

# **RICHIESTA AIPSI DI PATROCINIO GRATUITO OAD 2025**

**GENNAIO 2025**  
*(agg. 12/03/2025)*

## Sommario

1. L'iniziativa OAD .....	3
2. OAD 2025 .....	5
2.1. Il questionario OAD 2025 .....	6
2.2 Il Rapporto OAD 2025 .....	7
2.3 Le fasi di OAD 2025 .....	8
3. Il patrocinio gratuito di OAD 2025 .....	9
3.1 Perché conviene patrocinare OAD 2025 .....	10
3.2. Gli obblighi dell'Associazione patrocinante .....	10
4. La proprietà intellettuale di OAD 2025 .....	11
5. Come aderire al gratuito patrocinio di OAD 2025 .....	11
<i>AIPSI, Associazione Italiana Professionisti Sicurezza Informatica</i> .....	12

## 1. L'iniziativa OAD

L'iniziativa OAD, Osservatorio Attacchi Digitali in Italia (chiamata fino al 2015 OAI, Osservatorio Attacchi Informatici in Italia), nel 2025 arriva a 18 anni consecutivi di indagini sugli attacchi intenzionali digitali e sulle misure di sicurezza in essere nei Sistemi Informativi di aziende e Pubbliche Amministrazioni operanti in Italia. L'indagine OAD in tutti questi anni è stata operativamente realizzata da **Malabo Srl** ([www.malaboadvisoring.it](http://www.malaboadvisoring.it)), la società di consulenza direzionale sull'ICT (Information and Communication Technologies) che implementa l'indagine online, elabora i dati raccolti e stende il rapporto finale, sotto la guida di **AIPSI**, Associazione Italiana Professionisti Sicurezza Digitale, capitolo italiano di ISSA ([www.aipsi.org](http://www.aipsi.org), [www.issa.org](http://www.issa.org)), che imposta e supporta l'iniziativa, pubblica il rapporto finale dell'indagine e ne garantisce la qualità e l'indipendenza dell'analisi e dei contenuti anche dagli Sponsor.

OAD è l'**unica** iniziativa in Italia realizzata con una indagine anonima indirizzata a tutte le aziende, di ogni settore merceologico e dimensione, **e alle Pubbliche Amministrazioni** tramite un questionario on line con risposte preimpostate e compilabile con ogni moderno browser.

Il questionario è rivolto tipicamente ai Responsabili dei Sistemi Informatici (CIO), agli Amministratori di sistema, ai Responsabili della Sicurezza Informatica (CISO), alle Terze Parti che gestiscono la sicurezza digitale di loro clienti, e per le piccole e piccolissime organizzazioni ai responsabili di vertice che decidono sul sistema informativo e la sua sicurezza.

Obiettivo principale dell'iniziativa OAD è di analizzare **l'effettiva realtà del fenomeno degli attacchi digitali intenzionali** ai sistemi informativi di aziende ed enti pubblici in Italia, oltre che delle **misure di sicurezza in essere**, tramite un'indagine online anonima, indipendente, autorevole e liberamente accessibile da ogni persona che nel suo ambito lavorativo, pubblico o privato, a tempo pieno o parziale, opera e/o decide nell'ambito della sicurezza digitale; e di far conoscere tale realtà il più ampiamente possibile, per contribuire alla creazione in Italia di una vera e propria "cultura" della sicurezza digitale soprattutto nell'ambito di chi decide sui sistemi informati e più in generale sul mondo digitale.

La disponibilità di corrette informazioni "locali all'Italia" sugli attacchi digitali intenzionali rilevati, sulla tipologia e sull'ampiezza del fenomeno, sulle principali misure di sicurezza digitale, sia tecniche sia organizzative, risulta fondamentale per la crescita della conoscenza su queste tematiche, sulla già citata creazione di una "cultura" diffusa in merito, e di un **concreto ausilio**, soprattutto per le organizzazioni di piccole dimensioni, nella valutazione dei rischi digitali e nella scelta delle misure più idonee di prevenzione e protezione da attivare sui loro sistemi, così come richiesto da numerose normative nazionali ed internazionali, in primis il GDPR, il regolamento europeo per la privacy.

