CESEL
ACADEMY
YOUNG LEADER SCHOOL





MASTERCLASS

PRIVACY E CYBERSECURITY PER PUBBLICHE AMMINISTRAZIONI E PROFESSIONISTI

Rischi concreti, responsabilità e misure di mitigazione

Con test finale

(relatore Dott. Marco Massavelli)

02 Dicembre 2026

ore 09:00 – 13:00

Piattaforma Zoom

PRESENTAZIONE

Al termine del corso i partecipanti saranno in grado di:

1. riconoscere i principali rischi privacy e cybersecurity nelle attività quotidiane;
2. comprendere il collegamento tra GDPR, sicurezza informatica e responsabilità organizzativa;
3. individuare le misure tecniche e organizzative minime da adottare;
4. prevenire errori comuni su email, password, cloud, dispositivi, accessi, fornitori e documenti;
5. sapere cosa fare in caso di violazione dei dati personali o incidente informatico;
6. costruire una piccola checklist interna di controllo.

Il corso si fonda sul principio di **accountability**, cioè sulla necessità di documentare e dimostrare le misure adottate, non solo dichiararle. Il Garante richiama espressamente l'esigenza di misure tecniche e organizzative adeguate e la documentazione delle violazioni di dati personali.

PROGRAMMA

Modulo 1 — Privacy e cybersecurity: perché oggi non si possono più separare

- Differenza tra privacy, protezione dei dati e sicurezza informatica.
- Perché un problema cyber diventa quasi sempre anche un problema privacy.
- Il dato personale come bene da proteggere: dati comuni, dati particolari, dati giudiziari, credenziali, documenti, immagini, log, email.
- Responsabilità di PA e professionisti:
  - titolare del trattamento;
  - responsabile del trattamento;
  - autorizzati/incaricati;
  - amministratori di sistema;
  - fornitori esterni.
- Il concetto di rischio: non basta “avere i documenti privacy”, serve sapere come si lavora davvero.

Rischi trattati

- Trattamenti non mappati.
- Accessi non controllati.
- Documenti privacy formalmente presenti ma non applicati.
- Uso disordinato di email, cloud, WhatsApp, dispositivi personali.
- Mancanza di procedure in caso di incidente.

Modulo 2 — I principali rischi operativi per PA e professionisti

1. Errore umano

L’errore umano resta una delle cause più frequenti di incidenti: invio email al destinatario sbagliato, allegati errati, pubblicazione online di dati non oscurati, perdita di documenti, uso improprio di strumenti digitali.

Misure di mitigazione:

- doppio controllo prima dell’invio di documenti sensibili;
- regole interne sull’uso della posta elettronica;
- oscuramento dei dati non necessari;
- procedure per pubblicazioni su albo pretorio, amministrazione trasparente e siti web;
- formazione pratica con esempi reali.

2. Phishing, smishing e social engineering

I partecipanti imparano a riconoscere:

- email false;
- link malevoli;
- allegati pericolosi;
- messaggi SMS o WhatsApp ingannevoli;
- finte comunicazioni di banche, fornitori, gestionali, cloud, Agenzia Entrate, PEC;
- richieste urgenti del “capo” o del “cliente”.

Misure di mitigazione:

- formazione periodica anti-phishing;
- verifica del mittente;
- divieto di apertura allegati sospetti;
- canale di segnalazione interno;
- autenticazione a più fattori;
- blocco macro e allegati pericolosi;
- simulazioni periodiche.

3. Password deboli e assenza di MFA

Rischio concreto: una sola password rubata può consentire accesso a email, gestionali, fascicoli, cartelle condivise, cloud e dati dei cittadini/clienti.

Misure di mitigazione:

- password uniche e robuste;
- password manager;
- MFA obbligatoria su email, cloud, gestionali e accessi remoti;
- eliminazione account non più usati;
- revisione periodica degli utenti;
- divieto di condivisione delle credenziali.

4. Ransomware e blocco dell'attività

Il ransomware non è solo un problema tecnico: può bloccare uffici, studi professionali, servizi pubblici, pratiche, fatturazione, fascicoli e comunicazioni. ENISA, nel Threat Landscape 2025, ha analizzato migliaia di incidenti nel periodo luglio 2024-giugno 2025 e segnala il peso crescente degli attacchi verso il settore pubblico e delle violazioni di dati nella PA.

