AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

DELIBERA N. 259/25/CONS

APPROVAZIONE DELLA POLITICA PER LO SVILUPPO DELLA CONSAPEVOLEZZA SUI RISCHI ASSOCIATI ALLE MINACCE INFORMATICHE

L'AUTORITÀ

NELLA riunione di Consiglio del 28 ottobre 2025;

VISTA la legge 14 novembre 1995, n. 481, recante "*Norme per la concorrenza e la regolazione dei servizi di pubblica utilità. Istituzione delle Autorità di regolazione dei servizi di pubblica utilità*";

VISTA la legge 31 luglio 1997, n. 249, recante "*Istituzione dell'Autorità per le garanzie nelle comunicazioni e norme sui sistemi delle telecomunicazioni e radiotelevisivo*";

VISTA la legge 7 agosto 1990, n. 241, recante "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*";

VISTA la legge 28 giugno 2024, n. 90, recante "*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*";

VISTO il decreto legislativo 4 settembre 2024, n. 138, recante "*Recepimento della Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*", c.d. decreto NIS;

VISTA la delibera n. 223/12/CONS, del 27 aprile 2012, recante "*Adozione del nuovo Regolamento concernente l'organizzazione e il funzionamento dell'Autorità*" (di seguito, anche "Regolamento"), come modificata, da ultimo, dalla delibera n. 58/25/CONS, del 6 marzo 2025;

VISTA la delibera n. 201/22/CONS, del 15 giugno 2022, recante "*Organizzazione interna dell'Autorità per le Garanzie nelle Comunicazioni relativa agli adempimenti in materia di trattamento dei dati personali ai sensi dell'articolo 29 del regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 e dell'articolo 2-quaterdecies del d.lgs. 30 giugno 2003, n. 196*";

VISTA la delibera 204/25/CONS, del 30 luglio 2025 recante "*Individuazione della governance per la gestione della sicurezza informatica di cui alla determinazione ACN n. 164179 del 14 aprile 2025*" (di seguito, "delibera *governance*");

VISTA la determinazione ACN n. 164179 del 14 aprile 2025, ed in particolare il paragrafo 3.2 dell'Allegato 2 che reca la misura: *"Consapevolezza e formazione (PR.AT): Il personale dell'organizzazione è sensibilizzato e formato sulla cybersecurity in modo da poter svolgere i propri compiti inerenti alla cybersecurity"* (di seguito, "determinazione");

VISTO il *"Framework Nazionale per la Cybersecurity e la Data Protection"*, edizione 2025 (Framework nazionale), realizzato dal Centro di ricerca di *cyber intelligence and information security* (CIS) della Sapienza Università di Roma e dal Cybersecurity national lab del Consorzio

interuniversitario nazionale per l'informatica (CINI), in collaborazione con l'Agenzia per la cybersicurezza nazionale (ACN), quale strumento di supporto per le organizzazioni pubbliche e private in materia di strategie e processi volti alla sicurezza informatica;

CONSIDERATO che il decreto NIS, all'articolo 9, comma 2, lettera f) prevede *"la promozione e lo sviluppo di attività di istruzione, formazione e sensibilizzazione, di competenze e di iniziative di ricerca e sviluppo in materia di sicurezza informatica, nonché orientamenti sulle buone pratiche e sui controlli concernenti l'igiene informatica, destinati ai cittadini, ai portatori di interessi e ai soggetti essenziali e importanti";*

CONSIDERATO che il predetto decreto, all'articolo 23, comma 1, lettere a) e b) prevede che gli organi di amministrazione e gli organi direttivi dei soggetti essenziali: *"a) sono tenuti a seguire una formazione in materia di sicurezza informatica; b) promuovono l'offerta periodica di una formazione coerente a quella di cui alla lettera a) ai loro dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti".*

CONSIDERATO, pertanto, che la formazione e la sensibilizzazione assumono un ruolo strategico a tutti i livelli dell'organizzazione, come strumenti essenziali per accrescere la consapevolezza sulle minacce della *cybersecurity* e orientare l'adozione di pratiche digitali sicure;

CONSIDERATO che la **misura PR.AT-01** dell'allegato 2 alla determinazione prevede, al paragrafo 3.2.1, che "***Il personale*** *è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.*

1. È definito, attuato, aggiornato e documentato un ***piano di formazione in materia di sicurezza informatica del personale, ivi inclusi gli organi di amministrazione e direttivi****, che comprende almeno:*

a) la pianificazione delle attività di formazione previste con l'indicazione dei contenuti della formazione fornita;

b) le eventuali modalità di verifica dell'acquisizione dei contenuti.