L'iniziativa OAD contribuisce infatti alla "sensibilizzazione" e alla conoscenza in Italia della sicurezza digitale per tutti gli utenti ed i decisori dei sistemi informativi, che è uno degli obiettivi di AIPSI e di ISSA (si veda <https://www.issa.org/about-issa/> e <https://www.aipsi.org/associazione/perche-aipsi.html>). Conoscenza e sensibilizzazione ancora scarse in Italia, come anche evidenziato dagli indici dell'indagine europea DESI (si veda <https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts>). Per la sua importanza in termini di comunicazione, sensibilizzazione e formazione sulla cybersecurity, il progetto **OAD** fa parte dell'iniziativa strategica nazionale **Repubblica Digitale** <sup>1</sup> come evidenziato in <https://repubblicadigitale.innovazione.gov.it/it/i-progetti/>.

---

<sup>1</sup> Iniziativa strategica nazionale promossa dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri nel quadro della strategia "Italia 2025": ha l'obiettivo di combattere il divario digitale di carattere culturale presente nella popolazione italiana, per sostenere la massima inclusione digitale e favorire l'educazione sulle tecnologie del futuro, accompagnando il processo di trasformazione digitale del Paese (si veda: <https://repubblicadigitale.innovazione.gov.it/it/il-programma/>)

Tredici i rapporti annuali OAD/OAI che sono stati pubblicati (le loro copertine in fig. 1) e che coprono i sedici anni consecutivi di indagini online effettuate sugli attacchi rilevati dal 2007 al 2023: l'anno del Rapporto fa riferimento all'indagine effettuata per il rilevamento degli attacchi subiti e rilevati nell'anno precedente.

I più recenti rapporti OAD hanno un "executive summary" in italiano e in inglese.

Tutti i rapporti OAI/OAD sono scaricabili gratuitamente dallo specifico sito creato per questa iniziativa, <https://www.oadweb.it/>. Una parte del sito, pur ridotta rispetto a quella italiana, è in inglese: <https://www.oadweb.it/en/>. In questo sito è archiviata e resa disponibile a chi è interessato tutta la documentazione (in taluni casi anche la videoregistrazione) dei vari eventi, organizzati da AIPSI o ai quali ha partecipato, dove sono stati presentati e discussi i dati emersi dalle indagini OAD.

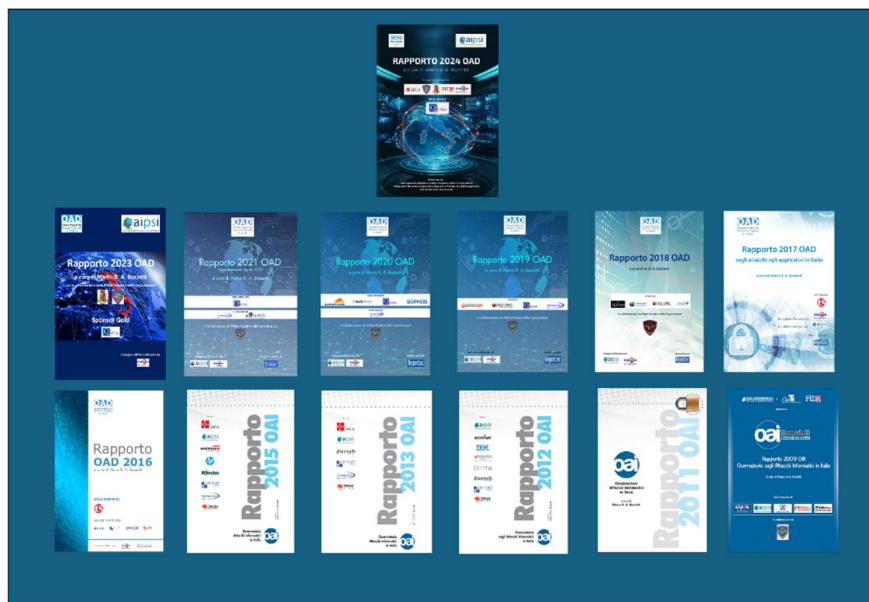


Fig. 1 Le copertine dei Rapporti OAD-OAI finora pubblicati

I potenziali rispondenti al questionario OAD sono informati dell'indagine ed invitati a compilare i questionari, come per le indagini precedenti, tramite i vari canali di comunicazione (siti web, eventi, social net, e-mail, articoli e banner, ...) di AIPSI, delle associazioni patrocinanti e degli Sponsor.

