UNIT SISTEMI TECHNOLOGY

Managed Service Provider | Milano & Lecco | Dal 1996

OBBLIGO DI LEGGE - Direttiva UE 2022/2555

Checklist Conformita NIS2

Guida operativa per la conformita alla Direttiva (UE) 2022/2555 e al D.Lgs. 138/2024

SCADENZA	SANZIONI	VERSIONE
1 Ottobre 2026	Fino al 2% fatturato	1.0 - Febbraio 2026

Unit Sistemi Technology S.r.l. | P.IVA 11139950965

Milano: Via Del Gonfalone 3, 20164 | Lecco: Corso Promessi Sposi 23/D, 23900

Tel. 02 2660 0445 | info@unitsistemi.it | www.unitsistemi.it

Indice

Come usare questa checklist

Ogni sezione contiene i requisiti specifici della Direttiva NIS2 e del D.Lgs. 138/2024. Utilizzare le caselle di spunta per verificare lo stato di conformita della propria organizzazione. Al termine, le sezioni non completate indicano le aree su cui intervenire prioritariamente. I riferimenti normativi sono indicati per ciascun requisito.

SEZIONE 01

Premessa e ambito di applicazione

Verificare se la propria organizzazione rientra nell'ambito di applicazione della Direttiva NIS2

La Direttiva (UE) 2022/2555 (NIS2), recepita in Italia con il D.Lgs. 138/2024, impone obblighi di cybersecurity a un ampio spettro di organizzazioni pubbliche e private. I soggetti obbligati sono classificati come **essenziali** o **importanti** in base al settore di appartenenza e alle dimensioni.

ATTENZIONE - Criteri dimensionali

Sono soggette alla NIS2 le organizzazioni con: almeno 50 dipendenti OPPURE fatturato annuo superiore a 10 milioni di euro. Tuttavia, anche organizzazioni piu piccole possono rientrare se operano come fornitori critici nella supply chain di soggetti obbligati, o se forniscono servizi di infrastruttura digitale (DNS, TLD, cloud, data center, CDN).

Settori ad alta criticita (Allegato I - Soggetti essenziali):

Energia, Trasporti, Settore bancario, Infrastrutture dei mercati finanziari, Sanita, Acqua potabile, Acque reflue, Infrastrutture digitali, Gestione servizi ICT B2B, Pubblica Amministrazione, Spazio.

Altri settori critici (Allegato II - Soggetti importanti):

Servizi postali, Gestione rifiuti, Fabbricazione/produzione/distribuzione sostanze chimiche, Produzione/trasformazione/distribuzione alimenti, Fabbricazione (dispositivi medici, computer, elettronica, macchinari, autoveicoli, altri mezzi di trasporto), Fornitori servizi digitali, Ricerca.

Rif. normativo: Art. 2, 3, 4 D.Lgs. 138/2024; Allegati I, II, III, IV Direttiva (UE) 2022/2555

Checklist: Verifica di applicabilita

- [ ] Verificata l'appartenenza a uno dei settori indicati negli Allegati I-IV
- [ ] Verificati i criteri dimensionali (dipendenti >= 50 OPPURE fatturato >= 10M EUR)
- [ ] Verificato se l'organizzazione e fornitore critico di soggetti NIS2
- [ ] Determinata la classificazione: soggetto essenziale o importante
- [ ] Identificata l'autorita competente di riferimento (ACN - Agenzia per la Cybersicurezza Nazionale)
- [ ] Verificata l'eventuale applicabilita di normative settoriali specifiche (es. DORA per il settore finanziario)

SEZIONE 02

Identificazione e registrazione

Adempimenti obbligatori di registrazione sulla piattaforma ACN

SCADENZA CRITICA

La registrazione annuale sulla piattaforma ACN deve essere completata entro il 28 febbraio di ogni anno. La mancata registrazione comporta sanzioni amministrative.

Checklist: Registrazione e identificazione

- [ ] Eseguita l'auto-valutazione per determinare lo status di soggetto NIS2
- [ ] Registrazione completata sulla piattaforma digitale ACN (portale.acn.gov.it)
- [ ] Designato un punto di contatto unico per le comunicazioni con ACN
- [ ] Comunicati i dati identificativi completi (ragione sociale, P.IVA, settore, dimensione)
- [ ] Comunicati gli indirizzi IP e i nomi di dominio utilizzati dall'organizzazione
- [ ] Comunicata la lista degli Stati membri UE in cui l'organizzazione opera
- [ ] Verificata la corretta classificazione ricevuta da ACN (essenziale/importante)
- [ ] Pianificata la registrazione annuale per gli anni successivi

Rif. normativo: Art. 7, 11, 12 D.Lgs. 138/2024; Art. 3(3) Direttiva NIS2

SEZIONE 03

Governance e responsabilita della direzione

La NIS2 introduce la responsabilita personale degli organi di gestione

RESPONSABILITA PERSONALE DEL CDA

A differenza del GDPR, la NIS2 prevede che gli organi di gestione (CdA, Amministratori) siano personalmente responsabili della mancata conformita. La direzione deve approvare le misure di gestione del rischio, supervisionarne l'attuazione e partecipare a formazione specifica in materia di cybersecurity. L'inosservanza puo comportare la sospensione temporanea dall'incarico dirigenziale.

