

Direttiva (UE) 2022/2555

Fornitori e sistemi compliant



NIS 2: cosa prevede e a chi si rivolge

La **direttiva (UE) 2022/2555** si propone di implementare misure per un **elevato livello comune di cybersicurezza** nell'Unione Europea. La NIS 2 si rivolge ad un numero ampio di organizzazioni che prestano i propri servizi o che svolgono attività commerciali all'interno dell'Unione, arrivando ad influenzare implicitamente anche numerosi fornitori. All'articolo 2, vengono specificati i soggetti coinvolti dalla direttiva:

Soggetti pubblici e privati che rientrano nelle categorie elencate nell'**allegato I e II** e sono considerabili **medie imprese** (almeno 50 dipendenti e un fatturato annuo o un bilancio annuo totale superiore ai 10 milioni di euro)

Soggetti essenziali, ossia coloro elencati nell'articolo 3, comma 1 e comprendono principalmente operatori presenti nell'allegato I che superano i massimali delle medie imprese, che forniscono particolari servizi in ambito informatico o reti pubbliche di comunicazione, pubblica amministrazione centrale o quelli definiti "critici" dalla stessa direttiva o considerati essenziali dagli stati membri

Soggetti importanti, cioè coloro che non appartengono nell'elenco di quelli essenziali ma presenti negli allegati I o II e quelli classificati come importanti dagli stati membri



La direttiva NIS 2 chiede che ogni stato adotti una strategia nazionale per la cybersicurezza (art. 7), impostando obiettivi, risorse, misure strategiche e normative. Le **organizzazioni pubbliche e private** oggetto della NIS 2 dovranno implementare una serie di misure, adeguate ai rischi esistenti, volte a **migliorare la cybersicurezza e la resilienza a livello informatico**. Gli obiettivi di sicurezza da raggiungere sono proporzionali all'esposizione ai rischi, alle dimensioni dell'azienda, alla probabilità che si verifichino degli incidenti e alla loro gravità o impatto socio-economico.



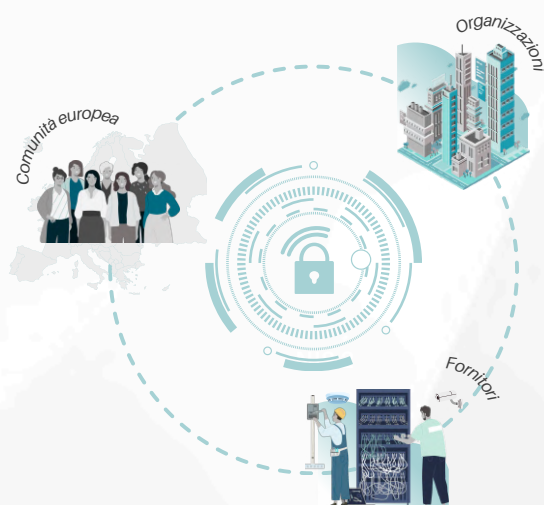
Una protezione inadeguata delle tecnologie e dei dati potrebbe **esporre le aziende a vulnerabilità** sfruttabili da cybercriminali in grado di introdursi nei sistemi e attuare attività fraudolente, potendo anche causare **interruzioni pericolose dei servizi** ed esporre personale e clienti a gravi **rischi** per la **privacy** e **sicurezza**. Oltre a ciò, il mancato rispetto della direttiva può comportare sanzioni fino a 10.000.000€ o il 2 % del totale del fatturato mondiale annuo, in aggiunta a quelle previste dai singoli stati membri o relative all'infrazione di altre norme (es. GDPR).

Sicurezza della catena di approvvigionamento

Particolare rilevanza assume il punto d) dell'articolo 21, riguardante le misure da implementare per le organizzazioni oggetto della direttiva, che specifica come le aziende interessate debbano provvedere alla "sicurezza della **catena di approvvigionamento**, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi".

La **sicurezza dell'intera filiera** è, quindi, fondamentale: i fornitori di beni e servizi critici dei soggetti NIS 2 devono implementare internamente adeguate misure di sicurezza per essere parte della catena di approvvigionamento. Da queste disposizioni si evince come la sicurezza informatica sia considerata una **responsabilità condivisa** tra aziende e fornitori, un obiettivo comune che prevede la collaborazione attiva e attenta per la gestione dei rischi.

Fornitori con standard di sicurezza elevati, in grado di fornire soluzioni compliant ed efficaci, migliorano il livello di sicurezza delle organizzazioni pubbliche e private e **contribuiscono alla resilienza complessiva** della supply chain. A sua volta, questi fattori tutelano gli interessi della collettività e i dati delle persone, promuovendo standard sempre maggiori di cybersicurezza.