Nelle precedenti edizioni, il numero di possibili rispondenti contattati è stimato nell'ordine delle 5.000 persone, appartenenti per lo più al mondo delle aziende, dei servizi, degli studi professionali e delle Pubbliche Amministrazioni.

Il numero di rapporti scaricati dal sito OAD o distribuiti via posta elettronica, file transfer, condivisione di file, etc. sono andati man mano crescendo negli anni, fino a raggiungere negli ultimi tre anni un numero per edizione **superiore ai 3000**. Questo dato è fornito dal preciso numero di download effettuati dai siti aipsi.org e oadweb.it, e non tiene conto dell'inoltro diretto del Rapporto finale OAD ad interessati da parte di Sponsor, Patrocinatori e di chi lo aveva già scaricato. Stimando anche questi inoltri, è ragionevole stimare che il Rapporto sia stato diffuso, nelle ultime edizioni, **a più di 5000 persone**. Per quanto riguarda, ad esempio, il

Rapporto OAD 2024, alla data si sono rilevati **4040** download tra il sito web di AIPSI e quello di OAD, un numero significativo dovuto alla possibilità di scaricarlo senza dover fare prima il login al sito, e quindi essere registrato. Anche per OAD 2025 si potrà scaricare il rapporto finale, che sarà disponibile sul sito di AIPSI e di OAD, senza doversi registrare.

## 2. OAD 2025

L'indagine OAD 2025 sarà simile alla precedente edizione, con un **questionario ridotto e semplificato** così da ridurre il tempo necessario a compilarlo, pur mantenendo significativi i contenuti per l'analisi del fenomeno attacchi digitali intenzionali nell'ambito business e garantire una continuità con le principali informazioni raccolte nelle precedenti indagini.

Per tali motivi il **questionario online**, rigorosamente anonimo, di OAD 2025:

- conterrà due sole domande sugli attacchi rilevati nel 2024 in riferimento alle tipologie di attacco ed alle famiglie di tecniche di attacco così da poter avere dati di trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 al 2024;
- le domande di approfondimento riguarderanno gli attacchi subiti nel **2024** ai **siti e agli ambienti web**, **alle applicazioni basate su Intelligenza Artificiale**, **ed agli ambienti OT, Operational Technology**;
- **saranno opzionali** le domande sulle **misure di sicurezza digitale** presenti nei sistemi informativi oggetto delle risposte.

Le prime due domande sugli attacchi subiti sarà obbligatoria per tutti i rispondenti: per chi non avesse rilevato attacchi, le domande relative verranno automaticamente saltate grazie all'applicazione che supporta il questionario online, basata su una specifica configurazione del software opensource Limesurvey.

Saranno obbligatorie anche le domande inerenti la tipologia di azienda/ente a cui appartiene il Sistema Informativo oggetto delle risposte, i futuri attacchi più temuti, il ruolo del compilatore del questionario.

Al completamento dell'intero questionario, inclusa la parte opzionale sulle misure di sicurezza in essere, verrà fornita in automatico una macro valutazione qualitativa del livello di sicurezza digitale del sistema informativo che emerge dalle risposte fornite, contestualizzata, in linea generale, alla tipologia di azienda (settore merceologico, numero dipendenti, fatturato, etc.) ed alla conseguente sua necessità di sicurezza digitale. Questa macro valutazione è di particolare interesse soprattutto per le piccole e piccolissime organizzazioni.

