

The logo for OAD (Osservatorio Attacchi Digitali in Italia) features the letters 'OAD' in a bold, white, sans-serif font, set against a solid blue rectangular background.

Osservatorio
Attacchi Digitali
in Italia

PROPOSTA SPONSORSHIP OAD 2020

UNA INIZIATIVA CONGIUNTA



CON LA COLLABORAZIONE DI



V3
Giugno 2020

Sommario

1. PREMESSA	3
2. PERCHÉ OAD.....	3
3. LA STORIA DI OAD	4
4. LE NOVITÀ 2020 NEL QUESTIONARIO E NEL RAPPORTO OAD	5
5. PER MEGLIO MOTIVARE E RINGRAZIARE I RISPONDENTI AL QUESTIONARIO 2020 OAD	8
7. PERCHÉ SPONSORIZZARE OAD 2020	9
8.1 Sponsorizzazione Silver.....	10
8.2 Sponsorizzazione Gold	11
9. LA PROPRIETÀ INTELLETTUALE DI OAD 2020.....	12
10. COME ADERIRE ALLA SPONSORIZZAZIONE DI OAD 2020	12
10.1 Arco temporale disponibile per confermare la sponsorizzazione a OAD 2020.....	12
MODULO DI ADESIONE SPONSORIZZAZIONE OAD 2020	13

1. PREMESSA

L'iniziativa OAD, Osservatorio Attacchi Digitali in Italia (già conosciuto negli scorsi anni come OAI, Osservatorio Attacchi Informatici in Italia), nel 2020 arriva a ben 12 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 dell'autore Marco R. A. Bozzetti che realizza l'indagine on line, elabora i dati raccolti e stende il rapporto finale, e Reportec Srl (www.reportec.com), il media partner, oltre al maggior coinvolgimento di AIPSI, Associazione Italiana Professionisti Sicurezza Digitale, capitolo italiano di ISSA (www.aipsi.org, www.issa.org).

Grazie alla collaborazione tra AIPSI, Malabo e Reportec, l'iniziativa OAD intende aumentare continuamente l'autorevolezza, la visibilità e la diffusione dei Rapporti OAD sugli attacchi digitali in Italia: e in tale ottica è stato realizzato un sito web ad hoc, <https://www.oadweb.it/>, sia in Italiano che in Inglese, che costituisce l'archivio storico di tutti i rapporti OAI e OAD pubblicati, e di tutte le presentazioni ed articoli che su di essi sono stati realizzati.

Anche per il 2020 verrà realizzata l'indagine OAD sugli **attacchi rilevati nel corso dell'intero 2019 e nel primo quadrimestre 2020** da aziende ed enti operanti con Sistemi Informatici, o loro parti, sul territorio italiano. E per fornire una **più forte motivazione** alle/ai potenziali rispondenti al questionario on line, quest'ultimo fornirà a chi completa il questionario **una stima qualitativa del livello di sicurezza del sistema informatico** cui fa riferimento nelle risposte.

Grazie ai numerosi patrocini con varie associazioni, anche di categoria e non solo del mondo digitale, si tende ad allargare l'indagine alla quasi totalità dei settori merceologici (OAD segue la classificazione ATECO) e alle Pubbliche Amministrazioni, per poter avere indicazioni settoriali significative come numero di rispondenti.

2. PERCHÉ OAD

L'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 tramite una indagine anonima indirizzata a tutte le aziende e alle Pubbliche Amministrazioni** di ogni settore merceologico e dimensione. **tramite un questionario compilabile on line con un browser**. Il questionario è rivolto principalmente ai Responsabili dei Sistemi Informativi e della Sicurezza Informatica.

Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT.

