Open
ADVISOR STP

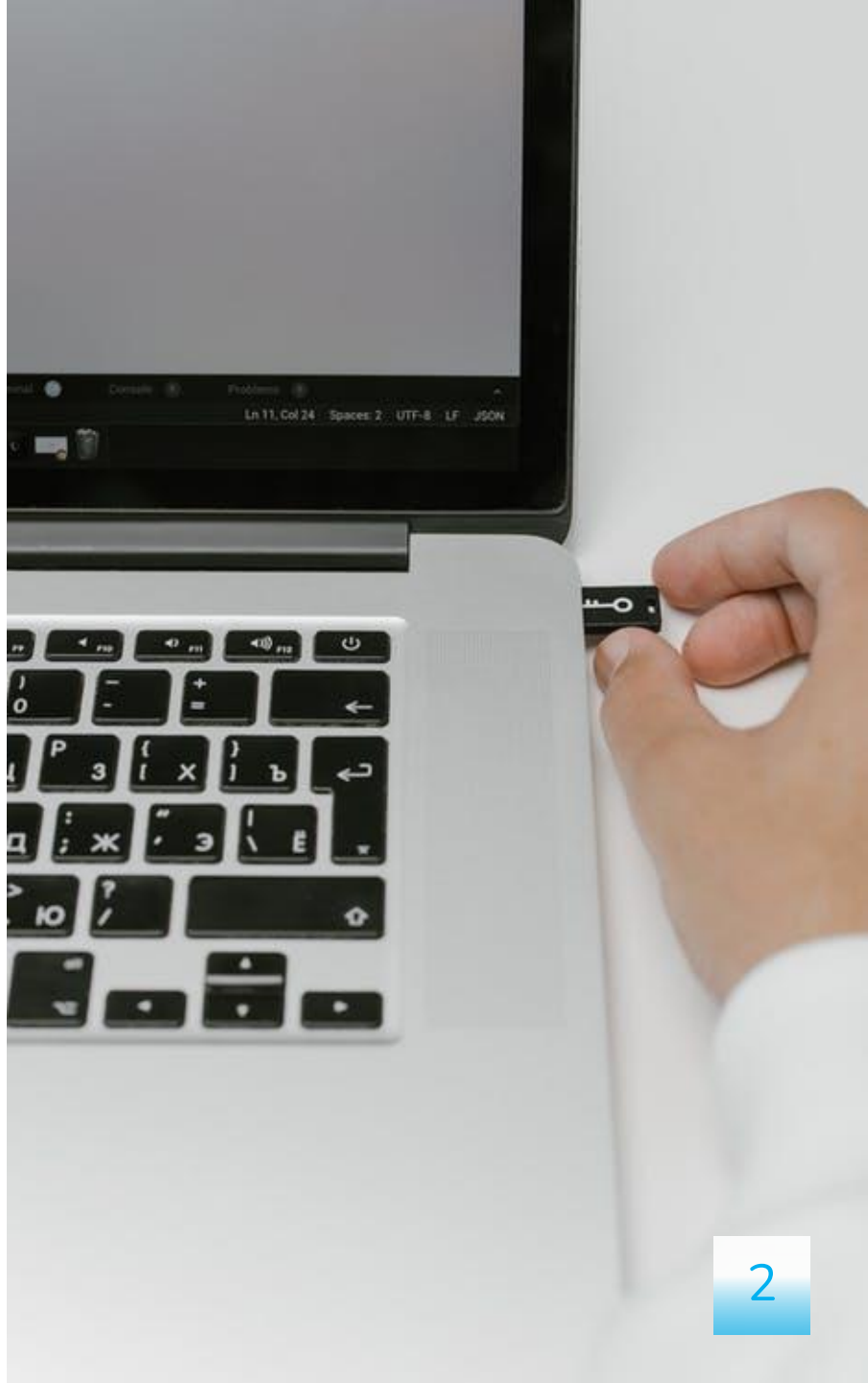
CYBERSECURITY

Le nuove minacce degli attacchi informatici e degli incidenti alle nostre imprese

PRESENTAZIONE STRUTTURA ED ELEMENTI DEL CORSO

Gli **attacchi informatici** sono **in costante aumento** sia in termini quantitativi sia qualitativi e hanno ad oggetto soprattutto infrastrutture, servizi web aziendali, servizi e fornitori

Il percorso formativo è finalizzato a sensibilizzare il personale sui rischi (Risk management), sulle misure organizzative e tecniche per prevenire e contrastare gli incidenti di sicurezza e le violazioni dei dati e a illustrare le ultime novità normative, le sanzioni e le responsabilità in materia.