AIPSI cercherà poi di ampliare il numero dei **Media Partner**, e di ottenere un più incisivo coinvolgimento delle testate giornalistiche per far conoscere l'indagine OAD 2025 ed il suo rapporto finale. AIPSI si impegnerà con le Associazioni patrocinanti a tenere con e per loro specifici eventi, e se il numero di rispondenti per settore merceologico lo consentirà, di effettuare specifiche analisi per i settori con un numero di rispondenti superiore 100 (con un numero inferiore a 100 le analisi per settore non sarebbero significative).

AIPSI non può garantire la copertura completa dei vari settori merceologici e dei vari ruoli, e tantomeno può garantire l'effettiva e fattiva collaborazione delle Associazioni patrocinanti, con una significativa risposta da parte dei loro associati. La campagna che verrà intrapresa da AIPSI con tutti questi interlocutori, e la riduzione del numero di domande nel questionario online, dovrebbero portare ad un aumento del numero totale di rispondenti: ma non è possibile poter garantire una predeterminata estensione del bacino di rispondenti (e poi di lettori del Rapporto finale) per i vari settori.

## 2.1. Il questionario OAD 2025

Come già indicato nel precedente paragrafo, l'indagine OAD 2025 approfondirà gli **attacchi intenzionali agli ambienti web** e **agli applicativi basati su Intelligenza Artificiale** sia on premise che terzarizzate, **ed ai sistemi OT, Operational Technology**, rilevati dai rispondenti nel 2024.

Il **questionario online OAD 2025**, con risposte predefinite da selezionare, è strutturato con domande raccolte in 8 sezioni, molte delle quali opzionali e "saltabili" nel corso della compilazione. In alcune sezioni sono presenti delle sottosezioni per meglio articolare e contestualizzare le varie domande. Inoltre in alcune sezioni ci sono delle "domande" non visibili che effettuano calcoli sulle risposte selezionate per la valutazione del livello di sicurezza del SI oggetto delle risposte.

Le sezioni considerate nel questionario 2025:

- S1 - Brevi informazioni sulla Azienda/Ente della/del rispondente
- S2 - Attacchi digitali di ogni tipo al Sistema Informativo rilevati nell'intero 2024
- S3 - Approfondimento attacchi **ai siti e alle applicazioni web** del Sistema Informativo, con riferimento alle top ten vulnerabilità individuate da OWSAP per questi ambienti
- S3B - Approfondimento sugli attacchi ad applicativi basati su **Intelligenza Artificiale**, con riferimento alle top ten vulnerabilità 2025 individuate da OWSAP per questi ambienti
- S3C - Approfondimento sugli attacchi a **sistemi ed apparati OT** del Sistema Informativo
- S4 - Attacchi più temuti nel prossimo futuro
- S5 - Macro caratteristiche del Sistema Informativo cui la/il rispondente fa riferimento
- S6 - Misure tecniche in atto per la sicurezza digitale dell'intero Sistema Informativo
  - S6.1 - Misure fisiche di sicurezza digitale
  - S6.2 - Misure di Identificazione, Autenticazione e Autorizzazione
  - S6.3 - Misure per la sicurezza delle reti, locali e geografiche, incluse le connessioni ad Internet
  - S6.4 - Misure di sicurezza delle applicazioni del Sistema Informativo
  - S6.5 - Misure tecniche di sicurezza digitale per la protezione dei dati
  - S6.6 - Strumenti tecnici per il controllo e la gestione della sicurezza digitale del SI
  - S6.7 - La sicurezza nei sistemi OT in uso
- S7 - Misure organizzative di sicurezza digitale nell'Azienda/Ente della/del rispondente
- S8 - Ruolo della/del rispondente
- S10 – Calcoli (non visibili) e presentazione finale in tempo reale della macro valutazione del livello di sicurezza del SI a chi completa le risposte incluse quelle delle Sezioni 6 e 7.

Il completamento dell'intero questionario, incluse le parti opzionali, fornirà in automatico una **macro valutazione qualitativa del livello della sicurezza digitale** che emerge dalle risposte fornite, e l'elenco delle risposte più critiche in termini di sicurezza digitale.