I potenziali rispondenti sono contattati principalmente via e-mail (ed eventualmente sollecitati successivamente con chiamate telefoniche) grazie alle banche dati degli organizzatori e delle associazioni patrocinate: complessivamente vengono contattate, talvolta da più Enti contemporaneamente, più di 5.000 persone del mondo delle aziende, del commercio, dei servizi, degli studi professionali e delle Pubbliche Amministrazioni

La disponibilità di dati "locali all'Italia" sugli attacchi digitali intenzionali rilevati, sulla tipologia e sull'ampiezza del fenomeno è fondamentale anche per le organizzazioni di piccole dimensioni per

valutare i possibili rischi e attivare le misure più idonee di prevenzione e protezione, così come richiesto da numerose normative nazionali ed internazionali, non ultimo il **GDPR**, il regolamento europeo sulla privacy. Per la prima volta nell'edizione 2020 chi completa il questionario on line avrà anche in tempo reale una valutazione di sintesi di come le misure di sicurezza digitale indicate rispondano effettivamente alle esigenze di sicurezza digitale indicate per l'azienda/ente ed il suo sistema informatico: una seria, anche se sintetica, valutazione gratuita del livello di sicurezza digitale in essere, in funzione delle risposte fornite. OAD, con la sua indagine e con il supporto di AIPSI, intende inoltre contribuire alla "sensibilizzazione" in Italia sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti. Quest'ultimo obiettivo è particolarmente importante per creare una più diffusa cultura in materia di sicurezza digitale, che va oltre il mondo tecnico-informatico e tocca anche i vertici dell'organizzazione e tutti coloro che decidono requisiti e budget della sicurezza digitale nei processi organizzativi delle proprie strutture.

3. LA STORIA DI OAD

Nove i Rapporti annuali OAI finora pubblicati (le loro copertine in fig. 1), dal 2008 al 2020: tutti questi rapporti sono scaricabili dallo specifico sito creato per OAD, www.oadweb.it. Fino al 2015 l'indagine era conosciuta con l'acronimo OAI, Osservatorio Attacchi Informatici Italia, dal 2016 ha cambiato nome e logo sostituendo al termine "Informatica" quello di "Digitale", per meglio evidenziare che l'indagine verte su ogni sistema ICT, Information and Communication Technology, in suo presso le aziende/enti. Si noti che sulle copertine di ogni rapporto, a partire da quello del 2012, sono presenti i loghi degli Sponsor (e all'interno del Rapporto c'è la scheda di presentazione di ogni Sponsor).



Fig. 1 Le copertine dei Rapporti OAD-OAI pubblicati

Con le varie edizioni di OAI e di OAD, è andato crescendo il numero di Patrocinatori, da varie libere associazioni del mondo ICT ad associazioni di categoria e di rappresentanza di Ordini, quali Assintel, Assolombarda, FiiF -CNF). I Patrocinatori consentono l'ampliamento del bacino dei possibili

rispondenti al questionario annuale, oltre che dei lettori del Rapporto, ed è obiettivo di OAD di ampliare il numero di associazioni patrocinanti, per poter anche ampliare il numero di rispondenti e di lettori, soprattutto per i settori merceologici poco rispondenti, e quindi rappresentati, nelle precedenti edizioni.

La pubblicazione dei Rapporti, a conclusione delle indagini annuali, è stata l'occasione, anno per anno, per la partecipazione a vari Convegni e Workshop, oltre che per la pubblicazione di articoli su riviste italiane e straniere. Le edizioni di OAD/OAI dal 2012 sono state oggetto di sponsorship da parte di aziende del settore che hanno utilizzato i Rapporti per rafforzare la loro "brand awareness" e la relazione con i decisori, gli addetti ai lavori e gli influencer per i loro sistemi e servizi di sicurezza digitale. Gli articoli e le pubblicazioni inerenti alle diverse edizioni OAI/OAD sono disponibili sul sito web di OAD, www.oadweb.it, e referenziate su questo dai siti di AIPSI (www.aipsi.org), di Malabo Srl (www.malaboadvisoring.it), di alcuni Sponsor e Patrocinatori.