I **fornitori**, in particolare quelli in ambito security e safety, devono essere **affidabili e sicuri** dal punto di vista cyber. **Italsicurezza**, grazie alle competenze multidisciplinari trentennali e la certificazione ISO 27001:2022 per la sicurezza delle informazioni, rispetta le caratteristiche principali necessarie per la gestione della sicurezza nelle organizzazioni interessate dalla normativa. Le più importanti sono:

1

Conformità a standard di sicurezza informatica

implementiamo misure tecniche e organizzative adeguate

2

Gestione del rischio nella catena di fornitura

effettuiamo la valutazione dei rischi e il monitoraggio continuo

3

Trasparenza e comunicazione

condividiamo informazioni sulla sicurezza ed eventuali incidenti

4

Clausole contrattuali di sicurezza

gli impegni contrattuali sono chiari, eseguiamo audit e verifiche

5

Formazione e consapevolezza del personale

promuoviamo la formazione e la cultura aziendale della sicurezza

6

Piani di continuità operativa e di ripristino

abbiamo procedure di ripristino e piani di resilienza dei servizi

7

Conformità legale e regolamentare

rispettiamo le norme sulla sicurezza dei dati come il GDPR

8

Gestione dei subfornitori

valutiamo i subfornitori e contrattualizziamo i requisiti di sicurezza

9

Certificazioni e accreditamenti

ISO 27001:2022, ISO 9001, elevato rating di legalità

10

Impegno positivo nella sicurezza

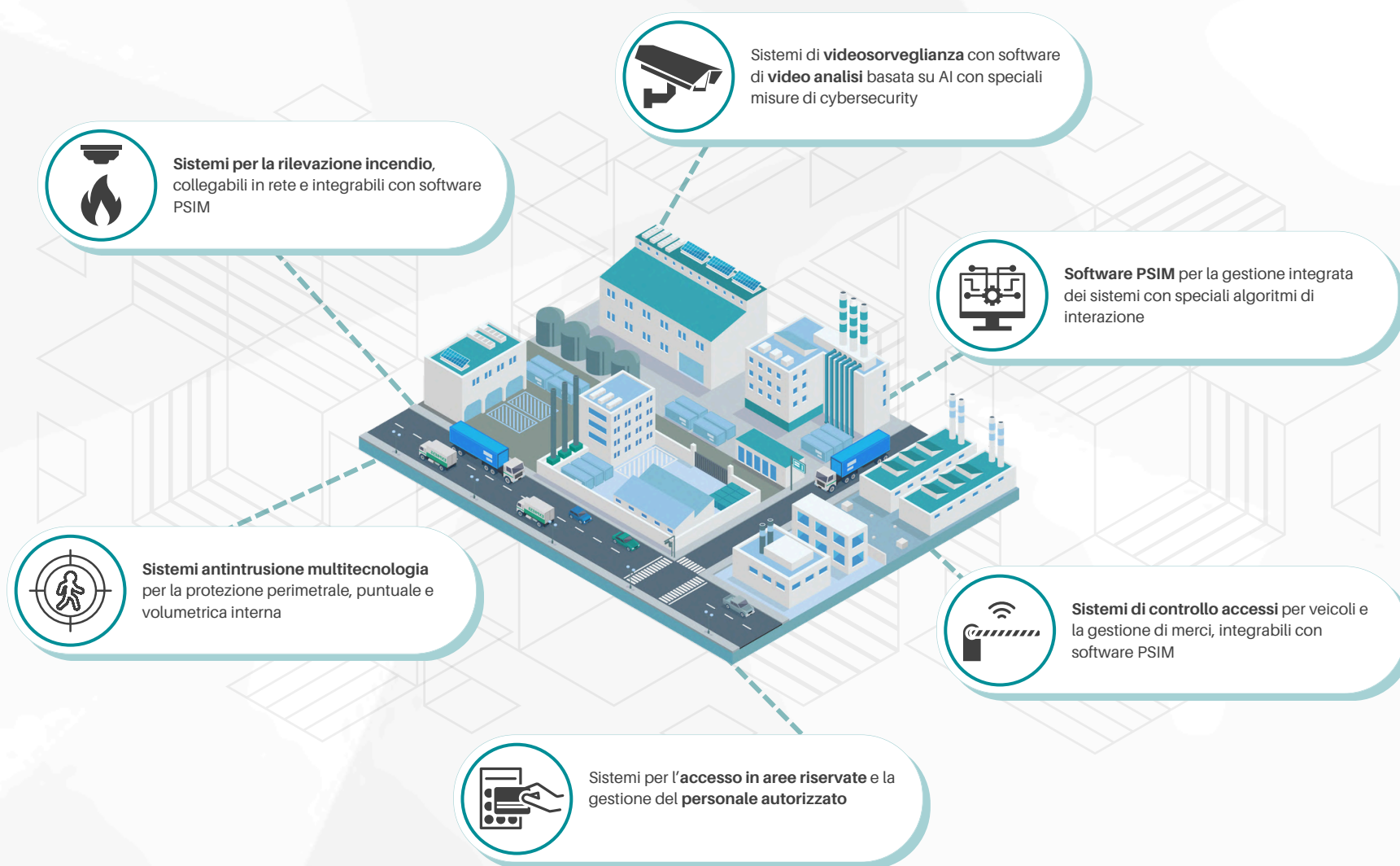
appliciamo il metodo Plan-Do-Check-Act

Approccio multirischio e adozione di sistemi di sicurezza

In un contesto come quello attuale, caratterizzato da una progressiva **convergenza tra security e cybersecurity** e un **aumento dei rischi informatici**, è indispensabile adottare un approccio definito dalla NIS 2 **"multirischio"**, ossia volto a proteggere a 360° le informazioni, le tecnologie, i sistemi e i siti da guasti, errori umani, azioni malevole o fenomeni naturali.

La direttiva poggia le proprie basi sulla presenza capillare di reti e sistemi informatici, oramai indispensabili in diversi aspetti delle attività lavorative e della vita quotidiana.

Il mondo della sicurezza fisica (security e safety) non fa eccezione: sono molteplici gli impianti e le tecnologie che sfruttano le reti, esponendosi a loro volta a possibili cyberattacchi. Sistemi di **videosorveglianza**, **antintrusione**, **controllo accessi**, ma anche **software** per la gestione degli impianti (PSIM) e centrali **antincendio**: questi sistemi, ritrovabili nella maggior parte delle organizzazioni interessate dalla NIS 2, devono essere compliant alle normative specifiche, nonché progettati e realizzati con i migliori requisiti di sicurezza informatica.



NIS 2: cosa prevede e a chi si rivolge

