*Centro Studi Paul H. Appleby*
*per l'Etica e l'Amministrazione Democratica | www.appleby.it*

CORSO DI FORMAZIONE

# Attaccati. E adesso?

*Cybersecurity pratica per Comuni, Unioni e piccoli Enti Pubblici*

Riconoscere le minacce, applicare le misure minime, reagire con metodo

| | |
|---|---|
| **Ente organizzatore** | Centro Studi Paul H. Appleby per l'Etica e l'Amministrazione Democratica — www.appleby.it |
| **Docente** | Dott. Antonio Fiorentino — Ispettore Polizia di Stato, esperto di digital forensics e cybersecurity |
| **Durata totale** | 2 ore \| 10:00 – 12:00 (90 min. lezione + 25 min. Q&A aperto + 5 min. pausa) |
| **Formato** | Lezione frontale + sessione Q&A guidata |
| **Destinatari** | Responsabili IT, segretari comunali, funzionari e amministratori di Comuni, Unioni di Comuni, Comunità Montane e piccoli Enti Locali |
| **Livello** | Introduttivo / Intermedio |

## 1. Obiettivi del Corso

Il corso nasce per rispondere a una domanda concreta: **cosa deve fare un piccolo ente pubblico per non farsi trovare impreparato?** Al termine i partecipanti saranno in grado di:

- ✓ Riconoscere le minacce più frequenti che colpiscono Comuni e Enti Locali
- ✓ Comprendere cosa prevede la normativa per la PA (AgID, ACN, NIS2)
- ✓ Applicare le Misure Minime di Sicurezza ICT con risorse limitate
- ✓ Gestire un incidente informatico: chi avvisare, cosa fare, come documentare
- ✓ Costruire comportamenti sicuri nella gestione quotidiana di dati e dispositivi

## 2. Agenda Oraria

| Orario | Attività / Argomento | Docente | Min. |
|---|---|---|---|
| **10:00 – 10:10** | Apertura, presentazioni e obiettivi del corso | *A. Fiorentino* | **10'** |
| **10:10 – 10:30** | Modulo 1 — Fondamenti e panorama delle minacce | *A. Fiorentino* | **20'** |
| **10:30 – 10:55** | Modulo 2 — Principali vettori di attacco | *A. Fiorentino* | **25'** |
| **10:55 – 11:15** | Modulo 3 — Difese, strumenti e best practice | *A. Fiorentino* | **20'** |
| **11:15 – 11:30** | Modulo 4 — Misure Minime di Sicurezza ICT (AgID) | *A. Fiorentino* | **15'** |
| | ***— PAUSA BREVE (5 minuti) —*** | | |
| **11:35 – 12:00** | Sessione Q&A aperta — Domande libere dai partecipanti | *A. Fiorentino* | **25'** |
| **TOTALE** | **10:00 – 12:00 \| 90 min. lezione + 25 min. Q&A + 5 min. pausa** | | **120'** |

## 3. Contenuto dei Moduli

### M1 Fondamenti e Panorama delle Minacce — 20 minuti

- Cos'è la cybersecurity: definizioni e perimetro — *CIA triad, riservatezza, integrità, disponibilità*
- Evoluzione del threat landscape — *dai virus degli anni '90 al ransomware-as-a-service*
- Tipologie di attaccanti — *script kiddie, cybercriminali organizzati, APT, insider threat*
- Statistiche e casi reali recenti — *incidenti italiani ed europei di rilievo*
- Concetto di superficie di attacco — *endpoint, cloud, supply chain, IoT*

### M2 Principali Vettori di Attacco — 25 minuti

- Phishing, spear phishing e Business Email Compromise (BEC) — *esempi pratici e indicatori di allarme*
- Malware: ransomware, spyware, trojan, worm — *modalità di diffusione e impatto*
- Social engineering e pretexting — *manipolazione cognitiva e tecniche di difesa*
- Vulnerabilità software e patch management — *CVE, CVSS, zero-day*
- Attacchi alle password — *brute force, credential stuffing, MFA bypass*
- Minacce in ambienti cloud e mobile — *misconfiguration, shadow IT, BYOD*

| M3 | Difese, Strumenti e Best Practice | 20 minuti |
|---|---|---|

› Autenticazione multi-fattore (MFA) e gestione delle credenziali — *password manager, policy aziendali*
› Backup e disaster recovery — *regola 3-2-1, RPO/RTO*
› Navigazione sicura e protezione delle email — *antispam, DMARC/SPF/DKIM, sandboxing*
› Segmentazione di rete e principio del minimo privilegio — *Zero Trust Architecture*
› Incident response: cosa fare in caso di attacco — *escalation, comunicazione, forensics di primo livello*
› Cultura della sicurezza e security awareness — *il fattore umano come prima linea di difesa*

| M4 | Misure Minime di Sicurezza ICT per le PA (AgID/ACN) | 15 minuti |
|---|---|---|