Qualora non si fossero rilevati attacchi, il sistema online del questionario **salta automaticamente le relative domande**, e passa a quelle successive.

### 2.1.2. Per ringraziare le/i rispondenti al questionario OAD 2025

Chi compila il Questionario OAD 2025 potrà scaricare gratuitamente due numeri della rivista ISSA Journal, riservata ai Soci AIPSI. E' attualmente in corso la verifica di quali numeri di ISSA Journal utilizzare, considerando gli argomenti di maggior interesse, nell'ambito della sicurezza digitale, per chi compilerà il questionario.

## 2.2 Il Rapporto OAD 2025

Il rapporto finale sarà pubblicato e reso gratuitamente disponibile a tutti gli interessati dal sito OAD e da quello di AIPSI, nei tempi previsti ed indicati in §2.2.

**Il Rapporto avrà all'inizio un Executive Summary in italiano e in inglese.**

Uno specifico capitolo sarà dedicato ai **dati forniti dal Servizio Polizia Postale e per la Sicurezza Cibernetica**, relativi all'intero 2024. Tali dati riguarderanno, come negli anni precedenti, gli attacchi alle infrastrutture critiche italiane, gli attacchi al mondo delle banche e della finanza, il terrorismo digitale.

Il rapporto finale includerà anche i seguenti allegati:

- Allegato A - Aspetti metodologici dell'indagine OAD 2025
- Allegato B - Glossario dei principali termini ed acronimi sugli attacchi informatici
- Allegato C - Profili Sponsor (una scheda "istituzionale" per ogni Sponsor, di 1, 2 o 3 pagine formato A4 a seconda del tipo di sponsorizzazione)
- Allegato D - Profili Patrocinatori (logo, URL sito web, 3-4 righe descrizione)
- Allegato E - Riferimenti e fonti
- Allegato F - Profilo Autore/i del Rapporto OAD 2025
- Allegati G, H - Profili di AIPSI e Malabo Srl

Come per i precedenti, il Rapporto OAD 2025, appena disponibile (si veda §2.2) sarà gratuitamente scaricabile dal sito OAD [www.oadweb.it](http://www.oadweb.it) e dal sito AIPSI [www.aipsi.org](http://www.aipsi.org)

Come esempio di un Rapporto finale, e della sua sintesi, si veda l'ultimo Rapporto pubblicato, OAD 2024: <https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/oad-2024/rapporto-oad-2024-pubblicato-e-scaricabile.html>

Tutti i precedenti rapporti sono archiviati, e scaricabili, anno per anno da <https://www.oadweb.it/it/rapporti-e-relativi-convegni.html>

### 2.2.1 Le prefazioni previste nel Rapporto OAD 2025

Come per l'edizione 2024, Il Rapporto finale OAD 2025 avrà delle prefazioni di conosciuti attori nella scena italiana della sicurezza digitale, quali rappresentanti delle più importanti istituzioni italiane. Si prevedono le prefazioni del Direttore del **Servizio Polizia Postale e per la Sicurezza Cibernetica**, e del **Dipartimento della Trasformazione Digitale della Presidenza del Consiglio dei Ministri**, già avute nel 2024. Si cercherà di avere prefazioni anche da ACN, da AIGID e/o da altre Istituzioni nazionali coinvolte nella sicurezza digitale.



Queste prefazioni sono fondamentali per il **riconoscimento dell'autorevolezza e della validità dell'indagine e del Rapporto OAD**, ed aiutare così la sua diffusione soprattutto nelle Pubbliche Amministrazioni e nelle sedi istituzionali italiane.