Il numero di Rapporti delle versioni precedenti scaricati dal sito OAD o distribuiti via posta elettronica, file transfer, condivisione di file, etc. sono andati man mano crescendo negli ultimi anni, fino a raggiungere negli ultimi due anni, in un numero per edizione stimabile tra 1000 e 1500. Questo dato è una stima forse riduttiva, dato che in molti casi gli stessi Sponsor e Patrocinatori hanno fatto avere i Rapporti OAD ai loro interlocutori tramite vari canali, ma mai comunicando quanti e chi erano. Allo stesso modo molti lettori hanno a loro volta distribuito il Rapporto tramite loro canali, a partire dalla posta elettronica, senza comunicare a OAD a chi l'avevano inoltrato.

Scaricare il Rapporto dal sito OAD è gratuito, ma richiede una semplice e veloce registrazione al sito, così da poter tracciare a chi interessa ed avere un preciso numero di download. Ma proprio questo, probabilmente, suscitare timore nel potenziale interessato, che teme, col registrarsi, di essere subissato da pubblicità ed inviti da AIPSI e dagli Sponsor: questo è sicuramente uno dei motivi per cui molti interessati preferiscono avere la copia del Rapporto dai loro interlocutori in e-mail o con altri mezzi, che non richiedono una specifica registrazione.

Come per le precedenti edizioni, la sponsorizzazione a OAD 2020 è rivolta ad Aziende ed Enti, sia lato offerta sia lato domanda ICT.

4. LE NOVITÀ 2020 NEL QUESTIONARIO E NEL RAPPORTO OAD

Rispetto agli anni precedenti, il questionario 2020 presenta un'importante novità: le sezioni relative alle principali caratteristiche del Sistema Informatico della/del rispondente, ed alle sue misure di sicurezza digitale tecniche ed organizzative in essere, sono state profondamente modificate per:

- Semplificare le domande e le risposte, soprattutto quelle più tecniche, così da facilitare la loro selezione;
- Pesare opportunamente le risposte fornite sulle misure di sicurezza digitale in essere, correlandole alle caratteristiche principali del Sistema Informatico, per fornire alla/al rispondente, in tempo reale alla fine della compilazione del questionario, una **valutazione qualitativa del livello di sicurezza** in essere, rispetto alle esigenze di sicurezza dell'azienda/ente; tipici esempi: buono, sufficiente, insufficiente, molto critico.
 - Questa valutazione viene fornita con un **Indice di Sicurezza Digitale**, rappresentato dalla differenza tra il peso delle necessità di sicurezza digitale derivate dal tipo di

azienda/ente e del suo sistema informatico e dal peso delle misure di sicurezza tecniche ed organizzative in uso. I pesi sono calcolati in base alle varie risposte fornite nella compilazione del questionario. La risposta fornita è una indicazione qualitativa. La fig. 2 sottostante mostra un esempio tipo della risposta che viene fornita alla/al rispondente al termine della compilazione.



Fig.2 Esempio della risposta sul livello di sicurezza che viene fornito alla fine della compilazione del questionario,

L'indagine 2020 OAD considera gli **attacchi intenzionali rilevati nel 2020 e nel 1° quadrimestre 2020**. Dato che il Rapporto finale sull'indagine non potrà che essere pubblicato verso novembre 2020, il riferimento al 1° quadrimestre 2020 consente di fornire un documento aggiornato, almeno in parte, anche sull'anno di pubblicazione.

Nel rapporto finale, oltre ai grafici ed ai commenti su questi dati si aggiunge uno specifico capitolo sui **dati forniti dalla Polizia Postale e delle Telecomunicazioni**, sempre riguardanti l'intero 2020 ed il 1° quadrimestre 2020.

La sezione iniziale, sugli attacchi rilevati, rimane sostanzialmente come quella dell'anno precedente. Si articola nelle diverse tipologie di attacco, in funzione del che cosa viene attaccato, (più avanti dettagliate) e per ciascun tipo sono poste specifiche domande su:

- le possibili tecniche di attacco usate (più avanti dettagliate);
- i più gravi impatti riscontrati dall'attacco più grave;
- le possibili motivazioni per l'attacco più grave;
- il tempo massimo per il ripristino del Sistema Informatico dopo aver subito l'attacco più grave.