Le peculiari caratteristiche di **Italsicurezza**, certificate ISO 27001:2022, e l'elevata competenza in sicurezza fisica, ci rendono **fornitori compliant** alla direttiva (UE) 2022/2555.

Al punto 79 la NIS 2 richiede soluzioni basate su **approccio multirischio** per “[...] proteggere i sistemi informatici e di rete e il loro ambiente fisico da eventi quali furti, incendi, inondazioni, problemi di telecomunicazione o interruzioni di corrente, o da qualsiasi accesso fisico non autorizzato nonché dai danni alle informazioni [...]”.

La nostra vision di sicurezza integrata ci ha portato a certificarci ISO 27001:2013 già nel 2020, aggiornando recentemente gli standard di sicurezza aziendale alla versione ISO 27001:2022 in ottica di miglioramento continuo.

Italsicurezza, grazie a questa attestazione, fornisce molteplici **vantaggi alle imprese** soggette alla normativa, semplificando i processi per l'adeguamento alla NIS 2.



COMPLIANT NIS 2

Facilità di allineamento alle disposizioni che mirano a proteggere l'intera filiera, mitigando i rischi provenienti dal contatto con aziende esterne



CONFORMITÀ

Certificati ISO 27001:2022 da ente accreditato ACCREDIA, quindi soggetti ad audit annuali allo scopo di verificare la conformità allo standard



SICUREZZA A 360°

Gestione dei processi con elevati livelli di sicurezza e adozione di misure hardware, software e operative per proteggere informazioni e tecnologie



COMPETENZA

Competenza elevata in ambito sicurezza fisica, cybersecurity e privacy



APPROCCIO MULTIRISCHIO

Approccio multirischio come da direttiva per una sicurezza integrata, completa ed efficace a 360°



SEMPRE AL TUO FIANCO

Affiancamento del cliente nel tempo, dalla progettazione, installazione e integrazione fino alla manutenzione e assistenza h 24

Da **più di 30 anni Italsicurezza** si occupa di Physical Security e Safety in territorio nazionale e internazionale, realizzando sistemi di sicurezza integrati per clienti business, enti pubblici e privati. Ci occupiamo della realizzazione dei nostri sistemi a 360°, affiancando il cliente lungo tutto il ciclo di vita dell'impianto e garantendo efficienti servizi di manutenzione e assistenza h 24.



Più di **900**
interventi all'anno



Circa **40** esperti
collaboratori



Quasi **8.000**
sistemi installati



Oltre **3.000** clienti
soddisfatti

Le nostre certificazioni **ISO 27001** per la sicurezza delle **informazioni** e **ISO 9001** per la **qualità** ci consentono di offrire soluzioni performanti, con particolare attenzione ai temi della privacy e della cybersecurity. Siamo, inoltre, membri **TAPA EMEA** (*Transported Asset Protection Association*) per la sicurezza della **supply chain**.