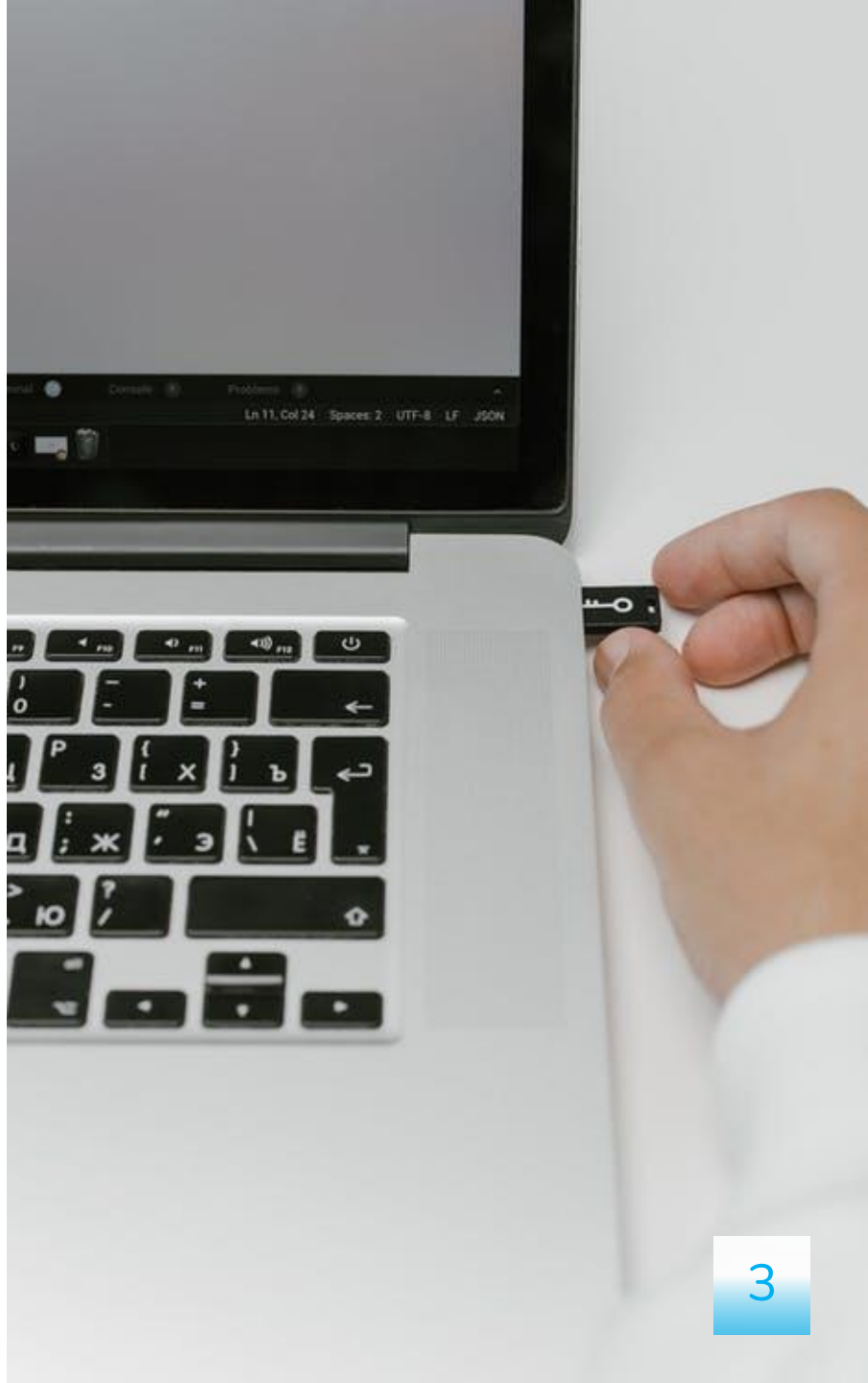
+Open ADVISOR STP

PRESENTAZIONE STRUTTURA ED ELEMENTI DEL CORSO

I **docenti** sono esperti in materia (docenze presso Master universitari ed Enti accreditati alla Regione) e hanno affrontato sia casi di sanzioni da parte dell'autorità Garante sia gestione di numerosi data breach.

Il corso ha un taglio operativo in un'ottica di forte interazione con la classe, un addestramento al personale per diminuire la vulnerabilità, in ottica di sensibilizzazione ed efficacia.