Per velocizzare il tempo di risposta, se un tipo di attacco non è stato rilevato si saltano in automatico tutte le sotto domande e si passa alla domanda successiva. Se nella prima domanda si afferma che non si sono rilevati attacchi, si salta direttamente alle domande sugli attacchi più temuti nel prossimo futuro.

L'indagine 2020 OAD individua 15 tipologie di attacchi digitali basate su che cosa viene attaccato, separandole il più chiaramente possibile dalle tecniche usate per portare l'attacco.

Le 15 tipologie di attacco (il che cosa si attacca) alla data considerate sono:

1. Distruzione fisica di dispositivi ICT o di loro parti
2. Furto di dispositivi d'utente mobili (PC, server, storage system, etc.)
3. Furto di dispositivi ICT fissi o di loro parti
4. Furto informazioni da sistemi ICT fissi
5. Furto informazioni da sistemi d'utente mobili (palmari, smartphone, tablet, etc.)
6. Attacchi all'identificazione, autenticazione e autorizzazioni degli utenti finali e privilegiati
7. Attacchi alle reti, locali e geografiche, fisse e wireless, e ai DNS
8. Attacchi ai singoli sistemi ICT nel loro complesso (dai dispositivi d'utente ai server-storage e ai servizi in cloud)
9. Attacchi per modifiche non autorizzate ai programmi applicativi e alle loro configurazioni
10. Attacchi per modifiche non autorizzate alle informazioni trattate dai sistemi ICT
11. Attacchi per saturazione risorse digitali (DoS/DDoS)
12. Attacchi ai propri sistemi in cloud o in housing/hosting presso fornitori terzi
13. Attacchi a dispositivi IoT (Internet of Things) in uso
14. Attacchi ai propri sistemi di automazione industriale e di robotica (OT, Operational Technology)
15. Attacchi a sistemi e/o servizi basati su blockchain

Le classi di tecniche di attacco attualmente 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 (come ad es. APT, Advanced Persistent Threat)

La struttura del Rapporto 2020 OAD, di circa 160 pagine formato A4, sarà articolata, come schema di massima, nei seguenti capitoli:

- Sintesi direzionale in italiano
- Executive Summary in inglese
- Introduzione
- Gli attacchi digitali rilevati dai rispondenti
 - La distribuzione percentuale degli attacchi rilevati per settore merceologico e per dimensioni di azienda/ente
 - Per ogni tipologia di attacco il dettaglio, in dettagliate in percentuali, grazie ai dati elaborati dai questionari, il tipo di tecnica usata, l'impatto subito, il tempo max di ripristino nell'attacco più critico, etc.
- Come sono stati rilevati e come sono gestiti gli attacchi digitali, ed i principali impatti economici subiti
- Strumenti e misure di sicurezza ICT adottate
 - Sicurezza fisica

- Sicurezza logica
- Gli strumenti per la gestione della sicurezza digitale
- Le misure organizzative e la conformità a standard e a “buone pratiche”
- Audit sicurezza digitale
- Gli attacchi più temuti nel prossimo futuro
- Il campione di rispondenti e delle loro aziende/enti emerso dall’indagine e le macrocaratteristiche dei sistemi informatici e delle loro misure di sicurezza in uso per il campione emerso
- I dati forniti dalla Polizia Postale e delle Telecomunicazioni
 - Infrastrutture critiche (C.N.A.I.P.I.C.) e computer crime
 - Financial Cyber Crime
 - Cyber Terrorismo
- 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” di 1 pagina A4 per ogni Sponsor)
- Allegato D – Profili Patrocinatori (logo, URL sito web, 3-4 righe descrizione)
- Allegato E – Riferimenti e fonti
- Allegato F – Profilo Autore del Rapporto 2020 OAD
- Allegati G, H, I - Profili AIPSI, Malabo, Reportec

5. PER MEGLIO MOTIVARE E RINGRAZIARE I RISPONDENTI AL QUESTIONARIO 2020 OAD

Per la buona riuscita dell’indagine OAD è fondamentale la più ampia partecipazione di rispondenti di vari settori merceologici e delle Pubbliche Amministrazioni, centrali e locali.

