L'iniziativa OAD
e
l'indagine OAD 2023
di AIPSI

Ultimo aggiornamento: 16/05/2023

Osservatorio Attacchi Digitali in Italia

Sommario

1. L'INIZIATIVA 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 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 si è consolidata anche grazie alla partnership tra **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, e **Malabo Srl** (www.malaboadvisoring.it), la società dell'ideatore dell'iniziativa, Marco R. A. Bozzetti, che realizza l'indagine online, elabora i dati raccolti e stende il rapporto finale, **indipendentemente** dalle eventuali sponsorizzazioni ottenute da AIPSI per coprire, almeno parzialmente, i costi per la realizzazione dell'intera iniziativa.

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 principalmente 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 far conoscere il più ampiamente possibile **l'effettiva realtà in Italia del fenomeno degli attacchi digitali intenzionali** ai sistemi informativi di aziende ed enti pubblici operanti 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 sulla 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.

L'iniziativa OAD inoltre contribuisce alla "sensibilizzazione" e alla conoscenza in Italia della sicurezza digitale per tutti gli utenti ed i decisori dei sistemi informativi, uno degli obbiettivi di AIPSI e di ISSA (si veda https://www.issa.org/about-issa/ e https://www.aipsi.org/aree-tematiche/sig-riservati-ai-soci/crescita-e-percorsi-professionali.html). In Italia è una improrogabile necessità giungere ad una più diffusa cultura in materia di sicurezza digitale, che consideri non solo il contesto strettamente tecnico-informatico ma anche i vertici dell'organizzazione e tutti coloro che decidono in merito a requisiti e budget per la sicurezza digitale.

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/.

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.

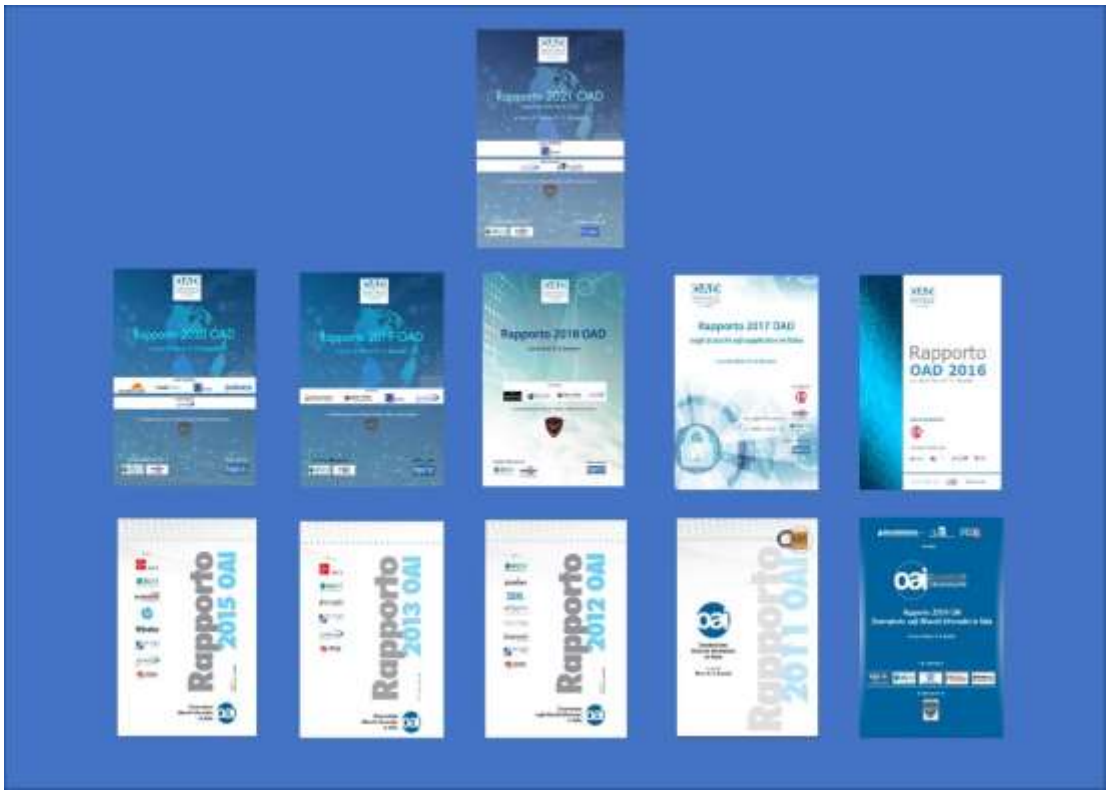

Fig. 1 Le copertine dei Rapporti OAD-OAI ad oggi pubblicati

Il target dei possibili rispondenti include i responsabili dei sistemi informativi (CIO, Chief Information Officer), della sicurezza digitale (CISO, Chief Information Security Officer e CSO, Chief Security Officer), delle tecnologie (CTO, Chief Technology Officer), il personale interno che a vario titolo si occupa di sistemi informativi e della loro sicurezza, eventuali Terze Parti e consulenti cui è stata

[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/)

terziarizzata la gestione del sistema informativo e/o della sua sicurezza; per le piccole e piccolissime organizzazioni, il vertice che sovente coincide con i proprietari (aziende private).