2. Il piano di formazione di cui al punto 1 è approvato dagli organi di amministrazione e direttivi*.*

3. È mantenuto un registro aggiornato recante l'elenco dei dipendenti che hanno ricevuto la formazione di cui al punto 1, i relativi contenuti e l'elenco delle verifiche svolte laddove previste.";

CONSIDERATO che la **misura PR.AT-02** dell'allegato 2 alla determinazione prevede, al paragrafo 3.2.1, che "***Gli individui che ricoprono ruoli specializzati sono sensibilizzati*** *e formati in modo da possedere le conoscenze e le competenze per svolgere i pertinenti compiti tenendo conto dei rischi di cybersecurity.*

1. Il piano di cui alla misura PR.AT-01 prevede una ***formazione dedicata al personale con ruoli specializzati****, ossia che richiedono una serie di capacità e competenze attinenti alla sicurezza, ivi compresi gli amministratori di sistema, che comprende almeno:*

a) le istruzioni relative alla configurazione e al funzionamento sicuri dei sistemi informativi e di rete;

b) le informazioni sulle minacce informatiche note;

c) le istruzioni sul comportamento da tenere in caso di eventi rilevanti per la sicurezza.

2. È mantenuto un registro aggiornato recante l'elenco dei dipendenti che hanno ricevuto la formazione di cui al punto 1, i relativi contenuti e l'elenco delle verifiche svolte laddove previste.";

CONSIDERATO che l'articolo 4 della delibera *governance* stabilisce, al comma 1, che "*Con delibera del Consiglio, su proposta del Segretario generale, è approvata la politica di sensibilizzazione, formazione e sviluppo della consapevolezza delle minacce e dei rischi in materia di sicurezza informatica per tutti i soggetti di cui all'articolo 1, comma 2 e per tutto il personale.*" e al comma 2 che "*La politica di cui al comma 1 comprende i percorsi di formazione e sensibilizzazione in materia di sicurezza informatica diversificati in funzione dei relativi destinatari, i relativi programmi di aggiornamento continuo e le eventuali modalità di verifica dell'acquisizione dei contenuti.*";

RAVVISATA, dunque, la necessità di promuovere una solida cultura della sicurezza informatica del personale dell'Autorità, che permetta di acquisire consapevolezza sui rischi informatici e adottare comportamenti adeguati nella quotidianità lavorativa attraverso un'attività di formazione e sensibilizzazione diversificata in funzione dei relativi destinatari, vale a dire il personale che utilizza gli strumenti informatici, il personale che ricopre ruoli specializzati in relazione agli strumenti informatici e il personale che fa parte della struttura amministrativa di cui all'articolo 1, comma 2 della delibera *governance* e che è competente nella gestione del rischio informatico;

VISTA la proposta del Segretario generale;

UDITA la relazione del Commissario Laura Aria, relatore ai sensi dell'articolo 31 del "*Regolamento concernente l'organizzazione ed il funzionamento dell'Autorità*";

DELIBERA

Articolo 1

(Approvazione della Politica per lo sviluppo della consapevolezza sui rischi associati alle minacce informatiche)

1. È approvata la Politica per lo sviluppo della consapevolezza sui rischi associati alle minacce informatiche, descritta nell'allegato alla presente delibera, che comprende (i) il percorso di formazione e sensibilizzazione in materia di sicurezza informatica diversificato in funzione dei relativi destinatari, (ii) i programmi di aggiornamento e (iii) le modalità di verifica dell'acquisizione dei contenuti.

2. Il percorso di formazione e sensibilizzazione sulle minacce e sui rischi in materia di sicurezza informatica, rivolto a tutto il personale dipendente dell'Autorità, è diversificato in funzione dei relativi destinatari, come indicati nelle premesse, ed è accompagnato da un'attività informativa di carattere generale tesa alla diffusione di una cultura in materia di sicurezza informatica.

3. Il Referente per la cybersicurezza verifica periodicamente che il percorso di formazione e sensibilizzazione sia conforme alle disposizioni vigenti e coerente con l'organizzazione interna dell'Autorità e, laddove necessario, propone al Segretario generale gli opportuni aggiornamenti. Il Segretario generale, previa informativa al Consiglio, provvede ad apportare le necessarie modifiche alla Politica per lo sviluppo della consapevolezza sui rischi associati alle minacce informatiche e a pubblicare la versione consolidata.

La presente delibera è pubblicata sul sito *web* dell'Autorità.

Roma, 28 ottobre 2025

IL PRESIDENTE
Giacomo Lasorella

IL COMMISSARIO RELATORE
Laura Aria

Per attestazione di conformità a quanto deliberato
IL SEGRETARIO GENERALE
Giovanni Santella

AGCOM

POLITICA PER LO SVILUPPO DELLA CONSAPEVOLEZZA SUI RISCHI ASSOCIATI ALLE MINACCE INFORMATICHE

Allegato alla delibera n. 259/25/CONS

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

Sommario

Premessa 2

1. Quadro normativo di riferimento 2

2. Criteri per la definizione del percorso formativo e di sensibilizzazione 5

3. Programmi di formazione e attività informativa generale 7

3.1 Formazione di carattere generale per il personale dell'Autorità 7

3.2 Formazione specifica per il personale "tecnico" 7

3.3 Formazione per il personale che fa parte della struttura amministrativa della *governance* 8

3.4 Attività informativa di carattere generale 9

4. Programmi di aggiornamento continuo per il personale 9

4.1 Avvisi sulla sicurezza ("news sicurezza") 9

4.2 Diffusione presso il personale dei rapporti ACN 10

5. Verifica dell'apprendimento del personale 11

5.1 Attacchi simulati con feedback personalizzato – Cyber Guru Phishing 11

5.2 Monitoraggio dell'apprendimento di tutto il personale, ivi incluso quello "tecnico" 11

5.3 Monitoraggio dell'apprendimento per il personale che fa parte della struttura amministrativa della *governance* 11

6. Conclusioni 12

Premessa

Il presente documento ha l'obiettivo di descrivere la Politica per lo sviluppo della consapevolezza sui rischi associati alle minacce informatiche, che comprende il percorso di formazione e sensibilizzazione in materia di sicurezza informatica diversificato in funzione dei relativi destinatari, i programmi di aggiornamento e le modalità di verifica dell'acquisizione dei contenuti.

