RICHIESTA
GRATUITO PATROCINIO
INDAGINE OAD 2023

UNA INIZIATIVA CONGIUNTA

Gennaio 2023

Sommario

1. L'indagine OAD 3
2. OAD 2023 4
2.1. Il questionario OAD 2023 5
2.2 Il rapporto finale OAD 2023 7
3. Per ringraziare i rispondenti OAD 2023 8
4. Le fasi dell'indagine OAD 2023 9
5. Perché patrocinare OAD 2023 10
5.1 I diritti delle associazioni/enti patrocinanti OAD 2023 10
5.2 Gli obblighi dell'ente patrocinante 10
6. Come aderire al gratuito patrocinio di OAD 2023 11

1. L'indagine OAD

L'iniziativa OAD, Osservatorio Attacchi Digitali in Italia (chiamata fino al 2015 OAI, Osservatorio Attacchi Informatici in Italia), nel 2023 arriva a 16 anni consecutivi di indagini sugli attacchi digitali in Italia, e nel tempo si è consolidata anche grazie alla partnership tra **Malabo Srl** (www.malaboadvisoring.it), la società di consulenza direzionale sull'ICT (Information and Communication Technologies) che realizza l'indagine online, elabora i dati raccolti e stende il rapporto finale, ed **AIPSI**, Associazione Italiana Professionisti Sicurezza Digitale, capitolo italiano di ISSA (www.aipsi.org, www.issa.org), che guida e supporta l'iniziativa, e ne garantisce la **qualità** e l'**indipendenza** dell'analisi e dei contenuti anche dagli Sponsor.

OAD, Osservatorio Attacchi Digitali in Italia, è **l'unica iniziativa in Italia** per l'analisi sugli attacchi intenzionali ai sistemi informativi delle Aziende e degli Enti Pubblici italiani, **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 compilabile con un moderno browser.

Obiettivo principale dell'iniziativa OAD è di far conoscere il più ampiamente possibile **l'effettiva realtà del fenomeno degli attacchi digitali intenzionali** ai sistemi informativi di aziende ed enti pubblici in Italia, 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.

La disponibilità di informazioni "locali all'Italia" sugli attacchi digitali intenzionali rilevati, sulla tipologia e sull'ampiezza del fenomeno è fondamentale anche, e soprattutto, per le organizzazioni di piccole dimensioni perché possano valutare i possibili rischi e attivare le misure più idonee di prevenzione e protezione, così come richiesto da numerose normative nazionali ed internazionali, in primis il GDPR, il regolamento europeo per la privacy.

Undici i rapporti annuali OAD/OAI che sono stati pubblicati (le loro copertine in fig. 1) e che coprono i quindici anni consecutivi di indagini online ad oggi effettuati, dall'anno 2007 al 2022. I più recenti rapporti hanno un "executive summary" in italiano e in inglese. Gli undici rapporti sono scaricabili gratuitamente dallo specifico sito creato per OAD, 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, ove sono stati presentati e discussi i dati emersi dalle indagini OAD. Scaricare dal sito OAD un rapporto ed i vari documenti correlati, è gratuito per ogni interessato.

Fig. 1 Le copertine dei Rapporti OAD-OAI pubblicati

2. OAD 2023

L'indagine OAD 2023 sarà diversa dalle precedenti, pur mantenendo molti elementi in comune, anche per poter avere una continuità sui principali trend emersi nei precedenti 15 anni consecutivi di indagini: l'obiettivo principale è di **ridurre e semplificare il questionario** in modo 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 precedente analisi.
Per raggiungere questo obiettivo, l'indagine OAD 2023:

- si **focalizza solo** sugli attacchi subiti nel **2022** ai **siti e agli ambienti web**, e contiene due sole domande sulle altre tipologie di attacco rilevate nel 2022 sui Sistemi Informativi dei rispondenti per poter avere dati di trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 ad oggi;
- utilizza un unico **questionario online,** rigorosamente anonimo, con la parte **sulle misure di sicurezza in essere a protezione dei siti e degli applicativi web resa opzionale,** e raccomandata soprattutto per le/i rispondenti dei Provider di hosting e di cloud.

