, dell'energia e dell'ambiente (approvvigionamento di acqua potabile).