Misure di mitigazione:

- backup 3-2-1;
- backup offline o immutabile;
- test periodico del ripristino;
- aggiornamenti software;
- antivirus/EDR;
- segmentazione della rete;
- limitazione privilegi amministrativi;
- piano di continuità operativa;
- piano di risposta agli incidenti.

5. Cloud, condivisioni e lavoro da remoto

Rischi frequenti:

- cartelle condivise con persone non autorizzate;
- link pubblici non controllati;
- ex collaboratori ancora attivi;
- file scaricati su dispositivi personali;
- uso di account privati per attività lavorative;
- mancata cifratura dei dispositivi.

Misure di mitigazione:

- policy cloud;
- accessi nominali;
- revisione periodica delle condivisioni;
- disattivazione immediata degli account cessati;
- cifratura dispositivi;
- VPN o accessi remoti sicuri;
- log degli accessi;
- classificazione dei documenti.

Modulo 3 — GDPR e misure di sicurezza: cosa bisogna davvero fare

- Art. 32 GDPR: sicurezza del trattamento.
- Misure tecniche e organizzative adeguate.
- Riservatezza, integrità, disponibilità e resilienza.
- Privacy by design e by default.
- Minimizzazione dei dati.
- Conservazione limitata.
- Controllo degli accessi.
- Formazione degli autorizzati.
- Gestione dei fornitori.
- Tracciabilità delle attività.

Rischi trattati

- Dati conservati troppo a lungo.
- Accessi non proporzionati.
- Assenza di istruzioni agli autorizzati.
- Fornitori senza nomina o senza verifiche.
- Mancanza di prova delle misure adottate.
- Sistemi non aggiornati.
- Backup mai testati.
- Procedure assenti o solo teoriche.

Misure di mitigazione

- Registro dei trattamenti.
- Analisi dei rischi.
- DPIA quando necessaria.
- Nomine a responsabile del trattamento.
- Lettere di autorizzazione.
- Policy password e accessi.
- Policy data breach.
- Policy conservazione documentale.
- Procedura di offboarding.
- Audit periodici.

Modulo 4 — Data breach e incidenti informatici: cosa fare nelle prime 72 ore

- Differenza tra incidente informatico e violazione dei dati personali.
- Tipologie di data breach:
  - perdita di riservatezza;
  - perdita di integrità;
  - perdita di disponibilità.
- Esempi:
  - email inviata al destinatario sbagliato;
  - furto di laptop;
  - ransomware;
  - accesso abusivo alla casella email;
  - pubblicazione online di dati non oscurati;
  - perdita di fascicoli o documenti.
- Valutazione del rischio per gli interessati.
- Quando notificare al Garante.
- Quando comunicare agli interessati.
- Registro interno delle violazioni.

Misure di mitigazione

- procedura data breach scritta;
- team interno di gestione incidente;
- contatti rapidi: IT, DPO, legale, responsabile interno;
- modulo interno di segnalazione;
- registro data breach;
- simulazione annuale;
- backup testati;
- log conservati;
- catena decisionale chiara.

Esercitazione pratica

Scenario: un dipendente apre un allegato malevolo, la postazione viene cifrata e alcuni file condivisi diventano inaccessibili.

I partecipanti devono individuare:

7. cosa fare nei primi 30 minuti;
8. chi avvisare;
9. quali informazioni raccogliere;
10. se può esserci un data breach;
11. quali misure documentare;
12. quali errori evitare.

Modulo 5 — NIS2, supply chain e sicurezza organizzativa

- Perché la cybersecurity non riguarda solo l’ufficio IT.
- La catena dei fornitori come punto debole.
- Gestionali, cloud provider, consulenti, manutentori, software house, società IT.
- Obblighi e buone pratiche ispirate alla normativa NIS2.
- Continuità operativa e gestione del rischio.

Rischi trattati

- Fornitore compromesso.
- Software non aggiornato.
- Assistenza remota non controllata.
- Mancanza di contratti e istruzioni.
- Assenza di verifica sulle misure del responsabile.
- Nessun piano di continuità.
- Nessun inventario degli asset.

Misure di mitigazione

- elenco aggiornato dei fornitori critici;
- nomine privacy corrette;
- clausole di sicurezza nei contratti;
- verifica periodica dei fornitori;
- gestione sicura degli accessi remoti;
- inventario di hardware, software, cloud e banche dati;
- classificazione dei servizi essenziali;
- piano di continuità e ripristino;
- procedure di escalation.