I potenziali rispondenti al questionario OAD sono informati dell'indagine OAD 2023 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 dai media partner di AIPSI.

AIPSI **non può garantire** la copertura completa dei vari settori merceologici e dei vari ruoli, e tantomeno possono garantire l'effettiva e fattiva collaborazione delle Associazioni patrocinanti, con una significativa risposta da parte dei loro associati.

Per poter coprire i diversi settori merceologici, oltre che le Pubbliche Amministrazioni Centrali e Locali, ampliando il più possibile il bacino di potenziali rispondenti all'anonimo questionario online, AIPSI richiede il patrocinio gratuito di associazioni di rappresentanza e di enti no profit che vi operino.

AIPSI propone anche delle sponsorizzazioni ad aziende/enti che servono solo a coprire una parte (storicamente purtroppo assai piccola) dei costi per la realizzazione dell'indagine, dall'impostazione del questionario online all'elaborazione dei dati raccolti e alla stesura del rapporto finale.

2. OAD 2023

2.1 Piano di lavoro OAD 2023

- **GENNAIO 2023**
  - Impostazione OAD 2023
  - Preparazione proposte di patrocinio ed inizio contattati con le varie Associazioni ed Enti no profit
  - Definizione ed installazione-attivazione questionario online sulla piattaforma oadweb.it

- **FEBBRAIO 2023**
  - Lancio campagna promozionale per la compilazione del questionario online OAD 2023
  - Correzioni questionario OAD 2023 dopo i primi test sul campo
  - Creazione banner OAD 2023

- **MARZO – LUGLIO 2023**
  - Continua campagna promozionale per la compilazione dei questionari
  - Continuano i contatti per i patrocini ed il potenziale allargamento del bacino di rispondenti
  - In funzione di se e quando si raggiungerà il numero minimo di rispondenti necessari perché un'indagine web anonima sia significativa, AIPSI effettuerà, tra giugno e luglio

e in collaborazioni con i Patrocinatori, una specifica promozione per la compilazione dei questionari persona per persona, in particolare con riferimento a CIO e CISO

- **LUGLIO – AGOSTO 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 interessati, contattati tramite i vari canali mediatici.

- **SETTEMBRE 2023**
  - Continua la campagna per il download del Rapporto OAD 2023 da parte degli interessati, contattati tramite i vari canali mediatici di AIPSI e dei Patrocinatori
  - 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.
  - 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 con i Patrocinatori e gli eventuali Sponsor.

- **OTTOBRE-DICEMBRE 2023**
  - Realizzazione e/o partecipazione di AIPSI a vari eventi presentando, in funzione del tema in oggetto, i dati emersi dall'indagine OAD 2023
  - Inizio impostazione OAD 2024

Data la libera ed anonima compilazione del questionario, AIPSI non può garantire la copertura "bilanciata" dei vari settori merceologici, e tantomeno può garantire l'effettiva e fattiva collaborazione delle Associazioni patrocinanti, con una significativa risposta da parte dei loro associati. La campagna intrapresa e in corso con tutti questi interlocutori, e la riduzione del numero di domande nei questionari, dovrebbero portare ad un aumento del numero totale di rispondenti.

2.2 Il questionario OAD 2023 e le sue caratteristiche

Il questionario è già on line, rigorosamente **anonimo**, accessibile da ogni potenziale compilatore da: https://www.oadweb.it/ls2023/limesurvey/index.php/279362?lang=it

Per ridurre il tempo necessario a compilarlo, 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 edizioni, il questionario OAD 2023:

- si focalizza sui soli **attacchi intenzionali ai siti ed alle applicazioni web**, sia on premise che terziarizzate, rilevati nel 2022, con due sole domande sulle altre tipologie di attacco rilevate nel 2022 ai Sistemi Informativi dei rispondenti;

- rende **opzionale** rispondere al gruppo di domande sulle **misure di sicurezza, tecniche ed organizzative,** in essere, anche se raccomandate per poter avere alla fine della compilazione la macro valutazione del livello di sicurezza digitale in essere.

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 ulteriori 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, e sempre in maniera anonima, una macro valutazione qualitativa del livello di sicurezza che emerge dalle risposte fornite, con l'elenco delle risposte più critiche in termini di sicurezza digitale.

2.2.1 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 eventuali sistemi in cloud o in housing/hosting presso fornitori terzi
  - Attacchi ai propri eventuali 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 queste modalità;
- 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.

