OAD
Osservatorio
Attacchi Digitali
in Italia

PROPOSTA SPONSORSHIP INDAGINE OAD 2024

REPUBBLICA DIGITALE

UNA INIZIATIVA aipsi

OPERATIVAMENTE REALIZZATA DA malabo ICT Advisory

Gennaio 2024

Sommario

1. L'INIZIATIVA OAD

L'iniziativa OAD, Osservatorio Attacchi Digitali in Italia (chiamata fino al 2015 OAI, Osservatorio Attacchi Informatici in Italia), nel 2024 arriva a 17 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 realizzata da **Malabo Srl** (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, 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**[1], come evidenziato in https://repubblicadigitale.innovazione.gov.it/it/i-progetti/.

Dodici 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 2022.
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.

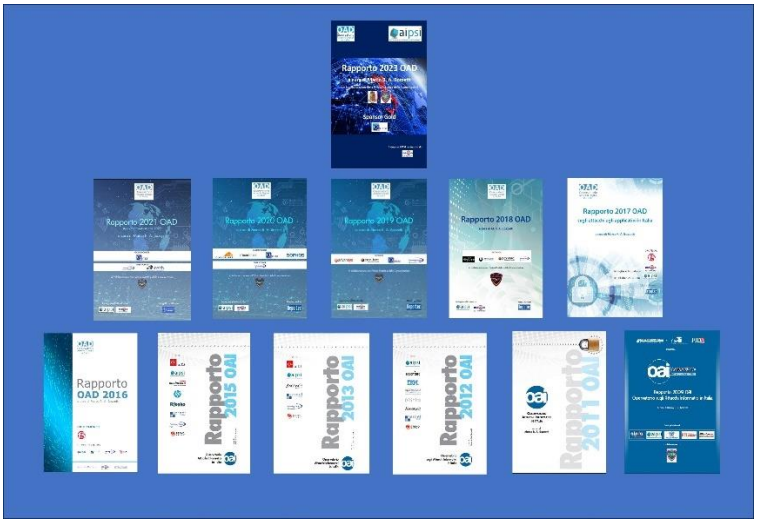

Fig. 1 Le copertine dei Rapporti OAD-OAI pubblicati

Come evidenziato nella fig. 1, sulle copertine di ogni rapporto, a partire da quello del 2012, sono presenti i loghi degli Sponsor e all'interno del rapporto è inserita come allegato la scheda di presentazione di ogni Sponsor.

I potenziali rispondenti al questionario OAD sono informati dell'indagine OAD 2024 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, in minor misura, 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 stimabile tra 1000 e 1500. Questo dato è solo una stima, che

[1] 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/)

include oltre al preciso numero di download effettuati dal sito oadweb.it, anche la stima di inoltro diretto del Rapporto finale da parte di Sponsor, Patrocinatori e di chi lo aveva già scaricato.

2. OAD 2024

L'indagine OAD 2024 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 2024:

- conterrà due sole domande sugli attacchi rilevati nel 2023 in riferimento alle tipologie di attacco ed alle famiglie di tecniche di attacco (si veda §2.1.1) così da poter avere dati di trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 al 2023;
- le domande di approfondimento riguarderanno **solo** gli attacchi subiti nel **2023** ai **siti e agli ambienti web** (ancora in discussione se aggiungere anche domande verticali sugli attacchi agli ambienti OT, Operational Technology);
- **saranno opzionali** le domande sulle **misure di sicurezza digitale** presenti nei sistemi informativi oggetto delle risposte.

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 grazie all'applicazione che supporta il questionario online, basata su una specifica configurazione del software opensource Limesurvey .
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.
Al completamento dell'intero questionario, inclusa la parte opzionale sulle misure di sicurezza in essere, viene fornita in automatico una macro valutazione qualitativa del livello di sicurezza 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.

Come negli anni precedenti, saranno stretti **accordi di patrocinio gratuito** con Associazioni, anche di categoria, dei **vari settori merceologici** oltre che delle **Pubbliche Amministrazioni**, e di specifiche professioni (ad esempio avvocati, notai, commercialisti, medici, CIO, CISO, DPO, CTO, etc.). Si cercherà poi di ampliare il numero dei **media** usati, e di ottenere un più incisivo coinvolgimento delle testate giornalistiche per far conoscere l'indagine OAD 2024 ed il suo rapporto finale. OAD ed AIPSI si impegnano 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 elevato (>100) numero di rispondenti.

