Perché partecipare a OAD 2026? Per l'importanza del contributo di ogni organizzazione

BY REDAZIONE LINEAEDP — 20/07/2026 6 MINS READ

OAD 2026 offre alle organizzazioni uno strumento di autovalutazione della sicurezza digitale e contribuisce a costruire una fotografia indipendente del panorama cyber italiano

Autore: Marco R. A. Bozzetti, Ideatore e curatore OAD

Partecipare a OAD 2026 significa contribuire a una fotografia indipendente della sicurezza digitale italiana, ma anche svolgere un esercizio concreto di autovalutazione sulla sicurezza digitale della propria organizzazione.

Negli ultimi anni gli attacchi digitali sono aumentati per numero, complessità e impatto economico. **La maggior parte delle indagini sul fenomeno si basa su raccolta dati di attacco, tipicamente provenienti:**

· da **provider** che gestiscono sistemi e servizi dei loro clienti, e in particolare di quelli che gestiscono la sicurezza digitale;

· da **enti** che effettuano specifiche analisi verticali, ad esempio per settore merceologico, per specifici sistemi (ad esempio OT, Intelligenza artificiale, cloud, etc.), o che raccolgono e rielaborano dati di provider e di altre indagini nazionali e/o internazionali;

· da **agenzie governative**, quali l'ACN in Italia e l'ENISA a livello Unione Europea, ma tipicamente focalizzati su infrastrutture critiche e sulle organizzazioni soggette alla NIS2.

Di fatto sono tutte indagini settoriali, e per gran parte fanno riferimento a organizzazioni medio-grandi. Come dettagliato dall'**ISTAT**, in Italia il 99,9% delle imprese sono PMI, Piccole e Medie Imprese, e tra queste molte sono microimprese, al di sotto dei 10 dipendenti. Analoga situazione anche per le Pubbliche Amministrazioni, soprattutto per quelle locali.

L'idea, più di vent'anni fa, di lanciare un'indagine annuale via web, rigorosamente anonima, indipendente, autorevole e aperta ad organizzazioni di ogni tipo e dimensioni, partiva da questo assunto basilare: rilevare non solo se le organizzazioni rispondenti avessero subito attacchi digitali, di che tipo e con quali tecniche, ma anche quali misure di sicurezza, tecniche ed organizzative, fossero implementate. Oltre a questo, rilevare informazioni di contesto, pur nell'anonimato, quali il settore merceologico, il numero di dipendenti (e possibilmente il range di fatturato), l'importanza del sistema informativo per il funzionamento dell'organizzazione. Con tali in formazioni è possibile correlare gli attacchi subiti alle misure di sicurezza in essere, ed al contesto operativo dell'azienda/ente.

Poiché il bacino di rispondenti varia ogni anno, OAD non si propone come rilevazione ...isticamente rappresentativa dell'intero sistema Paese. Offre tuttavia indicazioni

concrete e approfondite sulle tipologie di attacco, sulle misure adottate e sulle differenze tra settori e dimensioni organizzative. È significativo che in tutti i diciotto anni di analisi passate, circa il 60% dei rispondenti appartenesse ad organizzazioni con meno di 250 dipendenti, in ambito privato le PMI.

OAD rappresenta in Italia una delle poche indagini indipendenti aperte anche alle organizzazioni di piccole dimensioni e alle realtà che non rientrano nei tradizionali perimetri delle infrastrutture critiche.

I principali motivi per partecipare

Auto formazione ed auto valutazione sulla sicurezza digitale nel proprio contesto operativo.

Il compilare il questionario online costituisce un momento di formazione sulla sicurezza digitale, soprattutto se si compilano le domande opzionali sulle misure di sicurezza in essere. Compilandolo, si vengono a conoscere, pur non entrando in troppi dettagli tecnici, le principali famiglie di attacchi e di tecniche di attacco, e le principali misure di sicurezza digitale, sia tecniche che organizzative, e si confrontano con la situazione del proprio sistema informativo, piccolo o grande che sia.

Completando le domande opzionali sulle misure di sicurezza, alla fine si ottiene una macro-valutazione del livello di sicurezza digitale, con l'elenco delle criticità emerse dalle risposte fornite: macro-valutazione contestualizzata alla realtà dell'organizzazione. Questo è un ulteriore ausilio, soprattutto per le piccole organizzazioni, per poter migliorare e potenziare le misure di sicurezza, oltre che per impostare una analisi dei rischi digitali.

Un "Glossario OAD", liberamente scaricabile, fornisce la spiegazione degli innumerevoli acronimi dell'ambiente ICT, usati anche nel questionario.

La compilazione del questionario OAD 2026 non solo consente di fotografare gli attacchi digitali rilevati, ma, con le domande sulle contromisure adottate, contribuisce alla diffusione delle moderne misure di sicurezza, sia tecniche sia organizzative. Questo, unito alla macro-valutazione del livello di sicurezza del sistema informativo oggetto delle risposte, costituisce un vero valore aggiunto per chi compila.