L'adozione di sistemi tecnologici di protezione rappresenta un presupposto indispensabile, ma non sufficiente, per garantire un adeguato livello di sicurezza. Il fattore umano, infatti, continua a costituire una delle principali fonti di vulnerabilità, in particolare rispetto alle tecniche di *social engineering*, che fanno leva su comportamenti scorretti o inconsapevoli da parte degli utenti.

Per questo motivo, è fondamentale promuovere una solida cultura della sicurezza, che permetta di acquisire consapevolezza sui rischi informatici e adottare comportamenti adeguati nella quotidianità lavorativa.

In tale contesto, formazione e sensibilizzazione assumono un ruolo strategico a tutti i livelli della struttura amministrativa, rappresentando strumenti essenziali non solo per accrescere la consapevolezza rispetto alle minacce legate alla *cybersecurity*, ma anche per orientare l'adozione di pratiche digitali sicure.

Attraverso un percorso, per il personale, formativo e di sensibilizzazione mirato sarà possibile prevenire numerose minacce, agendo direttamente sul fattore umano, spesso identificato come l'anello più debole della catena della sicurezza.

La formazione e la sensibilizzazione saranno calibrate in funzione dei diversi ruoli e delle specifiche esigenze operative del personale, così da fornire un'adeguata preparazione a rispondere in maniera tempestiva e appropriata agli eventuali incidenti informatici. Un tale approccio, infatti, contribuisce a minimizzare i danni derivanti da incidenti di sicurezza, garantire una più rapida ripresa delle attività, rafforzare la resilienza complessiva dell'Autorità e promuovere un comportamento consapevole e responsabile da parte dei dipendenti.

A quanto sopra si aggiunge un'attività di carattere informativo generale per l'Autorità.

1. Quadro normativo di riferimento

Il percorso della formazione e della sensibilizzazione in materia di sicurezza informatica da implementare a carico dei soggetti essenziali è regolato dalla determina ACN n. 164179 del 14 aprile 2025[1], emanata in attuazione del decreto legislativo n. 138/2024[2], recante l'adeguamento della normativa nazionale alla direttiva (UE) 2022/2555 (Direttiva NIS2).

In particolare, la determina ACN n. 164179 specifica le modalità operative per adempiere agli obblighi previsti dagli articoli 23, 24, 25, 29 e 32 del suddetto decreto, fornendo indicazioni concrete sui requisiti minimi relativi alla consapevolezza, sensibilizzazione e formazione del personale in ambito di sicurezza informatica.

L'art. 9 del d.lgs. n. 138/2024 (Strategia nazionale di cybersicurezza) prevede, ai commi 1 e 2, che:

[1] https://www.acn.gov.it/portale/documents/d/guest/detacn_nis_specifiche_2025_164179_signed
[2] https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG

"*1. La Strategia nazionale di cybersicurezza individua gli obiettivi strategici e le risorse necessarie per conseguirli, nonché' adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cybersicurezza.*

2. La Strategia nazionale di cybersicurezza comprende almeno:

[omissis]

f) ***la promozione e lo sviluppo di attività di istruzione, formazione e sensibilizzazione, di competenze e di iniziative di ricerca e sviluppo in materia di sicurezza informatica, nonché' orientamenti sulle buone pratiche e sui controlli concernenti l'igiene informatica, destinati ai cittadini, ai portatori di interessi e ai soggetti essenziali e importanti****;*

[omissis]".

Inoltre, in base all'articolo 23 (Organi di amministrazione e direttivi), comma 2:

"*2.* ***Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali*** *e dei soggetti importanti:*

a) sono tenuti a seguire una formazione in materia di sicurezza informatica;

b) promuovono l'offerta periodica di una formazione coerente a quella di cui alla lettera a) ai loro dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti."

Ai sensi, poi, dell'art. 24 (Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica):

1. I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché' per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.

[omissis]

2. Le misure di cui al comma 1 sono basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché' il loro ambiente fisico da incidenti, e ***comprendono almeno i seguenti elementi****:*

[omissis]

g) ***pratiche di igiene di base e di formazione in materia di sicurezza informatica;***

[omissis]".

Con la determina n. 164179, ACN intende assicurare che i soggetti essenziali adottino misure strutturate e documentate per proteggere i propri sistemi informativi, rafforzando così la resilienza nazionale rispetto alle minacce *cyber*.