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 allo Sponsor una predeterminata estensione del bacino di rispondenti (e poi di lettori del Rapporto finale) per i vari settori.

2.1. Il questionario OAD 2024

Come già indicato nel precedente paragrafo, l'indagine OAD 2024 si focalizzerà sugli **attacchi intenzionali ai siti ed alle applicazioni web**, sia on premise che terziarizzate, rilevate nel 2023; si sta valutando se inserire un insieme di domande per gli attacchi al mondo OT, Operational Technology.

OAD 2024 utilizzerà un questionario online rigorosamente anonimo, sostanzialmente strutturato in due principali parti: gli **attacchi rilevati nel 2023**, e le **misure di sicurezza digitale in essere;** la parte sugli attacchi sarà **obbligatoria**, mentre quella sulle misure di sicurezza in essere sarà **opzionale,** ma necessaria per poter avere la macro valutazione qualitativa del livello di sicurezza in essere nel sistema informativo oggetto delle risposte.

Il completamento dell'intero questionario, incluse le parti opzionali, fornisce 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.

2.1.1 Le domande sugli attacchi digitali rilevati

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

- le **tipologie di attacco** (il che cosa si attacca), che includono:
  - Distruzione fisica di dispositivi ICT o di loro parti
  - Furto di dispositivi d'utente mobili (palmari, smartphone, tablet, etc.)
  - Furto di dispositivi ICT fissi o di loro parti(PC, server, storage system, etc.)
  - Furto informazioni da sistemi ICT fissi
  - Furto informazioni da sistemi d'utente mobili
  - 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 famiglie di **tecniche di attacco** considerate (il come si attacca):
  - Attacco fisico
  - Raccolta malevola e non autorizzata di informazioni
  - Script e programmi maligni
  - Agenti autonomi
  - Toolkit
  - Botnet e simili
  - Utilizzo di strumenti e tecniche di Intelligenza Artificiale
  - Utilizzo di due o più tecniche di attacco, inclusi gli APT, Advanced Persistent Threat.

Le **domande di dettaglio sugli attacchi rilevati** negli ambienti web (e forse in quelli OT) includono::

- se i sistemi attaccati 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 per gli ambienti web, quali vulnerabilità sono state probabilmente sfruttate facendo riferimento alle **top 10 di OWASP** nel caso dell'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 **opzionali**. Sarebbe comunque opportuno che venissero compilate, così da ottenere:

- un elenco di verifica delle misure di sicurezza digitali, tecniche ed organizzative, che potrebbero o dovrebbero essere implementate sul Sistema Informativo della azienda/ente rispondente;
- alla fine della compilazione dell'intero questionario, una macro analisi qualitativa del livello di sicurezza in essere, in funzione delle risposte fornite, con l'elenco, tra queste risposte, di quelle che evidenziano le più gravi mancanze. In pratica una prima indicazione dei principali miglioramenti nella sicurezza digitale che sarebbe opportuno attuare.

Come nei questionari degli ultimi anni, la rilevazione delle misure di sicurezza digitali in essere farà 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 e monitoraggio (gestione operativa della sicurezza digitale)
    - Governo (strategico) della sicurezza digitale
    - Disaster Recovery (piano, allocazione risorse alternative, etc.).

Ulteriori domande nel questionario riguarderanno:

- 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.

2.1.3. Per ringraziare le/i rispondenti al questionario OAD 2024

Chi compila il Questionario OAD 2024 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 2024

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 §2.3.