Modulo 6 — Checklist finale: le 15 misure da adottare subito

Le 15 misure operative

13. Aggiornare il registro dei trattamenti.
14. Verificare chi ha accesso a cosa.
15. Attivare MFA su email, cloud e gestionali.
16. Eliminare account non più utilizzati.
17. Usare password manager.
18. Aggiornare sistemi, software e dispositivi.
19. Proteggere endpoint e dispositivi mobili.
20. Eseguire backup regolari e testare il ripristino.
21. Limitare le condivisioni cloud.
22. Formalizzare autorizzazioni e istruzioni agli incaricati.
23. Nominare correttamente i fornitori.
24. Predisporre procedura data breach.
25. Definire tempi di conservazione dei dati.
26. Fare formazione periodica.
27. Documentare controlli, verifiche e decisioni.

DOCENTE

Dott. Marco Massavelli dott. Marco Massavelli – Consulente, esperto e formatore GDPR, cybersecurity, AI – DPO – CISO – già Comandante Polizia Locale

PARTNER SOCIALE

GEFIL srl

SOFTWARE PER
GLI ENTI LOCALI

STRUTTURA

Corso da remoto in modalità sincrona con possibilità di differita.

DATE E ORARI

02 Dicembre 2026 dalle ore 09:00 alle ore 13:00

QUOTA DI PARTECIPAZIONE

A) Una iscrizione.....€. 90,00 (Cod. Me.Pa. n. AF106/2026)
B) Due iscrizioni.....€. 160,00 (Cod. Me.Pa. n. AF107/2026)
C) Tre iscrizioni e più (a partecipante).....€. 70,00 (Cod. Me.Pa. n. AF108/2026)

N.B. GLI ENTI LOCALI SONO ESENTI DA IVA AI SENSI ART.14 COMMA 10 LEGGE 24/12/1993 N. 537
Bollo a carico nostro - Privati e aziende aggiungere il 22% di IVA

*Alla fine del corso verrà inviato un **attestato di partecipazione nominativo con indicazione delle ore e l'aver superato il test finale anche al fine di garantire le progressioni verticali,** materiale didattico e la possibilità di avere il tutoraggio post-corso (con iscrizione gratuita alla nostra news-letter).*

PER INFORMAZIONI ED ISCRIZIONI RIVOLGERSI:

CE.S.E.L. – Segreteria Didattica tel. 0922.511033 mob. 328.6729362
e-mail segreteria@ceselformazione.it associazionecesel@pec.it
www.ceselformazione.it

WEBINAR

PRIVACY E CYBERSECURITY PER PUBBLICHE AMMINISTRAZIONI E PROFESSIONISTI

02 Dicembre 2026

PIATTAFORMA ZOOM

Cognome e nome……

Settore……comune di……..Prov……..

Professione…….. ordine di……..

Tel…….. Cell……email……..

DATI PER LA FATTURAZIONE:

Ragione sociale ……

Indirizzo…….CAP……Città……..

P.I./…….. C.F……

CODICE UNIVOCO……

SCEGLIERE OPZIONE A / B / C =……..

Totale Complessivo €. ……..

1) MODALITA' DI PAGAMENTO

Il pagamento deve essere effettuato a fine corso previo Ns presentazione fattura elettronica :

- **BONIFICO BANCARIO a favore di:**

Associazione CE.S.E.L. – Corso Francesco Crispi, 137 - San Giovanni Gemini (AG)

P.IVA: 02750650844 C.F.: 93068110845 CODICE UNIVOCO M5UXCR1

Banca CREDEM iban: IT 17 C 03032 83120 010000003499 - Indicando nella causale numero di fattura/anno.

Inviare scheda compilata e determina per le pubbliche amministrazioni e scheda compilata e copia bonifico per privati e aziende) a: **segreteria@ceselformazione.it**

2) I dati del partecipante compreso immagini video (diretta-webinar e in differita) verranno trattati come previsto dal nuovo regolamento europeo sulla privacy UE 2016/679.

FIRMA PRIVATO E/O TIMBRO E FIRMA DEL RESPONSABILE DI SETTORE……

Dichiaro di ricevere copia del seguente contratto conforme all'originale, di aver letto ed accettato le clausole di cui ai numeri: 1)2) ai sensi ed agli effetti degli artt. 1341-1342 c.c.

FIRMA PRIVATO E/O TIMBRO E FIRMA DEL RESPONSABILE DI SETTORE……..

LUOGO E DATA……..

CE.S.E.L.
SCUOLA DI GOVERNO LOCALE