Ottenere contenuti di valore con la compilazione del questionario

Chi completa il questionario può inoltre accedere a tre opportunità messe a disposizione da AICA: due corsi online gratuiti, dedicati rispettivamente alla sicurezza digitale e all'uso consapevole dell'intelligenza artificiale, e uno sconto sul servizio di autovalutazione delle competenze ICT basato sul framework europeo e-CF.

Per approfondimenti su questi tre servizi, che anch'essi contribuiscono alla formazione e alla cultura digitale, si veda QUI.

Contribuire a una fotografia indipendente della sicurezza digitale italiana

Le informazioni raccolte dalle risposte al questionario sono e rimangono anonime, ed il nuovo questionario, semplificato e ridotto a circa 1/3 delle domande rispetto a quelli delle precedenti edizioni, richiede tra i 10 ed i 20 minuti per la sua completa compilazione, in funzione delle conoscenze sulla sicurezza digitale, degli attacchi rilevati e della compilazione della parte opzionale sulle misure di sicurezza. Le risposte al questionario, anche se non si sono rilevati attacchi digitali, contribuiscono in maniera essenziale alla realizzazione del Rapporto OAD 2026. Più compilazioni avremo, e possibilmente per tutti i diversi settori merceologici, più la fotografia della sicurezza digitale potrà essere accurata.

[illegible] parte della Comunità OAD

Come già illustrato nell'articolo su LineaEDP "OAD evolve: dall'indagine annuale a una comunità permanente sulla sicurezza digitale", si veda QUI, OAD 2026 diviene una comunità collaborativa e indipendente, la Comunità OAD, che, attraverso l'indagine annuale, iniziative condivise e il confronto tra esperienze e competenze, promuove una migliore conoscenza degli attacchi digitali e delle pratiche di sicurezza digitale da adottare per prevenirli e contrastarli.

Per diffondere la cultura digitale, e in particolare quella per la sicurezza digitale, una indagine ed un rapporto finale all'anno non bastano più. La sicurezza digitale non dipende soltanto dalle tecnologie, ma soprattutto dalle competenze delle persone chiamate ad operare e a decidere in merito. Con la continua e rapida evoluzione sia degli attacchi sia delle misure di sicurezza digitale, è necessaria una continua collaborazione e scambio di esperienze, garantendo in questo una effettiva terzietà ed autorevolezza. La sicurezza digitale non cresce soltanto grazie alle tecnologie, ma anche attraverso la condivisione delle esperienze e la costruzione di una conoscenza comune. La Comunità OAD non è destinata solo agli specialisti della sicurezza digitale, ma a chiunque debba e voglia utilizzare strumenti informatici in maniera sicura. In quest'ottica è stata lanciata OAD Insight, la rubrica della Comunità OAD dedicata alla diffusione di approfondimenti, analisi e indicazioni operative sulla sicurezza digitale. Attraverso contributi brevi e di taglio divulgativo, OAD Insight affronta temi di prevenzione e analizza gli insegnamenti che possono essere tratti da recenti attacchi digitali, con un linguaggio accessibile anche ai non specialisti: si veda QUI ed il primo OAD Insight #1 dedicato alla autenticazione multi-fattore.

Perché iscriversi alla Comunità OAD? Per ricevere aggiornamenti riservati e selezionati sui temi critici della sicurezza digitale, sulle attività e sulle iniziative dell'Osservatorio, e sui principali temi emersi dall'indagine in corso. La Comunità OAD non ha finalità commerciali: non vengono inviate pubblicità né proposte di prodotti, sistemi o servizi. Per approfondimenti, oltre al citato articolo su LineaEDP, si veda QUI.

Come partecipare

· Compila il questionario OAD 2026 QUI

· Iscriviti alla Comunità OAD QUI

· Segui OAD Insight QUI

· Partecipa al Gruppo OAD LinkedIn

· Diffondi l'iniziativa OAD con un passaparola ai tuoi interlocutori interessati alla sicurezza digitale.

OAD 2026

REDAZIONE LINEAEDP

LineaEDP è parte di BitMAT Edizioni, una casa editrice che ha sede a Milano con copertura a 360° per quanto riguarda la comunicazione rivolta agli specialisti dell'Information & Communication Technology.

CORRELATI

I o StaaS per gestire l'imprevisto

2026

Italia: cresce adozione AI ma non l'automazione

21/07/2026

MIX e ielo insieme per rafforzare la connettività tra Francia e Italia

20/07/2026

NEWSLETTER

Iscriviti alla Newsletter per ricevere gli aggiornamenti dai portali di BitMAT Edizioni.

ISCRIVITI ADESSO

SECURITY WORDS

INFRASTRUTTURA APPLICATIVA: PROTEGGIAMOLA

29/01/2024