Nel rispetto del principio di accountability e a tutela delle nostre imprese, sono previste anche **esercitazioni** e **test**.



+Open ADVISOR STP

PRIVACY-GDPR UE

Artt. 29, 32 e 39 GDPR

1. **La formazione sulla cybersecurity è obbligatoria nel modello organizzativo previsto dal GDPR:** nessuno può trattare dati se non è istruito in tal senso.

2. **Necessaria per rispettare l'accountability:** il titolare deve essere in grado di dimostrare di aver formato i soggetti autorizzati al trattamento dei dati.

3. **Prerequisito per il trattamento dati:** finalizzata a illustrare i rischi generali e specifici dei trattamenti di dati, le misure organizzative, tecniche e informatiche adottate, nonché le responsabilità e le sanzioni.

4. **Nei controlli è richiesta l'evidenza documentale** dei corsi svolti in materia.

5. **La sanzione può arrivare fino a 10 Mln di euro**, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

INDICE ARGOMENTI

1° SESSIONE

1. Cybersecurity: definizione e nozione

2. Le conseguenze economiche per le aziende: non solo dati personali, gli attacchi e gli incidenti che "bloccano/inchiodano" le aziende (analisi di casi avvenuti di recente)

3. Risk management: il rischio cyber per le nostre imprese alla luce dei dati europei e nazionali (rapporti Clusit e Censis)

4. La strategia europea e nazionale in materia di prevenzione e contrasto del cybercrime, il ruolo dell'Agenzia della Cybersicurezza nazionale

5. **Le tipologie di attacchi (Cryptolocker, Ransomware, phishing, whaling, malware, spear-phishing, revenge porn)**

6. **Reputation: I costi dei data breach, i danni reputazionali degli attacchi e degli incidenti informatici**

7. **Il ruolo della formazione: riconoscere le minacce e i malfunzionamenti, come proteggere reti e dati, gli attacchi informatici e data breach, il ruolo delle policy**

8. **Il ruolo della compliance (interazioni tra normative): la crisi d'impresa, la 231 e il GDPR e i Modelli di prevenzione**

9. **Sanzioni: le conseguenze del mancato assetto organizzativo e le sanzioni e ispezioni del Garante GPDP**

10. **Best practice:** l'addestramento alla minaccia per ridurre la vulnerabilità, la gestione delle password e degli account, cose da fare e da non fare nel caso di attacchi, le regole per la gestione del data breach e la nuova piattaforma on line per le segnalazioni dei data breach del GPDP.

2° SESSIONE

1. L'Information Security per la protezione dei dati e dell'infrastruttura informatica
2. L'Industrial Security per la protezione dei dispositivi di produzione
3. Navigazione Internet: Browser, cookies e Web (in chiaro, Deep e Dark Web)
4. Tipologie di attacchi: Man in the middle, Phishing, Malware, Ransomware, Ddos
5. Governance, compliance e policies per la sicurezza informatica

6. Le protezioni di base ed avanzate (password, Anti-virus, VPN, FireWall, Siem e software Web Protection)

7. Penetration Testing e Vulnerability Assessment

- **L’esperienza sul campo: testimonianze e casi concreti**
- **Esercitazione collettiva e test: presentazione di un caso di data breach**

MODALITA' DI EROGAZIONE

CORSO DI FORMAZIONE

1. **Durata e costi del corso**: parametrati su criteri tecnici, quali il n. dei dipendenti, le esigenze aziendali, e la disponibilità di Fondi Interprofessionali.

2. **Credito formazione 4.0**: con il Decreto Aiuti 2022: **dal 30% al 70% dei costi orari** per le ore dei dipendenti partecipanti e dei docenti interni qualificati; **il 100% del costo della docenza esterna**, se affidata ad Enti accreditati o formatori certificati UNI EN ISO 9001:2015 - EA37.

    - **Spese di personale** dei formatori accreditati/tutor e docenti interni perle ore di formazione.
    - **Costi di esercizio** (spese di viaggio, materiali, forniture attinenti al progetto).
    - Costi di **servizi di consulenza** connessi al progetto di formazione.
    - Spese di personale relative ai **partecipanti** e spese generali indirette (amministrative, di locazione).
    - Spese di **certificazione contabile** (per le imprese non soggette a obbligo di revisione) → extra credito fino a 5.000,00 €.

3. **Formazione finanziata**: pagamento del costo della docenza esterna mediante i Fondi Interprofessionali.

+Open
ADVISOR STP

www.opengroupitalia.it
+39 011 6970046
sviluppo@opengroupitalia.it