La parte di domande sugli attacchi subiti è obbligatoria per tutti i rispondenti: per chi non avesse rilevato attacchi, le domande relative vengono automaticamente saltate.
Sono 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.
Il completamento dell'intero questionario, inclusa la parte opzionale sulle misure di sicurezza in essere, fornisce in automatico una macro valutazione qualitativa del livello di sicurezza che emerge dalle risposte fornite.

L'iniziativa OAD ha sempre ottenuto dei patrocini gratuiti, ma prevalentemente da Associazioni del o vicine al mondo ICT[1]. Per il 2023 AIPSI-OAD intende richiedere patrocini ad Associazioni degli altri settori merceologici, cercando di coinvolgere Associazioni a livello nazionale e territoriale (es. regionale e/o provinciale), quali CONFAPI, Confartigianato, Confesercenti, Confindustria, Confcommercio, Camere di Commercio a livello generale, e per settore secondo la classificazione ATECO, cui si aggiungono le Pubbliche Amministrazioni Centrali, PAC, e quelle Locali, PAL. Per le specifiche professioni si è fatto e si farà riferimento sia agli Ordini, ad esempio degli amministratori di condominio, degli avvocati, dei commercialisti, dei medici, dei notai, sia alle relative libere Associazioni per ruoli professionali non normati, quali il personale delle risorse umane e dell'organizzazione, quello del procurement, quello dell'ICT (CIO, CISO, CTO, outsourcer), gli archivisti-gestori della documentazione, i DPO per la privacy, etc.

[1] I Patrocinatori di OAD 2021-22 includevano: AICA, AIPSI, AISIS, AITASIT, Anorc, Assi-BO, Assintel, Assinform-Anitec, Aused, CDI Torino, CDTI Roma, CIOClub Italia, ClubTI Emilia Romagna, ClubTILiguria, ClubTI Milano, FIDA Inform, Inforav.

2.1. Il questionario OAD 2023

Come già indicato nel precedente paragrafo, l'indagine OAD 2023 si focalizza sui soli **attacchi intenzionali ai siti ed alle applicazioni web**, sia on ptemise che terziarizzate, con due sole domande sulle altre tipologie di attacco rilevate nel 2022 sui Sistemi Informativi.

OAD 2023 utilizzerà un questionario online rigorosamente anonimo, sostanzialmente strutturato in due principali parti: gli **attacchi rilevati nel 2022**, e le **misure di sicurezza in essere;** la parte sugli attacchi sarà **obbligatoria** per tutti i rispondenti, mentre quella sulle misure di sicurezza in essere sarà **obbligatoria** solo per i Provider di hosting e di cloud. Tutti gli altri rispondenti saranno liberi di compilarla, se vogliono: per incentivarli, il sistema fornirà in automatico, alla fine della compilazione, una macro valutazione qualitativa del livello della sicurezza digitale che emerge dalle risposte fornite.

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

2.1.1 Le domande sugli attacchi digitali rilevati

Le due domande generali, necessarie per garantire continuità con quelle dei precedenti quindici anni sulla diffusione in Italia degli attacchi digitali intenzionali, riguardano:

- le 13 **tipologie di attacco** (il che cosa si attacca) considerate sono:
  - Distruzione fisica di dispositivi ICT o di loro parti
  - Furto di dispositivi d'utente mobili (PC, server, storage system, etc.)
  - Furto di dispositivi ICT fissi o di loro parti
  - Furto informazioni da sistemi ICT fissi
  - Furto informazioni da sistemi d'utente mobili (palmari, smartphone, tablet, etc.)
  - Attacchi all'identificazione, autenticazione e autorizzazioni degli utenti finali e privilegiati
  - Attacchi alle reti, locali e geografiche, fisse e wireless, e ai DNS
  - Attacchi ai singoli sistemi ICT nel loro complesso (dai dispositivi d'utente ai server-storage e ai servizi in cloud)
  - Attacchi per modifiche non autorizzate ai programmi applicativi e alle loro configurazioni
  - Attacchi per modifiche non autorizzate alle informazioni trattate dai sistemi ICT
  - Attacchi per saturazione risorse digitali (DoS/DDoS)
  - Attacchi ai propri sistemi in cloud o in housing/hosting presso fornitori terzi
  - Attacchi ai propri sistemi di OT, Operational Technology, per dispositivi IoT (Internet of Things), l' automazione industriale e la robotica

- le 7 famiglie di **tecniche di attacco** considerate (il come si attacca) sono le seguenti:
  - Attacco fisico
  - Raccolta malevola e non autorizzata di informazioni
  - Script e programmi maligni
  - Agenti autonomi
  - Toolkit
  - Botnet e simili
  - Utilizzo di due o più tecniche di attacco, inclusi gli APT, Advanced Persistent Threat.

Le **domande specifiche sugli attacchi ai siti ed alle applicazioni web** riguardano:

- Se i siti e le applicazioni web attaccate sono on premise, terziarizzate in hosting o in cloud, o in un mix tra terziarizzazione e on premise;
- le probabili tecniche di attacco usate (sopra elencate) e , in maggior dettaglio, quali vulnerabilità sono state probabilmente sfruttate facendo riferimento alle **top 10 di OSWAP** per l'attacco più grave subito;
- i più gravi impatti tecnici ed economici riscontrati dall'attacco più grave;
- le possibili motivazioni per l'attacco più grave;
- il tempo massimo per il ripristino dopo aver subito l'attacco più grave.

2.1.2 Le domande sulle misure di sicurezza digitali in essere

Come già indicato in precedenza, queste domande saranno rese **obbligatorie** dal sistema online **solo per i compilatori che appartengono a società di provider di hosting/cloud**.
Il motivo è che questo società supportano, nella maggior parte dei casi, i siti e le applicazioni web dei rispondenti: le loro misure di sicurezza sono l'argine ed il baluardo per gli attacchi intenzionali di questo tipo, ed è importante rilevare quali misure di sicurezza sono in atto, e di quale livello. Per tutti gli altri rispondenti possono essere saltate, così da rendere più veloce e più semplice la compilazione del questionario. Per motivare i rispondenti di questa parte, il sistema fornisce in automatico, alla fine della compilazione dell'intero questionario, una macro analisi qualitativa del livello di sicurezza in essere, in funzione delle risposte fornite.
Come nei questionari degli ultimi anni, la rilevazione delle misure di sicurezza digitali in essere fa riferimento alle seguenti misure.

- **Misure tecniche**
  - Architettura complessiva delle misure della sicurezza digitale, integrata con l'intera architettura del sistema informatico, che può includere Zero Trust, SASE, SOAR, etc.
  - Contromisure fisiche
  - Misure di Identificazione, Autenticazione, Autorizzazione (IAA)
  - Contromisure tecniche sicurezza digitale a livello di reti locali e geografiche
  - Contromisure tecniche per la protezione logica dei singoli sistemi ICT
  - Contromisure tecniche per la protezione degli applicativi
  - Contromisure per la protezione dei dati
- **Misure organizzative**
  - Struttura organizzativa, ruoli, competenze, certificazioni
  - Policy e procedure organizzative
  - Contratti e clausole sicurezza digitale con le Terze Parti (GDPR dovrebbe aiutare!!)
  - Consapevolezza della sicurezza digitale a tutti i livelli della struttura organizzativa
  - Auditing
- **Misure di gestione e di governo**
  - Sistemi di controllo, monitoraggio e gestione della sicurezza digitale
  - Piano di Disaster Recovery (DR).