## 2.3 Le fasi di OAD 2025

Il quadro complessivo delle attività previste per OAD 2025 è articolato, mese per mese, nelle seguenti attività (calendario di massima che potrà subire cambiamenti):

- **GENNAIO 2025**
  - Impostazione iniziativa OAD 2025 nell'ambito del Comitato Direttivo AIPSI con il supporto dell'ideatore di OAD, Marco R. A. Bozzetti, e della sua azienda Malabo
  - Stesura proposte di sponsorizzazione e richieste di patrocinio gratuito e loro invio a potenziali aziende ed enti interessati.
- **FEBBRAIO 2025**
  - Preparazione questionario online sulla piattaforma oadweb.it e test/messa a punto dei pesi delle diverse risposte per il calcolo del livello di sicurezza digitale del sistema informativo oggetto delle risposte.
  - Continuano i contatti per i patrocini e per le sponsorizzazioni
- **MARZO 2025**
  - Pubblicazione del questionario OAD 2025 online
  - Inizio campagna promozionale per la compilazione dei questionari
  - Continuano i contatti per i patrocini e per le sponsorizzazioni
- **APRILE - MAGGIO 2025**
  - Continua la campagna promozionale per la compilazione dei questionari
  - Continuano i contatti per i patrocini e per le sponsorizzazioni.
- **GIUGNO 2025**
  - In funzione di se e quando si raggiungerà il numero minimo di rispondenti necessari perché un'indagine web anonima sia significativa, chiusura dei questionari online ed inizio della elaborazione dei dati raccolti. In caso contrario AIPSI effettuerà, in collaborazione con i Patrocinatori e gli Sponsor, una ulteriore specifica promozione per la compilazione dei questionari persona per persona, in particolare con riferimento a CIO, CISO, CTO ed ai responsabili di vertice per le piccole organizzazioni.
- **GIUGNO-LUGLIO 2025**
  - Elaborazione dati raccolti dai questionari online
  - Stesura del Rapporto finale OAD 2025 e sua pubblicazione
  - Inizio campagna promozionale per il download del Rapporto OAD 2025 da parte dei degli interlocutori dei Patrocinatori e degli Sponsor, oltre che di tutti i possibili interessati contattati tramite i vari canali multimediali di AIPSI e degli Sponsor e dei Patrocinatori di OAD 2025



- Evento in videoconferenza o “ibrido” (incontro fisico e da remoto in videoconferenza) AIPSI di presentazione ufficiale del Rapporto OAD 2025 con una tavola rotonda di discussione dei dati emersi con i referenti degli Sponsor Gold e Diamond (questo evento potrebbe essere spostato a settembre).
- **AGOSTO-SETTEMBRE 2025**
  - Stesura e/o ausilio alla stesura di note ed articoli sui vari media inerenti il Rapporto OAD 2025 ed i dati pubblicati.
  - Eventuale realizzazione di webinar e di articoli per Sponsor Gold e Diamond
- **SETTEMBRE-DICEMBRE 2025**
  - Fornitura periodica agli Sponsor dei dati di download del Rapporto OAD 2025 (numero di download, non nominativo di chi l’ha scaricato, dato che il download non richiederà il login di chi lo scarica)
  - Partecipazione di AIPSI-OAD a vari eventi presentando, in funzione del tema in oggetto, alcuni dei dati emersi dall’indagine OAD 2025.

### 3. Il patrocinio gratuito di OAD 2025

Data la modalità on line e libera a tutti gli interessati a rispondere al questionario OAD 2025, per poter coprire i diversi settori merceologici, oltre che le Pubbliche Amministrazioni Centrali e Locali, è basilare per AIPSI **ampliare il più possibile il bacino dei potenziali rispondenti**. Per questo, oltre alle mailing-list ed ai canali di comunicazione di AIPSI, è fondamentale il coinvolgimento delle associazioni, degli enti istituzionali e degli ordini professionali, perché informino e promuovano al loro interno prima la compilazione del questionario, poi lo scarico e la lettura del finale Rapporto OAD 2025.

In tale ottica AIPSI richiede il patrocinio gratuito di Associazioni no profit, di Ordini professionali di rappresentanza, di Enti istituzionali nazionali coinvolti o interessati alla sicurezza digitale.