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

Uno specifico capitolo sarà dedicato ai **dati forniti dalla Polizia Postale e delle Telecomunicazioni,** relativi all'intero 2023. 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 2024
- 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, Silver, Gold, Diamond, si veda §4)

- 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 2024
- Allegati G, H - Profili di AIPSI e Malabo Srl

Come per i precedenti, il Rapporto OAD 2024, appena disponibile (si veda §2.3) sarà gratuitamente scaricabile dal sito OAD www.oadweb.it e dal sito AIPSI www.aipsi.org

Come esempio di un Rapporto finale, e della sua sintesi, si veda l'ultimo Rapporto pubblicato, OAD 2023: https://www.aipsi.org/eventi/eventi-in-programma/902-aipsi-ha-pubblicato-il-rapporto-oad-2023-ora-scaricabile.html
Tutti i precedenti rapporti sono archiviati, e scaricabili, anno per anno da https://www.oadweb.it/it/rapporti-e-relativi-convegni.html

2.3 Le fasi di OAD 2024

Il quadro complessivo delle attività previste per OAD 2024 è articolato, mese per mese, nelle seguenti attività (calendario di massima che potrà subire cambiamenti):

- **GENNAIO 2024**
  - Impostazione iniziativa OAD 2024 nell'ambito del Comitato Direttivo AIPSI
  - Stesura proposte di sponsorizzazione e richieste di patrocinio gratuito e loro invio a potenziali aziende ed enti interessati

- **FEBBRAIO 2024**
  - Definizione ed installazione-attivazione questionario online sulla piattaforma oadweb.it
  - Inizio campagna promozionale per la compilazione dei questionari
  - Continuano i contatti per i patrocini e per le sponsorizzazioni

- **MARZO - GIUGNO 2024**
  - Continua la campagna promozionale per la compilazione dei questionari
  - Continuano i contatti per i patrocini e per le sponsorizzazioni

- **MAGGIO-GIUGNO 2024**
  - 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 specifica promozione per la compilazione dei questionari persona per persona, in particolare con riferimento a CIO e CISO

- **GIUGNO-LUGLIO 2024**
  - Elaborazione dati raccolti dai questionari online
  - Stesura del Rapporto finale OAD 2024 e sua pubblicazione

- Inizio campagna promozionale per il download del Rapporto OAD 2024 da parte dei Soci dei Patrocinatori, degli interlocutori degli Sponsor e di tutti i possibili interessati contattati tramite i vari canali AIPSI
- Evento "ibrido" (incontro fisico e da remote in audio videoconferenza) AIPSI di presentazione ufficiale del Rapporto OAD 2024 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 2024**
  - Stesura e/o ausilio alla stesura di note ed articoli sui vari media inerenti il Rapporto OAD 2024 ed i dati pubblicati.
  - Realizzazione dei primi webinar e della pubblicazione di articoli per Sponsor Gold e Diamond

- **SETTEMBRE-DICEMBRE 2024**
  - Fornitura periodica agli Sponsor dei dati di download del Rapporto OAD 2024
  - Partecipazione di AIPSI-OAD a vari eventi presentando, in funzione del tema in oggetto, alcuni dei dati emersi dall'indagine OAD 2024.

3. PERCHÉ CONVIENE SPONSORIZZARE OAD 2024

La sponsorizzazione di OAD 2024 consente ad ogni aziende/ente, in particolare alle imprese dell'offerta ICTe della cyber security, di ottenere una **importante e qualificata visibilità** della loro azienda/ente e dei prodotti/servizi offerti, grazie alle schede degli Sponsor pubblicate nell'Allegato C del Rapporto OAD 2024, al loro logo sulla copertina del Rapporto e presentato anche nei vari convegni e a tutte le iniziative concordate per e con gli Sponsor da AIPSI.
Visibilità accentuata dal fatto che chi completa la parte sulle misure di sicurezza nel questionario ha immediatamente una valutazione del livello di sicurezza digitale del sistema informativo alla base delle sue risposte. E, in caso di valutazione negativa, ha subito a disposizione i riferimenti delle aziende sponsor che potrebbero aiutarlo nel migliorare il livello di sicurezza digitale: un "time to market" immediato!
Sponsorizzando si contribuisce inoltre, e fattivamente, alla r**ealizzazione dell'unica e consolidata indagine in Italia via web sulla sicurezza digitale** e **si fa conoscere la propria azienda ed i propri brand** alle migliaia di interlocutori di AIPSI, lettori dei rapporti e degli articoli su OAD, e che partecipano ai vari eventi dell'associazione: tutti professionisti interessati a vario titolo alla sicurezza digitale e potenziali acquirenti.
I vari eventi AIPSI, la circolazione dei dati del rapporto in numerosi convegni e, soprattutto, la loro circolazione nelle business community qualificate di decisori ed "influencer ICT" permette agli Sponsor di ottenere una loro ampia visibilità e presenza online sui temi della sicurezza digitale.