In particolare, il paragrafo 3.2 dell'allegato 2 della determina ACN, riguardante la "*Consapevolezza e formazione*", si colloca all'interno della misura PR.AT del *framework* nazionale, ed è strettamente legato al dominio della protezione e preparazione organizzativa. L'obiettivo principale è quello di garantire **che tutto il personale**, a ogni livello, sia consapevole del proprio ruolo nella protezione delle infrastrutture digitali e che riceva una formazione continua e aggiornata in materia di sicurezza informatica. Nel medesimo paragrafo sono altresì

elencate le misure da implementare a carico dei soggetti essenziali, aspetto cruciale della *compliance* con la normativa NIS2.

È fondamentale, infatti, che i soggetti essenziali si assicurino di avere un percorso di formazione e sensibilizzazione adeguato che copra i settori critici, affronti le minacce specifiche e sia parte di un processo continuo di miglioramento.

Passando allo specifico, in base alla **misura PR.AT-01 (paragrafo 3.2.1)**:

"*Il personale* *è sensibilizzato e formato in modo da possedere le conoscenze e le competenze per svolgere compiti di carattere generale tenendo conto dei rischi di cybersecurity.*

1. È definito, attuato, aggiornato e documentato un ***piano di formazione in materia di sicurezza informatica del personale, ivi inclusi gli organi di amministrazione e direttivi****, che comprende almeno:*

a) la pianificazione delle attività di formazione previste con l'indicazione dei contenuti della formazione fornita;

b) le eventuali modalità di verifica dell'acquisizione dei contenuti.

2. Il piano di formazione di cui al punto 1 è approvato dagli organi di amministrazione e direttivi*.*

3. È mantenuto un registro aggiornato recante l'elenco dei dipendenti che hanno ricevuto la formazione di cui al punto 1, i relativi contenuti e l'elenco delle verifiche svolte laddove previste."

Con la misura PR.AT-01, pertanto, **tutto il personale dell'Autorità** deve ricevere formazione e sensibilizzazione su *cybersecurity*, in modo da possedere le conoscenze e competenze necessarie per eseguire compiti generici tenendo conto dei rischi informatici. Elementi chiave della misura PR.AT-01 sono:

- Formazione base su *cyber-hygiene*: *patching*, *password*, protezione credenziali, uso accettabile delle risorse.
- Riconoscimento di attacchi (es. *social engineering*) e segnalazione di anomalie.
- Consapevolezza delle conseguenze di violazioni di *policy*.
- Test periodici sulla comprensione (*test*, simulazioni).
- Aggiornamenti annuali per consolidare o aggiornare le pratiche.

In base alla misura **PR.AT-02 (paragrafo 3.2.2)**:

"*Gli individui che ricoprono ruoli specializzati sono sensibilizzati* *e formati in modo da possedere le conoscenze e le competenze per svolgere i pertinenti compiti tenendo conto dei rischi di cybersecurity.*

1. Il piano di cui alla misura PR.AT-01 prevede una ***formazione dedicata al personale con ruoli specializzati****, ossia che richiedono una serie di capacità e competenze attinenti alla sicurezza, ivi compresi gli amministratori di sistema, che comprende almeno:*

a) le istruzioni relative alla configurazione e al funzionamento sicuri dei sistemi informativi e di rete;

b) le informazioni sulle minacce informatiche note;

c) le istruzioni sul comportamento da tenere in caso di eventi rilevanti per la sicurezza.

2. È mantenuto un registro aggiornato recante l'elenco dei dipendenti che hanno ricevuto la formazione di cui al punto 1, i relativi contenuti e l'elenco delle verifiche svolte laddove previste."

Con la misura PR.AT-02, pertanto, **il personale con ruoli specializzati e privilegiati deve ricevere formazione mirata**, acquisendo conoscenze e competenze specifiche necessarie per svolgere i compiti legati alla posizione rivestita, sempre considerando i rischi informatici. Gli elementi chiave della misura PR.AT-02 sono:

- Identificazione di ruoli specifici che necessitano di formazione avanzata (es. amministratori, IT, sicurezza).
- Addestramento su configurazione sicura di sistemi, procedure operative.
- Test periodici su conoscenze specifiche.
- Preparazione al ruolo in risposta a incidenti e attività forensi.
- Formazione estesa anche a terzi, anche con responsabilità di *governance*.

2. Criteri per la definizione del percorso formativo e di sensibilizzazione

L'Autorità ha sviluppato una strategia formativa organica e strutturata per dare piena attuazione agli obblighi previsti dalla Direttiva NIS2 e dal d.lgs. n. 138/2024.

Questa strategia mira a garantire una formazione continua e costantemente aggiornata sui temi della sicurezza informatica, coinvolgendo attivamente tutti i livelli della struttura amministrativa.

L'obiettivo principale è promuovere una cultura diffusa di consapevolezza del personale – la cosiddetta *cyber awareness* – che favorisca non solo la prevenzione, ma anche una gestione proattiva ed efficace dei rischi digitali.