L’Ente patrocinante potrà partecipare attivamente all’indagine ed offrire così ai propri Soci ed interlocutori un servizio informativo e di riferimento sugli attacchi digitali riscontrati in Italia, oltre che sulle misure di sicurezza digitale in essere da parte dei rispondenti: una chiara e contestualizzata fotografia della effettiva situazione in Italia sulla sicurezza digitale. Tale fotografia è un utile strumento per acquisire **consapevolezza** sulla sicurezza digitale e sui suoi rischi, con analisi generali ma anche settoriali, necessaria anche **per aiutare ad effettuare le specifiche analisi dei rischi ICT**, in molti casi obbligatorie per adempiere a talune normative europee, si pensi ad esempio alla privacy e alla NIS2, e per talune certificazioni.

Il fornire poi ai singoli rispondenti una macro valutazione del livello di sicurezza digitale del sistema informativo, in funzione delle risposte selezionate, fornisce un ulteriore strumento di ausilio e di indirizzo per rafforzare e migliorare la consapevolezza sulla sicurezza digitale a livello azienda/ente.

Con il singolo Patrocinante e/o con un gruppo di Patrocinatori AIPSI potrà inoltre effettuare specifiche **iniziative congiunte**, ad esempio webinar, con presentazione e discussione dei principali dati emersi dall’indagine e, se si raggiungesse un sufficiente numero (come minimo 100) di risposte ricevute per settore merceologico (incluse PAC e PAL), OAD 2025 realizzerebbe una specifica analisi dei dati emersi per lo specifico settore cui il’Ente Patrocinante appartiene e fa riferimento.

### 3.1 Perché conviene patrocinare OAD 2025

Con il patrocinio gratuito di OAD 2025, il Patrocinatore fruisce di una significativa visibilità ed offre ai propri Soci ed interlocutori un autorevole servizio di conoscenza ed approfondimento sulla sicurezza digitale dei loro sistemi informativi.

#### In termini di visibilità:

- il nome ed il logo a colori dell'Ente patrocinante è inserito e chiaramente visibile, nelle pagine dei siti web di AIPSI, OAD e Malabo, che introducono ed illustrano l'indagine OAD 2025 ed il suo stato di avanzamento;
- il nome ed il logo a colori dell'Associazione patrocinante è inserito sotto la dicitura "Patrocinatori" nella pagina web introduttiva (messaggio di benvenuto) del Questionario OAD 2025 online;
- il logo a colori dell'Associazione patrocinante è posto nella quarta di copertina del Rapporto OAD 2025;
- una breve descrizione dell'Associazione patrocinante, con logo a colori e link al sito web, nell'Allegato D del Rapporto OAD 2025;
- il logo a colori del Patrocinatore nelle slide AIPSI per gli eventi organizzati da AIPSI, o ai quali partecipa, che trattano dati e considerazioni su OAD 2025.

#### In termini di servizi ai propri Soci ed interlocutori:

- se si raggiunge un numero idoneo di compilazioni, almeno 100, per il singolo settore merceologico (incluse PAC e PAL), rappresentato dall'Ente, OAD può realizzare specifiche analisi per quel settore; e con tali dati la realizzazione congiunta di uno specifico evento per la loro presentazione e discussione;
- la possibilità di iniziative/webinar congiunti tra AIPSI ed il Patrocinatore;
- la possibilità per i Soci e gli interlocutori del Patrocinatore di partecipare a tutti gli eventi, in particolare webinar, organizzati da AIPSI (o da altre Associazioni/Enti) sui temi trattati da OAD 2025;
- la compilazione online del questionario, anonimo, consente a chi lo compila di conoscere l'ampia tipologia di che cosa può essere attaccato e con quali tipologie di tecniche; e se risponde alle misure di sicurezza in essere, di conoscere le principali misure tecniche ed organizzative, confrontandole con quelle che il suo sistema informativo utilizza. Ed in questo secondo caso, di poter disporre di una macro valutazione del livello di sicurezza digitale del sistema informativo oggetto delle risposte al questionario, in funzione di quelle selezionate, e con l'elenco di quelle che risultano più critiche nella valutazione del livello di sicurezza;
- possibile coinvolgimento di esperti del Patrocinante per fornire suggerimenti al Comitato Scientifico AIPSI, oltre contributi e contenuti da pubblicare sul sito AIPSI e OAD (previa accettazione da parte AIPSI).