Per motivarli il più possibile, la presente edizione 2020:

- ha introdotto la **valutazione di sintesi del livello di sicurezza digitale** in essere per il sistema informatico oggetto delle risposte, come illustrato in §4
- offre la possibilità di scaricare gratuitamente, sempre al termine della compilazione dell’intero questionario 2020, in formato pdf:
 - il numero di **maggio 2020** di **ISSA Journal**, che tratta un argomento di frontiera nell’evoluzione delle tecniche per la sicurezza digitale: la crittografia quantistica;
 - la seconda edizione 2019, l’ultima ad oggi, del libro di G. Saccardi, G. Di Blasio, R. Florio "**Information Security e Data Protection 2019**", pubblicato per i tipi di Reportec.

6. LA SCHEDULAZIONE DI OAD 2020

Il quadro complessivo delle attività previste dal progetto è la seguente:

- fine APRILE – inizio MAGGIO 2020: lancio di OAD 2020
- MAGGIO – GIUGNO 2020
 - preparazione Questionario 2020 OAD
 - attivazione strumenti web per la raccolta delle risposte al questionario via web
 - acquisizione sponsorizzazioni e patrocini
 - inizio campagna per la compilazione del Questionario verso tutti i potenziali rispondenti (CIO, CISO, CTO, CEO piccole imprese, etc.) grazie alle mailing list di AIPSI, Malabo, Reportec, e di tutti gli Enti Patrocinatore, oltre che degli Sponsor;
- LUGLIO- SETTEMBRE 2020
 - Continua l'acquisizione di sponsorizzazioni e patrocini
 - Continua la campagna per la compilazione del Questionario con solleciti ed avvisi tramite diversi canali di comunicazione quali banner, newsletter, social, partecipazione ad eventi, etc.
 - attivazione strumenti per il download del Rapporto 2020
- SETTEMBRE – OTTOBRE 2020
 - raccolta, analisi questionari compilati ed elaborazione dati di sintesi
 - stesura Rapporto 2020
 - pubblicazione comunicato stampa
 - Inizio campagna per presso gli interessati per il download del Rapporto 2020
 - presentazione principali risultati a SMAU Milano e in altri convegni e workshop
 - pubblicazione articoli sul Rapporto 2020 su riviste
- FINE OTTOBRE - NOVEMBRE 2020
 - Realizzazione webinar con gli Sponsor Gold (si veda §8.2)
 - Pubblicazioni articoli per gli Sponsor Gold (si veda §8.2)
 - Partecipazione ad eventi e convegni
- DICEMBRE 2020 - 1° Trimestre 2021
 - Fornitura periodica agli Sponsor dell'elenco di chi ha scaricato il Rapporto
 - Continua la partecipazione ad eventi e convegni in cui si citano i dati OAD 2020.

7. PERCHÉ SPONSORIZZARE OAD 2020

La sponsorizzazione di OAD 2020 consente alle Imprese dell'Offerta ICT, e in particolare della cyber security, ma anche alle Imprese/Enti della Domanda, di ottenere una **importante e qualificata loro visibilità** nel settore della sicurezza digitale e dell'informatica in Italia, grazie alle proprie schede istituzionali all'interno del Rapporto 2020, al proprio logo sulla copertina e nelle numerose presentazioni dei dati OAD nei vari convegni, a tutte le iniziative concordate per gli Sponsor Gold.

Visibilità accentuata dal fatto che chi completa il questionario ha immediatamente una valutazione del livello di sicurezza digitale del sistema informatico alla base delle sue risposte. E soprattutto in caso di valutazione negativa, ha subito in mente le aziende sponsor che potrebbero aiutarlo nel migliorare il livello di sicurezza digitale: un'azione

Vengono inoltre inviati agli Sponsor l'elenco di chi ha scaricato il Rapporto OAD 2020 dal sito OAD e di chi ha partecipato ai vari eventi OAD 2020 e/o scaricato la documentazione relativa e gli articoli pubblicati su OAD 2020.