La definizione del percorso di formazione e sensibilizzazione in materia di sicurezza informatica si basa sui seguenti criteri:

a) Ampiezza dei destinatari

La formazione viene modulata in funzione del livello di esposizione ai rischi e delle responsabilità operative del personale, coinvolgendo:

- Tutto il personale dell'Autorità;
- Il personale "tecnico", vale a dire i soggetti che svolgono attività con accesso privilegiato ai sistemi informativi
- Il personale che fa parte della struttura amministrativa di cui all'articolo 1, comma 2 della delibera n. 204/25/CONS ("delibera *governance*") e che è competente nella gestione del rischio informatico, vale a dire:
  - il Segretario generale;
  - i Vicesegretari generali, ed in particolare il Vicesegretario generale appositamente delegato in materie attinenti alla sicurezza informatica, che opera con funzioni di coordinamento e come sostituto del Punto di Contatto;
  - il Responsabile della cybersicurezza;
  - il Punto di Contatto;

- il Responsabile dell'unità organizzativa di primo livello competente per lo sviluppo e la gestione dell'infrastruttura di rete e dei sistemi informativi (di seguito, anche "Servizio sistemi informativi");
- i Responsabili delle unità organizzative di primo livello, ove gestiscano direttamente sistemi informativi;
- il Responsabile dell'unità organizzativa di primo livello competente in materia di acquisizione di beni strumentali e informatici, di servizi software e dei relativi inventari (di seguito, anche "Servizio risorse umane, strumentali e contratti");
- il Datore di lavoro;
- il Responsabile della protezione dati personali (di seguito, anche "RPD");
- il Designato di primo livello.

b) Tempistica

Il percorso formativo e di sensibilizzazione è sviluppato su un orizzonte biennale (2025-2026) ed è articolato in:

- Sessioni iniziali di formazione (entro il primo semestre 2025).
- Sessioni di aggiornamento.
- Simulazioni periodiche (*phishing*, incidenti simulati).
- Formazione tramite piattaforma fruibile in qualsiasi momento.

c) Efficacia

Per garantire l'efficacia del percorso formativo e di sensibilizzazione, sono adottati i seguenti strumenti:

- Test di valutazione.
- Reportistica sui tassi di partecipazione e apprendimento.
- Simulazioni realistiche (ad es. campagne simulate di *phishing*).

d) Contenuti mirati in base al ruolo

I contenuti formativi sono differenziati sulla base dell'attività svolta e delle connesse responsabilità. In particolare:

- **Formazione base per tutto il personale**: concetti fondamentali di sicurezza, uso sicuro della posta elettronica, gestione delle *password*, riconoscimento delle minacce comuni, conoscenza di *policy* e procedure, consapevolezza delle responsabilità e delle buone pratiche sottese al proprio ruolo professionale, consapevolezza delle minacce e dell'impatto potenziale dei rischi connessi ai comportamenti adottati da ciascun dipendente nel proprio ruolo.
- **Formazione avanzata per il personale "tecnico"**: gestione degli incidenti, *log management*, sicurezza di rete, conoscenza dei metodi, delle tecniche e degli strumenti per poter implementare operativamente misure preventive e contromisure protettive sul

campo, conoscenza approfondita dei fenomeni rischiosi connessi alle piattaforme tecnologiche interne ed esterne al perimetro della propria organizzazione.

- **Formazione specifica per il personale che fa parte della struttura amministrativa della *governance***: aspetti strategici della sicurezza, gestione della *governance* dei processi legati alla *cybersicurezza* all'interno di un quadro normativo nazionale ed europeo in continua evoluzione.

3. Programmi di formazione e attività informativa generale

3.1 Formazione di carattere generale per il personale dell'Autorità

L'Autorità ha acquisito la piattaforma *Cyber Guru Awareness* per il raggiungimento degli obiettivi sopra indicati per la formazione di tutti i dipendenti.

La piattaforma è progettata per supportare la formazione in sicurezza informatica attraverso moduli brevi, interattivi e costantemente aggiornati, pensati per mantenere alto il livello di preparazione del personale.

Inoltre, la piattaforma si aggiorna in modo dinamico per includere le nuove minacce e i rischi emergenti, garantendo così una formazione sempre al passo con l'evoluzione del panorama delle cyberminacce. L'utilizzo di contenuti multimediali innovativi facilita l'attenzione e favorisce un apprendimento graduale e progressivo.

Il modello formativo adottato si fonda sul principio della formazione continua articolata in micro-interventi a cadenza periodica, al fine di mitigare il carico cognitivo degli utenti, migliorare la memorizzazione e il consolidamento delle competenze. Questo approccio garantisce la disponibilità costante di conoscenze aggiornate e specifiche per la gestione efficace delle minacce più rilevanti, quali *phishing* e *spear phishing*, *malware*, *ransomware*, *trojan*, furto di identità digitale e tecniche di *social engineering*.

L'adozione della piattaforma *Cyber Guru Awareness* permette all'Autorità di soddisfare pienamente gli obblighi normativi previsti, fornendo evidenze documentate relative alle attività di formazione e sensibilizzazione del personale, conformemente alle disposizioni dell'ACN.

Questa soluzione, infatti, consente di ridurre il rischio di errore umano, che resta la principale causa di incidenti informatici, e di rafforzare la resilienza promuovendo una cultura diffusa della sicurezza.