4. LE POSSIBILI SPONSORIZZAZIONI PER OAD 2024

La sponsorizzazione di OAD 2024 prevede tre alternative possibili, nel seguito dettagliate:

1. **Silver**, la sponsorizzazione di base dal costo di **€ 2.000,00 + IVA,** che da diritto**:**
    a. al **logo dello Sponsor** sul questionario online e sulla copertina del Rapporto 2024 OAD;
    b. a **una pagina A4** all'interno del Rapporto 2020 di presentazione "istituzionale" dello Sponsor, che evidenzi anche il ruolo della sicurezza ICT nel suo business e/o attività;
    c. alla disponibilità delle figure e dei grafici del Rapporto 2024 in alta definizione per eventuali pubblicazioni on line (blog, siti web, social net, ecc.) o su carta (anche intestata) da parte dello Sponsor; AIPSI richiede **obbligatoriamente** di pubblicare sempre, per ogni figura, **©OAD 2024** (già presente nelle figure e nei grafici forniti, e da non cancellare);
    d. all'evidenza del logo dello Sponsor in tutte le presentazioni relative a OAD che si faranno in vari Convegni (a conferma si veda la documentazione per i vari eventi delle precedenti edizioni sul sito oadweb.it);
    e. al logo dello Sponsor nella pagina web OAD e AIPSI che specificano come scaricare il Rapporto OAD 2024;
    f. alla promozione dell'iniziativa OAD sui social network e altri media in cui AIPSI, Malabo ed i vari Patrocinatori e Sponsor sono attivi.

    Allo Sponsor Silver viene emessa da AIPSI una sola fattura di € 2.000,00 + IVA alla ricezione dell'ordine; il pagamento deve avvenire entro 30 giorni dalla data della fattura.

2. **Gold**, dal costo di **€ 5.000,00 + IVA, che** che da diritto**, in aggiunta** e/o in modifica a quanto previsto per quella Silver:
    a. a una maggior dimensione del logo dello Sponsor nella copertina del Rapporto e nei siti di AIPSI e di OAD come Sponsor Gold;
    b. fino a **due pagine A4** nella sua presentazione istituzionale nell'Allegato C del Rapporto OAD 2024;
    c. alla partecipazione di un rappresentante dello Sponsor alla **Tavola Rotonda** del webinar di presentazione del Rapporto OAD 2024.

    E' possibile pagare in una unica soluzione o in due. Allo Sponsor Gold possono essere emesse da AIPSI anche 2 fatture, la prima di € 3.000,00 + IVA alla ricezione dell'ordine, la seconda di € 2.000,00 + IVA alla pubblicazione del Rapporto finale. Il pagamento deve avvenire entro 30 giorni dalla data delle fatture.

3. **Diamond, dal costo di € 10.000,00 +IVA,** che da diritto**, in aggiunta** e/o in modifica a quanto previsto per quella Gold:
    a. ad una ancor maggior dimensione del logo dello Sponsor nella copertina del Rapporto e nei siti di AIPSI e di OAD come Sponsor Diamond;
    b. **fino a 3 pagine A4** nella sua presentazione istituzionale nel Rapporto (Allegato C);
    c. alla possibilità di partecipare e collaborare nella definizione delle domande e delle risposte nel questionario OAD 2024, se l'ordine firmato per la sponsorship avviene entro il 15/3/2024;
    d. all'inserimento del logo e del link al sito dello Sponsor Diamond nella home page del sito AIPSI sotto la dicitura "Sponsor AIPSI 2024";
    e. alla possibilità per una persona di vertice (top manager) dello Sponsor Diamond di partecipare ai Consigli Direttivi di AIPSI per l'intero anno 2024, suggerendo/proponendo specifiche iniziative;