OAD inoltre fornirà a tutti i Patrocinatori un banner da inserire sul proprio sito web per promuovere la compilazione del questionario OAD 2025.

### 3.2. Gli obblighi dell'Associazione patrocinante

L'Associazione/Ente patrocinante si impegna fattivamente e concretamente a :

- **promuovere** e **coinvolgere** i propri Soci ed interlocutori **a compilare il Questionario OAD 2025**, tramite i propri canali multimediali, dal sito web alle news, dal banner OAD alle newsletter
- **far scaricare** dai propri Soci ed interlocutori il **Rapporto finale OAD 2025**

- **promuovere** presso i propri Soci, simpatizzanti ed interlocutori le varie iniziative AIPSI sull'indagine OAD 2025.

## 4. La proprietà intellettuale di OAD 2025

La proprietà intellettuale ed il copyright dell'intera iniziativa, inclusi il Questionario on line ed i contenuti, le figure ed i grafici del Rapporto OAD 2025, sono, come per le precedenti edizioni, di AIPSI e di Malabo Srl che **consentono il loro utilizzo agli Sponsor**, con l'obbligo di citare la fonte sulle figure sia sui grafici del Rapporto tramite la dicitura ©OAD 2025.

## 5. Come aderire al gratuito patrocinio di OAD 2025

Per aderire al gratuito patrocinio di OAD 2025, basta che il Responsabile con diritti di firma invii una email a [m.bozzetti@aipsi.org](mailto:m.bozzetti@aipsi.org), e/o in PEC a [aipsi@gigapec.it](mailto:aipsi@gigapec.it), nella quale venga specificato che “.. l'Associazione/Ente xxx conferma il suo patrocinio gratuito all'indagine OAD 2025 e si impegna a contribuire al successo dell'indagine attuando al meglio quanto elencato al punto §2.2.2 della Richiesta AIPSI di patrocinio gratuito indagine OAD 2025. ”, indicando l'indirizzo della sede legale, il nominativo del Responsabile che invia la e-mail, il nome del responsabile legale dell'Ente con la sua e-mail, un numero telefonico di riferimento, possibilmente di cellulare.

Gli interlocutori indicati saranno contattati da AIPSI nel più breve tempo possibile.

---

### ***AIPSI, Associazione Italiana Professionisti Sicurezza Informatica***

Associazione no profit, capitolo italiano della mondiale ISSA, è costituita da sole persone fisiche interessate e/o operanti a qualsiasi livello e ruolo nell'ambito della sicurezza digitale.

Obiettivo primario di AIPSI è la crescita professionale e delle competenze dei propri Soci e la promozione e diffusione in Italia della cultura della sicurezza digitale. In tale ottica, oltre ai servizi ed eventi forniti da ISSA, quali la rivista mensile ISSA Journal, convegni, webinar, gruppi di lavoro e corsi in inglese, un network mondiale tra i Soci, sconti su corsi e certificazioni individuali, AIPSI fornisce servizi specifici per il contesto italiano: alcuni riservati ai soli Soci, quali mentorship gratuita per la crescita professionale, gruppi di lavoro di approfondimento, network nazionale tra i Soci, sconti su corsi e certificazioni individuali in Italia, ma la maggior parte aperta a tutti gli interessati: convegni e webinar, l'indagine annuale OAD sugli attacchi e le misure di sicurezza digitali in aziende/enti in Italia, AIPSI Giovani, il gruppo di lavoro e l'indagine sul lavoro femminile nella sicurezza digitale in Italia (CSWI).

CF 9741515015 - P.IVA 05311540966 e-mail: [aipsi@aipsi.org](mailto:aipsi@aipsi.org) PEC: [aipsi@gigapec.it](mailto:aipsi@gigapec.it)  
Sede Centrale e Legale: AIPSI c/o Malabo Srl Via Savona 26 - 20144 Milano tel. (+39) 02 39443632