Ulteriori domande nel questionario riguardano:

- tipo e macro caratteristiche dell'Azienda/Ente del rispondente: tipologia azienda/ente e settore merceologico, numero di dipendenti, struttura organizzativa per la cybersecurity e primarie necessità di misure di sicurezza per le sue attività (questa domanda è posta all'inizio del questionario)
- come sono stati rilevati e come sono gestiti gli attacchi quando occorrono
- tipologie di attacchi più temuti nel prossimo futuro.
- ruolo del compilatore del questionario.

2.2 Il rapporto finale OAD 2023

Il rapporto finale sarà pubblicato e reso gratuitamente disponibile a tutti gli interessati dal sito oadweb.it, nei tempi previsti ed indicati nel §5.

I contenuti del rapporto completo includeranno, commentandoli, tutti i temi presenti sia nella parte attacchi rilevati sia nella parte misure di sicurezza del questionario.
Il Rapporto avrà all'inizio un Executive Summary in italiano e in inglese.
Nel rapporto finale uno specifico capitolo sarà dedicato ai **dati forniti dalla Polizia Postale e delle Telecomunicazioni,** relativi all'intero 2022, che saranno commentati dall'autore del rapporto. 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
- 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, si veda §8)
- 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 2023
- Allegati G, H - Profili di AIPSI e Malabo Srl

Come per i precedenti, il Rapporto OAD 2023, appena disponibile (si veda §6) sarà gratuitamente scaricabile dal sito www.oadweb.it, **previa registrazione sempre gratuita** al sito stesso alla pagina: https://www.oadweb.it/it/component/comprofiler/registers.html
Come mostrato nella fig. 2 sottostante, la registrazione richiede, oltre a poche informazioni, di fornire il **consenso esplicito** al trattamento dei propri dati personali, in particolare perché essi possano essere forniti ai vari Sponsor di OAD 2023: questo è infatti un elemento basilare e tra i motivi più importanti per la sponsorizzazione (§7 e §8). Il trattamento dei dati personali da parte AIPSI e OAD segue le normative GDPR, ed è descritto nella informativa sulla privacy e sui cookie in https://www.oadweb.it/it/informativa-privbacy-e-cookie.html