3.2 Formazione specifica per il personale "tecnico"

Come già evidenziato, la Direttiva NIS2 stabilisce obblighi specifici per le organizzazioni classificate come soggetti essenziali, in particolare riguardo alla formazione e alla sensibilizzazione del personale "tecnico", vale a dire i dipendenti che svolgono attività con accesso privilegiato ai sistemi informativi.

In questo contesto, il d.lgs. n. 138/2024, all'art. 21, comma 1, lettera b), prevede che "*gli individui che ricoprono ruoli specializzati siano adeguatamente sensibilizzati e formati, acquisendo le conoscenze e le competenze necessarie per svolgere i propri compiti tenendo conto dei rischi legati alla cybersecurity*".

L'obiettivo di questa previsione è assicurare che il personale che svolge funzioni tecniche, quali amministratori di sistema, amministratori di rete e amministratori di *database*, ricevano una formazione specifica e periodica in materia di sicurezza informatica, in linea con le responsabilità assegnate e il profilo di rischio associato al loro ruolo.

Per ottemperare a quanto richiesto dalla normativa, l'Autorità si avvale dei servizi di formazione del progetto "*CyberPro Train: elevating CYBERsecurity PROfessionals by critical infrastructure cybersecurity TRAINing professionals*"[3].

Tale progetto è finanziato dall'Unione Europea con i fondi del *Digital Europe Programme* (DIGITAL), ed offre alle aziende e alla Pubblica Amministrazione corsi altamente specializzati in ambito cybersecurity, usufruibili gratuitamente, a supporto degli obiettivi della Cybersecurity Skills Academy[4].

Il progetto *CyberPro Train* ha un duplice obiettivo:

- Implementare un modello educativo in *cybersecurity* innovativo e scalabile in tre Paesi dell'UE comprendente corsi teorici e pratici gratuiti, formazione pratica e formazione sul campo, da replicare in Europa per contribuire a ridurre la carenza di professionisti qualificati.
- Creare un Manuale Digitale del *CyberPro Train*, sotto forma di una piattaforma *one-stop-shop,* comprendente le migliori pratiche, linee guida, procedure ed esperienze in cybersecurity per l'industria e il pubblico, disponibile in 10 lingue dell'UE, che mira a diventare un punto di riferimento per le PMI e le PA in Europa.

Il corso, progettato da professionisti delle infrastrutture con una conoscenza approfondita delle vulnerabilità e delle sfide più pressanti nell'ambito della *cybersecurity,* fornisce l'aggiornamento, la riqualificazione e la comprensione interdisciplinare della sicurezza informatica per i funzionari pubblici.

I corsi sono erogati in modalità sincrona con docenti specialisti in materia. Successivamente, i corsi già erogati potranno essere seguiti in modalità asincrona poiché resi disponibili sulla piattaforma di *e-learning* e sono suddivisi in base al livello di esperienza.

L'accesso a tali corsi è gratuito per l'Autorità.

3.3 Formazione per il personale che fa parte della struttura amministrativa della *governance*

La Politica per lo sviluppo della consapevolezza in materia di sicurezza informatica viene ulteriormente rafforzata attraverso l'integrazione di un *focus* specifico sulla formazione e, laddove previsto, sulla responsabilità del personale che fa parte della struttura amministrativa della *governance*, in linea con quanto previsto dalla Direttiva NIS2, dal d.lgs. n. 138/2024 e dalla l. n. 90/2024, con l'obiettivo di superare un approccio puramente formale o burocratico alla sicurezza, promuovendo invece un modello di responsabilità attiva e consapevole.

Per il personale che fa parte della struttura amministrativa della *governance*, è previsto un percorso formativo volto a favorire una gestione consapevole e proattiva degli scenari di sicurezza informatica. In questo ambito rientra la partecipazione al *Servizio Cyber Crisis Assessment*, un'attività di valutazione della sicurezza che ha l'obiettivo principale di verificare

[3] EU Funding & Tenders Portal | EU Funding & Tenders Portal: CyberPro Train
[4] EU Funding & Tenders Portal: Cyber Academy

se il livello di preparazione della *governance* di un'organizzazione nel rispondere a un attacco informatico sia sufficiente a garantire continuità operativa e protezione, evitando ulteriori rischi durante la gestione della crisi.

L'attività si sostanzia in una simulazione immersiva presso il *Cyber Theatre della IBM Rome Cyber Academy*, una sala all'avanguardia dove, attraverso un gioco di ruolo, viene testata la capacità di ciascun partecipante di affrontare scenari di crisi. La simulazione utilizza diversi elementi per massimizzare il coinvolgimento e mira a sensibilizzare e preparare i membri della governance ad affrontare rischi di sicurezza informatica.

Al termine della sessione, viene redatto un *report* che evidenzia eventuali lacune organizzative e tecnologiche, fornendo raccomandazioni concrete per migliorare le capacità di risposta e gestione della crisi.