f. alla realizzazione di un **evento/webinar specifico AIPSI-Sponsor,** i cui contenuti, che includeranno alcuni dei dati emersi dall'indagine 2024, saranno concordati con AISPI. Il webinar potrà utilizzare la piattaforma o di AIPSI o quella fornita dallo Sponsor Diamond stesso;
g. alla **realizzazione di una articolo ad hoc,** in collaborazione con AIPSI, da pubblicare sui siti web di AIPSI e di OAD, e su una o più riviste scelte tra quelle dei Media Partner AIPSI o indicate dallo Sponsor (la fattibilità di quest'ultima opzione non può essere garantita a priori da AIPSI).

E' possibile pagare in una unica soluzione o in due. Allo Sponsor Diamond possono essere emesse da AIPSI anche 2 fatture, la prima di € 6.000,00 + IVA alla ricezione dell'ordine, la seconda di € 4.000,00 + IVA alla pubblicazione del Rapporto finale. Il pagamento deve avvenire entro 30 giorni dalla data delle fatture.

5. LA PROPRIETÀ INTELLETTUALE DI OAD 2024

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 2024, 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 2024**.

6. COME ADERIRE ALLA SPONSORIZZAZIONE DI OAD 2024

Per aderire alla sponsorizzazione di OAD 2024 basta completare tutte le voci della scheda di adesione a **pagina 13**, firmarlo da parte di chi ha i poteri di firma, scannerizzarlo ed inviarlo in posta elettronica come allegato alla PEC aipsi@gigapec.it. Dopo la ricezione del modulo, il richiedente sarà contattato telefonicamente e/o via e-mail, e verrà poi emessa da AIPSI la relativa fattura.

6.1 Arco temporale disponibile per sottoscrivere la sponsorizzazione

L'arco temporale per la sottoscrizione della presente offerta va da **gennaio 2024 a giugno 2024**, ed ha di fatto il limite massimo di **2-3 settimane prima che venga pubblicato il Rapporto finale**, perché si possa inserire la scheda dello Sponsor nell'Allegato C ed il suo logo in copertina.
E' bene evidenziare che **prima** l'Azienda/Ente conferma la propria sponsorizzazione, **più a lungo** il suo logo ed il suo link saranno visibili e seguiti dai visitatori dei siti web, dei social, degli eventi che promuoveranno OAD 2024 e la compilazione del questionario online.

MODULO SPONSORIZZAZIONE OAD 2024

da inviare, dopo averlo completato, firmato e scannerizzato, alla PEC aipsi@gigapec.it

La nostra Società/Ente conferma ad AIPSI la propria sponsorizzazione a OAD 2024 con la scelta di sponsorizzazione sotto selezionata, **con i relativi diritti e alle condizioni dettagliate nelle pagine precedenti** della presente proposta (*porre una croce sulla casella prescelta*)

☐	Sponsorizzazione Silver	€ 2.000,00 + IVA
☐	Sponsorizzazione Gold	€ 5.000,00 + IVA
☐	Sponsorizzazione Diamond	€ 10.000,00 + IVA

Società: .....

Indirizzo: .....

Città: ..... **Cap**: ..... **Prov**: .....

Partita IVA/Codice Fiscale: .....

Codice destinatario per fattura elettronica: .....

PEC: .....

Verrà da noi emesso un ordine d'acquisto*:* NO/SI **N. ORDINE**: .....

Persona operativa di riferimento

Nome: ..... **Cognome:** .....

Tel.: .....**Cell**.: .....**E-mail:** .....

Responsabile con potere di firma

Nome: .....**Cognome :** .....

Ruolo: .....

Tel.: .....**Cell**.: .....**E-mail:** .....

***Firma del Responsabile*:** .....

Luogo: .....***Data***: .....

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

MALABO S.r.l.
www.malaboadvisoring.it
Sede operativa: Via Savona 26 - 20144 Milano
Tel: +39 02 39443632
E-mail: info@malaboadvisoring.it
Sede Legale: Via del Caravaggio 14 20144 Milano
Partita IVA: 13343460153