*Le Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni (Circ. AgID n. 2/2017) definiscono tre livelli di adeguamento obbligatorio — **Minimo, Standard, Avanzato** — articolati in 15 controlli (ABSC) derivati dal framework CIS Controls.*

› ABSC 1 — Inventario dei dispositivi autorizzati e non autorizzati — *asset management attivo e passivo*
› ABSC 2 — Inventario dei software autorizzati e non autorizzati — *application whitelisting, software non approvati*
› ABSC 3 — Protezione delle configurazioni hardware e software — *hardening, configurazioni sicure di default*
› ABSC 4 — Valutazione e correzione continua delle vulnerabilità — *vulnerability scan periodici, patch management*
› ABSC 5 — Uso appropriato dei privilegi di amministrazione — *least privilege, account dedicati per admin*
› ABSC 7 — Protezione dai malware — *antimalware aggiornato, controllo dispositivi rimovibili*
› ABSC 8 — Difese perimetrali e filtraggio del traffico — *firewall, IDS/IPS, proxy, DNS filtering*
› ABSC 10 — Copie di sicurezza (backup) — *regola 3-2-1, cifratura dei backup, test di ripristino*
› ABSC 13 — Protezione dei dati — *cifratura a riposo e in transito, DLP*
› ABSC 17 — Formazione e sensibilizzazione del personale — *security awareness, phishing simulation*

Livello **Minimo** = obbligatorio per tutte le PA | **Standard** = raccomandato | **Avanzato** = per PA ad alta esposizione al rischio

## 4. Sessione Q&A — Domande Aperte

### 11:35 – 12:00 | Q&A Aperto (25 minuti)

La sessione finale è aperta e libera: i partecipanti possono porre qualsiasi domanda emersa durante il corso o legata alla propria esperienza professionale. Il docente risponde in modo diretto, anche su casi reali (nel rispetto della riservatezza), stimolando il confronto tra pari.

**Modalità consigliate per raccogliere le domande:**

- Intervento spontaneo dall'aula

*Non sono previste domande prestabilite: la qualità della sessione è generata dall'interazione autentica tra docente e partecipanti.*

## 5. Profilo del Docente

**Dott. Antonio Fiorentino**

*Ispettore della Polizia di Stato*

Sezione Operativa Sicurezza Cibernetica

**Specializzazioni**

Digital Forensics
Hacking Aziendale
Financial Crimes
Incident Response
Notifiche CSIRT ACN (NIS2)

*linkedin.com/in/antonio-fiorentino-0726b124*

Il Dott. Antonio Fiorentino opera dal 2008 come esperto di digital forensics e sicurezza dei sistemi informativi. Laureato in Giurisprudenza presso l'Università degli Studi di Parma (2006), è Ispettore della Polizia di Stato in servizio presso la Sezione Operativa Sicurezza Cibernetica, con responsabilità diretta sulla gestione delle notifiche CSIRT ACN degli incidenti informatici delle aziende NIS2 di Brescia e provincia.

Nel corso della propria carriera ha collaborato con diverse Procure della Repubblica in qualità di consulente tecnico, portando competenze di digital forensics su procedimenti penali di rilievo. È perfezionato e accreditato in digital forensics, cybersecurity e gestione degli incidenti informatici presso l'Università degli Studi di Milano.

### Attività accademica e formativa

- Docente a contratto presso l'Università Cattolica del Sacro Cuore di Brescia
- Collaboratore didattico, Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Brescia
- Formatore per dipendenti pubblici e privati, CDA aziendali: Distretto della Corte di Appello di Brescia, Polizia Locale di Brescia e Bergamo, Questura di Brescia, istituti bancari, aziende

## 6. Ente Organizzatore

### Centro Studi Paul H. Appleby

*per l'Etica e l'Amministrazione Democratica*

Il Centro Studi Paul H. Appleby è un think tank indipendente dedicato alla promozione della qualità democratica, dell'etica pubblica e dell'innovazione responsabile nella Pubblica Amministrazione italiana. Le sue attività spaziano dalla ricerca applicata alla formazione specialistica, con un focus su trasformazione digitale, intelligenza artificiale nella PA, trasparenza amministrativa e governance democratica degli enti locali.

**Sito web:** www.appleby.it
**LinkedIn:** linkedin.com/company/centro-studi-paul-h-appleby
**YouTube:** youtube.com/@CS-Appl3by