3.4 Attività informativa di carattere generale

Altre iniziative, di carattere generale per l'Autorità, si sostanziano in una generalizzata attività informativa consistente nell'invio trimestrale di dispense tematiche volte a rafforzare la consapevolezza e l'adozione delle buone prassi; trattasi, in particolare di materiale informativo avente ad oggetto:

- approfondimento della conoscenza delle misure di sicurezza previste dalla Direttiva NIS2, con particolare riferimento alla resilienza cibernetica e alla protezione delle infrastrutture critiche;
- approfondimento e applicazione della normativa italiana ed europea in tema di gestione del rischio e sicurezza dei dati.
- riconoscimento dell'attendibilità delle informazioni reperite *online*;

L'iniziativa informativa intende garantire la diffusione di una generale cultura digitale fondata sulla valutazione critica delle fonti e sulla mitigazione dei rischi informativi, reputazionali e di sicurezza, in coerenza con i principi di buona governance e in conformità alla normativa.

4. Programmi di aggiornamento continuo per il personale

I programmi di aggiornamento forniscono una costante informazione sugli sviluppi normativi e operativi nel campo della sicurezza informatica, incrementando la consapevolezza sulle minacce cibernetiche e riducendo i rischi di incidenti o compromissioni.

4.1 Avvisi sulla sicurezza ("news sicurezza")

Una azione strategica e operativa prevede la diffusione regolare di avvisi e comunicazioni informative, denominati "news sicurezza", che hanno l'obiettivo di mantenere il personale costantemente aggiornato sulle principali novità e sulle evoluzioni nel campo della sicurezza informatica. Questi avvisi rappresentano uno strumento strategico per alimentare e rafforzare la cultura della sicurezza all'interno dell'organizzazione, promuovendo un'attenzione continua e condivisa verso i rischi *cyber*.

Le "news sicurezza" includono aggiornamenti sulle minacce emergenti, sulle vulnerabilità recentemente scoperte, sulle campagne di attacco più diffuse e sulle misure preventive

consigliate. Inoltre, queste comunicazioni forniscono indicazioni pratiche e suggerimenti concreti su come riconoscere tentativi di *phishing*, evitare comportamenti rischiosi e adottare abitudini di sicurezza informatica efficaci nella quotidianità lavorativa. La diffusione di tali avvisi avviene attraverso canali di comunicazione interni, come *newsletter*, intranet aziendale, *email,* infografiche, per garantire la massima accessibilità e fruibilità delle informazioni. Questo approccio multicanale consente di raggiungere tutto il personale in modo tempestivo e coinvolgente, stimolando l'interesse e la partecipazione attiva.

Le "news sicurezza" sono pensate per integrare e supportare le altre iniziative formative previste dalla Politica per lo sviluppo della consapevolezza sui rischi informatici, creando un flusso continuo di informazione e consapevolezza che accompagna il personale anche al di fuori delle sessioni di formazione strutturata. Ciò contribuisce a mantenere alta l'attenzione sulle tematiche di sicurezza informatica, favorendo una gestione più consapevole e responsabile del rischio informatico.

Infine, per garantire l'efficacia e l'aggiornamento costante dei contenuti, il materiale delle "news sicurezza" viene elaborato e revisionato dal Servizio sistemi informativi e digitalizzazione, che monitora costantemente il panorama delle minacce e le normative di riferimento, assicurando così che le comunicazioni siano sempre pertinenti, accurate e in linea con le *best practice* internazionali.

4.2 Diffusione presso il personale dei rapporti ACN

Per aumentare la consapevolezza del rischio informatico tra il personale dell'Autorità, si ritiene strategico promuovere la diffusione periodica di rapporti, analisi e aggiornamenti provenienti da fonti ufficiali e autorevoli nel campo della *cybersecurity*.

I contenuti condivisi nell'ambito di questa iniziativa comprendono rapporti [5], avvisi e comunicazioni provenienti da enti di rilievo nel settore della *cybersecurity*, quali l'ACN (Agenzia per la Cybersicurezza Nazionale), il CSIRT Italia (*Computer Security Incident Response Team*) e la Polizia Postale e delle Comunicazioni.

Questi documenti rappresentano una fonte preziosa di aggiornamenti fondamentali riguardanti le minacce informatiche emergenti, gli attacchi reali rilevati sia a livello nazionale che europeo, le vulnerabilità note e le *best practice* da adottare per garantire una sicurezza digitale efficace e aggiornata.

Per garantire una ricezione efficace e una corretta comprensione da parte del personale, la diffusione di tali contenuti avverrà attraverso diversi canali, tra cui *newsletter* e comunicazioni interne tematiche, sessioni informative e aggiornamenti formativi integrativi. Inoltre, saranno introdotti incentivi mirati a favorire la lettura e l'assimilazione dei materiali proposti.

La regolare condivisione di queste informazioni avrà l'effetto di incrementare la consapevolezza del personale sulle minacce cibernetiche, migliorare le pratiche quotidiane di sicurezza digitale e ridurre i rischi di incidenti o compromissioni. In questo modo si contribuirà a rafforzare la resilienza organizzativa agli attacchi informatici, promuovendo una cultura della prevenzione diffusa a tutti i livelli.