Non ultimo, sponsorizzando OAD 2020 si contribuisce alla realizzazione dell'unica e consolidata indagine in Italia via web sull'argomento cyber security e si fa conoscere la propria azienda alle migliaia di lettori dei Rapporti, dei webinar, degli articoli su OAD, tutti professionisti interessati a vario titolo alla sicurezza digitale.

Gli eventi OAD, 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 immediata visibilità e "presenza" online associata ad un tema di grande rilevanza e a contenuti di elevato e qualificato valore.

Con la sponsorizzazione Gold (si veda §8.2) si ha inoltre la possibilità di realizzare con gli specialisti di Malabo Srl, di Reportec Srl e di AIPSI uno specifico webinar inerente OAD 2020 per ogni singolo Sponsor Gold, oltre alla redazione di uno specifico articolo per lo Sponsor Gold sulla rivista on line "Security & Business" di Reportec.

8. LA SPONSORIZZAZIONE DI OAD 2020

OAD 2020 prevede due tipi di sponsorizzazione possibili, nel seguito dettagliate:

1. **Silver**, la sponsorizzazione di base dal costo di **€ 2.000,00 + IVA**
2. **Gold**, che oltre a tutti i diritti della Silver aggiunge due pagine A4 nella sua presentazione istituzionale nel Rapporto (Allegato C), ad un webinar ad hoc realizzato solo per lui, ad un articolo ad hoc sulla rivista Security& Business dell'Editore Reportec, dal costo di **€ 5.000,00 + IVA**

8.1 Sponsorizzazione Silver

E' la sponsorizzazione di base e dà diritto allo Sponsor:

- al logo dello Sponsor sul questionario online e sulla copertina del Rapporto 2020
- a **una pagina A4** all'interno del Rapporto 2020 di presentazione "istituzionale" dello Sponsor, che evidenzia anche il ruolo della sicurezza ICT nel suo business e/o attività;
- alla disponibilità delle figure e dei grafici del Rapporto 2020 in alta definizione per eventuali pubblicazioni on line (blog, siti web, social net, ecc.) o su carta (anche intestata) da parte dello Sponsor; si richiede di pubblicare sempre, per ogni figura, il logo ©OAD 2020 (normalmente già presente nelle figure e nei grafici forniti, e da non cancellare);
- all'evidenza del logo dello Sponsor in tutte le presentazioni relative a OAD 2020 che si faranno in vari Convegni (ad esempio nel passato: SMAU, AICA, eventi AIPSI/ISSA, Club TI Milano-Assolombarda, Fida Inform, etc.);
- al logo dello Sponsor nella pagina web AIPSI per scaricare il Rapporto 2020;
- all'elenco dei nominativi, dell'azienda di appartenenza e dell'indirizzo e-mail di chi ha scaricato il Rapporto. Questo è probabilmente il diritto più importante per le aziende sponsor: chi si registra sul sito OAD per poter scaricare i rapporti, oltre ad altra documentazione, **fornisce il consenso esplicito a fornire il suo nominativo ed indirizzo e-mail agli Sponsor, oltre che ad Aipsi, Malabo e Reportec**. Si veda nella sottostante fig.2 il form di registrazione con il consenso esplicito.

- alla promozione dell’iniziativa OAD 2020 sulle riviste di Reportec oltre che su altre, e quindi dei loghi degli Sponsor, sui social network e media in cui OAD, AIPSI, Malabo, Reportec ed i vari Patrocinatori e Sponsor sono attivi.
- alla partecipazione ad un webinar sulla presentazione del Rapporto 2020 OAD e dei più interessanti dati emersi, realizzato da AIPSI in collaborazione con Malabo e Reportec.

Il prezzo della sponsorizzazione **Silver** è di **€ 2.000,00 + IVA**, da pagarsi all’ordine (si veda §10).

Il pagamento delle fatture emesse si intende a 30 g/df via bonifico bancario sulla banca indicata nella fattura stessa, emessa da Malabo Srl.



Fig. 3 Il modulo di registrazione dell’utente al sito web OAD, con la richiesta di consenso esplicito

Nella fig.3, alla fine della videata, in blu, si noti anche la richiesta di accettazione dei cookie, richiesta che appare per qualsiasi visitatore del sito da qualunque pagina del sito cui accede per la prima volta.