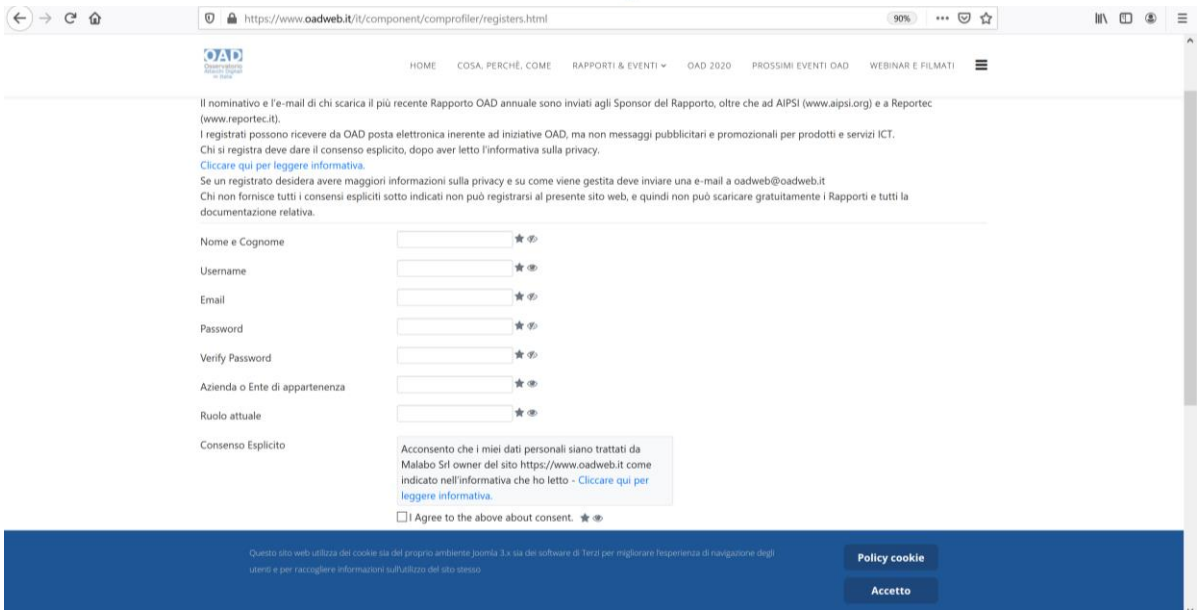

Fig. 2 Il modulo di registrazione dell'utente al sito web OAD, con la richiesta di consenso esplicito

Come esempio di un Rapporto finale, e della sua sintesi, si veda l'ultimo Rapporto pubblicato, OAD 2021 aggiornato ad aprile 2022: https://www.oadweb.it/it/rapporti-e-relativi-convegni/2021-22/per-scaricare-il-rapporto-oad-2021-aggiornamento-aprile-2022.html.
Si ricorda che anche tutti i precedenti rapporti sono archiviati, e scaricabili, anno per anno da https://www.oadweb.it/it/rapporti-e-relativi-convegni.html

3. Per ringraziare i rispondenti OAD 2023

Come ringraziamento per il tempo dedicato, chi completa il Questionario OAD 2023, potrà scaricare gratuitamente i seguenti due numeri della rivista ISSA Journal, riservata ai Soci AIPSI :

- il numero di **Febbraio 2023** di **ISSA Journal**

- il numero di **Marzo 2022** di **ISSA Journal**, con un articolo di AIPSI sul gender gap in Italia per le professioni inerenti la sicurezza digitale.

4. Le fasi dell'indagine OAD 2023

Il quadro complessivo delle attività previste per OAD 2023 è articolato, mese per mese, nei seguenti punti:

- **GENNAIO 2023**
  - Definizione ed installazione-attivazione questionario online sulla piattaforma oadweb.it
  - Invio proposte di sponsorizzazione e richieste di patrocinio gratuito

- **FEBBRAIO 2023**
  - Inizio campagna promozionale per la compilazione dei questionari
  - Continuano i contatti per i patrocini e per le sponsorizzazioni

- **MARZO - GIUGNO 2023**
  - Continua campagna promozionale per la compilazione dei questionari
  - Continuano i contatti per i patrocini e per le sponsorizzazioni

- **GIUGNO 2023**
  - 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 collaborazioni con i Patrocinatori e gli Sponsor, una specifica promozione per la compilazione dei questionari persona per persona, in particolare con riferimento a CIO e CISO

- **LUGLIO 2023**
  - Elaborazione dati raccolti dai questionari online
  - Stesura del Rapporto finale OAD 2023 e sua pubblicazione
  - Inizio campagna promozionale per il download del Rapporto OAD 2023 da parte dei Soci dei Patrocinatori, degli interlocutori degli Sponsor e di tutti i possibili interessati contattati tramite i vari canali a disposizione
  - Webinar AIPSI di presentazione ufficiale del Rapporto OAD 2023 con "comunicato stampa" riservato ai giornalisti e tavola rotonda di discussione dei dati emersi con i referenti degli Sponsor Gold e Diamond.

- **AGOSTO-SETTEMBRE 2023**
  - Stesura e/o ausilio alla stesura di note ed articoli sui vari media inerenti il Rapporto OAD 2023 ed i dati pubblicati.
  - Realizzazione dei primi webinar e della pubblicazione di articoli per Sponsor Gold e Diamond

- **SETTEMBRE-DICEMBRE 2023**
  - Fornitura periodica agli Sponsor dei download del Rapporto OAD 2023
  - Partecipazione di AIPSI-OAD a vari eventi presentando, in funzione del tema in oggetto, alcuni dei dati emersi dall'indagine OAD 2023.