[5] https://www.acn.gov.it/portale/w/minaccia-cyber-il-quinto-report-di-acn

5. Verifica dell'apprendimento del personale

La verifica dell'apprendimento si sviluppa attraverso azioni strategiche e operative mirate a garantire la valutazione delle competenze acquisite.

5.1 Attacchi simulati con feedback personalizzato – Cyber Guru Phishing

Il modulo *Phishing* si concentra sulla formazione *anti-phishing* tramite campagne simulate che riproducono scenari di attacco realistici, quali *phishing*, *smishing* e *spear phishing*. Queste simulazioni sono progressivamente calibrate in base al comportamento di ciascun utente e gestite tramite intelligenza artificiale, che adatta automaticamente la difficoltà delle esercitazioni al livello di preparazione dimostrato.

Questo approccio adattivo rende il percorso formativo coinvolgente e realistico, potenziando la capacità degli utenti di riconoscere e contrastare efficacemente le minacce informatiche. Inoltre, agli utenti che risultano vulnerabili nelle simulazioni vengono forniti manuali operativi, spiegazioni dettagliate e suggerimenti mirati per migliorare la loro preparazione.

5.2 Monitoraggio dell'apprendimento di tutto il personale, ivi incluso quello "tecnico"

Con il fine di incrementare la consapevolezza sulle responsabilità e sulle azioni del personale dell'Autorità, al termine di ciascun modulo erogato dalla piattaforma Cyber Guru e del CyberPro Train è previsto un test finale per verificare l'effettiva acquisizione dei contenuti. Il superamento delle prove rappresenta un requisito essenziale per completare con successo l'intero percorso formativo.

Le piattaforme mettono a disposizione report sia individuali sia aggregati, utili a tracciare i progressi della formazione, insieme a *dashboard* periodiche che consentono di misurare il livello di consapevolezza offrendo materiali di supporto per facilitare la redazione dei *report* di conformità normativa.

Per il personale tecnico il progetto formativo offerto da CyberPro Train può essere integrato con le certificazioni CompTIA Security+, EC-Council CEH (Certified Ethical Hacker), EC-Council LPT (Licensed Penetration Tester), GIAC Certified Forensic Analyst (GCFA), CHFI (Computer Hacking Forensic Investigator), selezionate sulla base dell'ambito di applicazione: generale, PT e VA, analisi forense.

5.3 Monitoraggio dell'apprendimento per il personale che fa parte della struttura amministrativa della *governance*

Per il personale che fa parte della struttura amministrativa della *governance* e che usufruisce della simulazione del *Servizio Cyber Crisis Assessment* viene elaborato un *report* che restituisce una fotografia chiara e dettagliata dei risultati ottenuti. Nel documento vengono messi in evidenza i

punti di forza, le criticità emerse e le possibili soluzioni per colmare i *gap* individuati, offrendo così una base concreta su cui costruire i passi successivi.

In particolare, come momento conclusivo di verifica dell'apprendimento, si apre un tavolo di confronto al fine di condividere riflessioni, approfondire le evidenze raccolte e, soprattutto, definire una *roadmap* che accompagni l'organizzazione nel percorso di rafforzamento della propria sicurezza.

6. Conclusioni

La Politica per lo sviluppo della consapevolezza sui rischi associati alle minacce informatiche si configura come una risposta completa e strutturata agli obblighi normativi e agli *standard* internazionali in materia di *cybersecurity*; in particolare, (i) assicura il rispetto di quanto previsto dall'articolo 9 del d.lgs. n. 138/2024, riguardo alla necessità *della promozione e lo sviluppo di attività di istruzione, formazione e sensibilizzazione, di competenze e di iniziative di ricerca e sviluppo in materia di sicurezza informatica, nonché orientamenti sulle buone pratiche e sui controlli concernenti l'igiene informatica, destinati ai cittadini, ai portatori di interessi e ai soggetti essenziali e importanti*; (ii) assicura inoltre il rispetto dell'articolo 23 riguardo alla necessità, per i soggetti essenziali, di *implementare una formazione in materia di sicurezza informatica e promuovere l'offerta periodica di una formazione coerente ai dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti;* da ultimo (iii) assicura il rispetto di implementare ***pratiche di igiene di base e di formazione in materia di sicurezza informatica.***

Integra, inoltre, le *best practice* del *framework* NIST CSF con la misura PR.AT-01 dedicata alla formazione di base per tutto il personale e la PR.AT-02 che prevede un *training* mirato per le funzioni tecniche.

Non meno importante è l'attenzione, nell'ambito della formazione e sensibilizzazione, al comportamento post-incidente, come indicato nella misura relativa alla *Gestione degli incidenti* (RS.MA – paragrafo 5.1) in base alla quale "*Le risposte agli incidenti di cybersecurity rilevati sono gestite*".

Nel complesso, la Politica per lo sviluppo della consapevolezza sui rischi associati alle minacce informatiche rappresenta uno strumento strategico per garantire una cultura della sicurezza diffusa, rafforzare la resilienza organizzativa e adempiere pienamente agli obblighi della Direttiva NIS2, del D.lgs. n. 138/2024 e degli *standard* riconosciuti a livello internazionale.