2.2.2 Le domande sulle misure di sicurezza digitali in essere

Come già indicato in precedenza, queste domande sino opzionali, ma si raccomanda fortemente la loro compilazione a tutti i rispondenti, così che possano ottenere due importanti risultati:

- una verifica delle misure di sicurezza digitali che potrebbero o dovrebbero essere implementate sui loro Sistemi Informativi;
- 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 relativamente più gravi mancanze in determinate misure di sicurezza. In pratica una prima indicazione dei principali miglioramenti nella sicurezza digitale che sarebbe opportuno realizzare.

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.

2.2.3 Per ringraziare i rispondenti al questionario 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.

2.2.4 Privacy

La compilazione del questionario è **totalmente anonima**: non viene richiesta alcuna informazione identificativa della/del rispondente e della sua Azienda/Ente, non viene rilevato e tanto meno registrato il suo indirizzo IP (l'ambiente di indagine ed il dominio oadweb.it sono in cloud presso un provider), sulla banca dati delle risposte non viene registrata la data di compilazione, tutti i dati forniti verranno usati solo a fini statistici e comunque il dettaglio generico delle domande non consente in alcun modo di poter individuare la/il rispondente e/o la sua Azienda/Ente di appartenenza. **La compilazione del questionario non può pertanto ledere alcuna policy di riservatezza e confidenzialità**.

2.3 Il rapporto finale OAD 2023

Il rapporto finale sarà pubblicato e scaricabile gratuitamente da tutti gli interessati dal sito https://www.oadweb.it/it/, nei tempi previsti ed indicati nel §2.1.

Come per le precedenti edizioni, il rapporto OAD 2023 è distribuito con licenza Creative Commons Attribuzione - Non commerciale - Non opere derivate 4.0 Italia.

I contenuti del rapporto completo includeranno, commentandoli, tutti i temi presenti sia nella parte attacchi rilevati sia nella parte misure di sicurezza del questionario.

L'indice di riferimento del rapporto 2023, che potrà parzialmente cambiare nel corso della sua redazione, si articolerà nei seguenti principali capitoli_

1. Executive Summary in italiano e in inglese
2. L'indagine OAD
3. Il quadro generale degli attacchi digitali intenzionali a livello mondiale e italiano
4. I risultati dell'indagine OAD 2023
    a. Le tipologie e le tecniche di attacco rilevate nel 2022
    b. Approfondimento sugli attacchi ai siti e alle applicazioni web
    c. Le tipologie e le tecniche di attacco più temute nel prossimo futuro
    d. Le misure di sicurezza digitale adottate nei Sistemi Informativi (SI) delle Aziende/Enti rispondenti
    e. La macro valutazione qualitativa del livello di sicurezza digitale del SI oggetto delle risposte
    f. Il campione delle Aziende/Enti rispondenti e dei loro SI emerso dall'indagine
5. Attacchi alle infrastrutture critiche, cyber/financial crime e cyber terrorismo dai dati della Polizia Postale e delle Comunicazioni *(alla data ancora in attesa di conferma)*

- 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)
- 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 esempi dei contenuti si vedano i precedenti rapporti OAD scaricabili da https://www.oadweb.it/it/rapporti-e-relativi-convegni.html

OAD 2023 cerca di coprire i diversi **settori merceologici** (nel questionario fa riferimento ad un raggruppamento di codici ATECO) e le **Pubbliche Amministrazioni**, centrali e locali: qualora riuscisse ad avere per settore merceologico un sufficiente (>100) numero di rispondenti, potrà effettuare specifiche analisi per tali settori.

AIPSI si augura che anche per l'edizione 2023 possa avere, come per le precedenti edizioni, la collaborazione dalla **Polizia Postale e delle Telecomunicazioni,** per poter disporre di dati relativi all'intero 2022 sugli attacchi alle infrastrutture critiche italiane, sugli attacchi al mondo delle banche e della finanza, sul terrorismo digitale.

Come per i precedenti, il Rapporto OAD 2023, appena disponibile (si veda §2.1) 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

Questa registrazione richiede, oltre a poche informazioni, di fornire il **consenso esplicito** al trattamento dei propri dati personali, in particolare perché essi possano essere forniti agli eventuali Sponsor di OAD 2023. Il trattamento dei dati personali raccolti nel sito OAD da parte AIPSI **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

2.4 La proprietà intellettuale di OAD 2023

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 2023, sono, come per le precedenti edizioni, di AIPSI e di Malabo Srl che **consentono il loro utilizzo** agli Sponsor, ai Patrocinatori istituzionali e delle associazioni, ai media partner, o a chis sia interessato ad utilizzarle pubblicamente con **l'obbligo di citare la fonte** sulle figure sia sui grafici del Rapporto tramite la dicitura **©OAD 2023**.

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 PEC: aipsi@gigapec.it
Sede Centrale e Legale: AIPSI c/o Malabo Srl Via Savona 26 - 20144 Milano tel. (+39) 02 39443632
Sede Territoriale Lecce: AIPSI c/o Innovamind Srls Via Carducci 226 - 73050 Salve (LE)
Sede Territoriale Latina: AIPSI c/o DMXLAB srl - Via Grotte di Nottola 18 - 04012 Cisterna di Latina (LT)