5. Perché patrocinare OAD 2023

Il **gratuito** patrocinio del progetto OAD Extended è riservato alle Associazioni e agli Enti senza scopi di lucro interessate/i a coinvolgere i propri Soci, simpatizzanti ed interlocutori nella compilazione del questionario on line e poi a divulgare loro il rapporto finale, anche effettuando iniziative ad hoc in collaborazione con AIPSI quali webinar con presentazione e discussione dei principali dati emersi e, se possibile (dipende dal numero di risposte ricevute per settore, che devono come minimo superare il numero 100), di dati di analisi per lo specifico settore dell'Associazione stessa.
Partecipando attivamente a OAD 2023, l'Associazione/Ente offre 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 esercizio da parte dei rispondenti: una chiara e contestualizzata fotografia della effettiva situazione in Italia sulla sicurezza digitale nell'ambito . Tale fotografia è un utile strumento per acquisire consapevolezza sulla sicurezza digitale e suoi rischi, con analisi generali ma anche settoriali, necessaria anche **per aiutare ad effettuare le specifiche analisi dei rischi ICT**, in molti casi obbligatorie ad esempio in ambito privacy GDPR. Il fornire poi al singoli rispondenti una **macro valutazione** del livello di sicurezza digitale del sistema informatico, 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.

5.1 I diritti delle associazioni/enti patrocinanti OAD 2023

- apporre il loro logo sulla quarta di copertina del Rapporto OAD 2023
- breve descrizione dell'Associazione/Ente, con logo e link al sito web, nell'Allegato D
- apporre il loro logo ed il link al loro sito nella pagina del sito OAD relativa a OAD 2023
- apporre il loro logo nelle slide di presentazione di OAD e/o dei dati di OAD, sotto la dicitura "Con il patrocinio di", oppure di "Enti Patrocinatori"
- visibilità del Patrocinatore durante gli eventi organizzati da AIPSI, o ai quali partecipa, che trattano dati e considerazioni su OAD 2023
- se si raggiunge un numero idoneo di rispondenti, almeno 100, per il singolo settore merceologico rappresentato dall'Associazione/Ente, la realizzazione di specifiche analisi settoriali, e la realizzazione di uno o più webinar dedicati in merito
- possibile coinvolgimento di esperti del Patrocinante per fornire suggerimenti al Comitato Scientifico OAD e al Consiglio Direttivo AIPSI, oltre contributi e contenuti da pubblicare sul sito AIPSI e OAD (previa accettazione da parte AIPSI).

5.2 Gli obblighi dell'ente patrocinante

L'Associazione/Ente patrocinante si impegna fattivamente a :

- **promuovere** e **coinvolgere** i propri Soci ed interlocutori **a compilare il Questionario** OAD 2023, tramite i vari canali usati, dal sito web alle news, dal banner ad hoc OAD, alle news in agenda e alle newsletter
- **far scaricare** dai propri Soci ed interlocutori il Rapporto finale 2023

- **promuovere** presso i propri Soci, simpatizzanti ed interlocutori le varie iniziative AIPSI sull'indagine OAD 2023.

6. Come aderire al gratuito patrocinio di OAD 2023

Per aderire al gratuito patrocinio del progetto OAD Extended, basta che il Responsabile con diritti di firma invii **una email** a *m.bozzetti@aipsi.org*, o in PEC a aipsi@gigapec.it, nella quale venga specificato che *".. l'Associazione/Ente xxx conferma il suo patrocinio gratuito all'indagine OAD 2023",* indicando l'indirizzo della sede legale, il nominativo del Responsabile che invia la e-mail, il nome del responsabile legale dell'Associazione/ente con la sua e-mail, un numero telefonico di riferimento, possibilmente di cellulare.

AIPSI
www.aipsi.org
Sede Centrale: Via Savona 26 - 20144 Milano
Tel: +39 02 39443632
E-mail: aipsi@aipsi.org
Partita IVA: 05311540966