8.2 Sponsorizzazione Gold

La sponsorizzazione Gold dà diritto, oltre a quanto previsto per quella Silver, a:

- Maggior evidenza del logo dello Sponsor nella copertina del Rapporto e nei siti di AIPSI e di OAD come Sponsor Gold
- A **due pagine A4** nella sua presentazione istituzionale nell’Allegato C del Rapporto 2020
- Un webinar specifico con la sua sola partecipazione, curato da Malabo e Reportec, i cui contenuti, che includeranno alcuni dei dati emersi dall’indagine OAD 2020, saranno con lui concordati. Il webinar sarà attuato con la piattaforma Gotomeeting di AIPSI
- La realizzazione di una articolo ad hoc sulla rivista Security&Business dell’Editore Reportec (si veda <https://www.reportec.it/riviste-e-magazine-newsletter/security-business/>)

Il prezzo della sponsorizzazione Gold è di **€ 5.000,00 + IVA**, da pagarsi all’ordine (si veda §10).

Il pagamento delle fatture emesse si intende a 30 g/df via bonifico bancario sulla banca indicata nella fattura stessa, emessa da Malabo Srl.

9. LA PROPRIETÀ INTELLETTUALE DI OAD 2020

La proprietà intellettuale ed il copyright dell'intera iniziativa OAD 2020, inclusi il Questionario on line ed i contenuti, le figure ed i grafici del Rapporto 2020 OAD, sono, come per le precedenti edizioni, di Malabo Srl che consente il loro utilizzo agli Sponsor, con l'obbligo di citare la fonte OAD 2020 e sulle figure del Rapporto la presenza di ©OAD 2020.

10. COME ADERIRE ALLA SPONSORIZZAZIONE DI OAD 2020

Per aderire alla sponsorizzazione di OAD 2020 basta completare, anche manualmente, tutte le voci dello schema di adesione in pagina 12, firmarlo da chi ha i poteri di spesa, fotografarlo/scannerizzarlo ed inviarlo in posta elettronica come allegato a marco.bozzetti@malboadvisoring.it e/o alla PEC malabo_srl@pec.it. Dopo la ricezione del modulo, il richiedente sarà contattato telefonicamente e verrà poi emessa la relativa fattura.

10.1 Arco temporale disponibile per confermare la sponsorizzazione a OAD 2020

L'arco temporale per l'accettazione della presente offerta e del relativo pagamento va da fine aprile 2020 a fine settembre 2020, in pratica fino a 3 settimane prima venga pubblicato il Rapporto 2020 OAD.

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 di AIPSI, Malabo, OAD, Reportec.

Le Aziende/Enti che avessero chiusure dell'anno contabile nel corso del 2020 possono concordare con Malabo Srl le modalità ed i tempi di pagamento.

MODULO DI ADESIONE SPONSORIZZAZIONE OAD 2020

da inviare, dopo avere completato, firmato e scannerizzato, a marco.bozzetti@malaboadvisoring.it e/o alla PEC malabo_srl@pec.it

La nostra Società/Ente conferma la propria sponsorizzazione a OAD 2020 con la scelta di sponsorizzazione sotto selezionata, con i relativi diritti e alle condizioni dettagliate nelle pagine precedenti (*porre una croce sulla casella prescelta*)

- | | | |
|--------------------------|-------------------------|------------------|
| <input type="checkbox"/> | Sponsorizzazione Silver | € 2.000,00 + IVA |
| <input type="checkbox"/> | Sponsorizzazione Gold | € 5.000,00 + 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:**

Ruolo aziendale:

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

Responsabile con potere di firma

Nome: **Cognome :**

Ruolo aziendale:

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

Firma del Responsabile:

Luogo: **Data:**

AIPSI

www.aipsi.org

Sede Centrale: 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

REPORTEC S.r.l.

www.reportec.it

Via Marco Aurelio 8 - 20127 Milano

Tel: +39 02 36580441 E-mail: info@reportec.it

Partita IVA: 03704060965