Checklist: Governance e organizzazione

- ☐ Organi di gestione (CdA/Amministratori) informati degli obblighi NIS2 e delle responsabilita personali
- ☐ Approvazione formale delle politiche di gestione del rischio cyber da parte del CdA
- ☐ Nominato un responsabile della sicurezza informatica (CISO o ruolo equivalente)
- ☐ Definita la struttura organizzativa per la gestione della cybersecurity
- ☐ Definite e documentate le responsabilita di sicurezza per ciascun ruolo aziendale
- ☐ Implementato un processo di reporting periodico del CdA sullo stato della cybersecurity
- ☐ Organi di gestione hanno partecipato a formazione specifica sulla cybersecurity
- ☐ Definite le procedure di escalation per incidenti di sicurezza verso il vertice aziendale
- ☐ Documentata la policy di sicurezza delle informazioni approvata dalla direzione
- ☐ Previsto budget dedicato per la cybersecurity con revisione annuale

Rif. normativo: Art. 23 D.Lgs. 138/2024; Art. 20 Direttiva NIS2

SEZIONE 04

Gestione del rischio cyber

Approccio multi-rischio per l'analisi e il trattamento dei rischi informatici

La NIS2 richiede un approccio **multi-rischio** (all-hazards) che consideri non solo le minacce cyber, ma anche rischi fisici, ambientali e di supply chain. Le misure devono essere **proporzionate** al rischio, tenendo conto dello stato dell'arte, dei costi di attuazione, della dimensione dell'organizzazione e della probabilita e gravita degli incidenti.

Checklist: Analisi e gestione del rischio

- [ ] Adottata una metodologia strutturata di risk assessment (es. ISO 27005, NIST CSF 2.0 FNCS)
- [ ] Inventariati tutti gli asset informatici critici (hardware, software, dati, servizi)
- [ ] Identificate e classificate le minacce rilevanti per l'organizzazione
- [ ] Valutate le vulnerabilita dei sistemi e delle reti
- [ ] Calcolato il livello di rischio per ciascun asset/processo critico
- [ ] Definito il piano di trattamento dei rischi con misure proporzionate
- [ ] Identificati e documentati i rischi residui accettati dalla direzione
- [ ] Pianificate le revisioni periodiche della valutazione del rischio (almeno annuali)
- [ ] Considerati i rischi legati a fattori fisici e ambientali (incendi, alluvioni, accesso fisico)
- [ ] Integrato il risk assessment cyber con il risk management aziendale complessivo

Rif. normativo: Art. 24 D.Lgs. 138/2024; Art. 21(1)(2) Direttiva NIS2

SEZIONE 05

Misure di sicurezza tecniche

Requisiti tecnici minimi imposti dall'Art. 21 della Direttiva NIS2

L'Art. 21 della Direttiva NIS2 elenca le misure di sicurezza minime che devono essere implementate. Il framework di riferimento per l'Italia e il **FNCS (Framework Nazionale per la Cybersecurity e la Sicurezza)** basato su NIST CSF 2.0, con i requisiti tecnici di dettaglio attesi da ACN entro aprile 2026.

5.1 Politiche di sicurezza e analisi dei rischi

- [ ] Definita e documentata la politica di sicurezza dei sistemi informativi e di rete
- [ ] Implementate politiche di analisi dei rischi secondo metodologia riconosciuta
- [ ] Definite politiche di classificazione delle informazioni e dei dati
- [ ] Implementato un sistema di gestione della sicurezza delle informazioni (ISMS)

5.2 Gestione degli incidenti

- [ ] Definita procedura di rilevamento, analisi e risposta agli incidenti
- [ ] Implementati sistemi di rilevamento delle intrusioni (IDS/IPS)
- [ ] Configurato SIEM o sistema centralizzato di raccolta e correlazione log
- [ ] Definiti i livelli di severita degli incidenti e le procedure di escalation
- [ ] Implementato il processo di analisi post-incidente e lessons learned

5.3 Continuita operativa e disaster recovery

- [ ] Definito e documentato il Business Continuity Plan (BCP)
- [ ] Definito e testato il Disaster Recovery Plan (DRP)
- [ ] Implementata strategia di backup conforme alla regola 3-2-1
- [ ] Testato periodicamente il ripristino dei backup (almeno semestrale)
- [ ] Definiti RPO (Recovery Point Objective) e RTO (Recovery Time Objective) per i servizi critici

5.4 Sicurezza della rete e dei sistemi

- [ ] Implementata segmentazione della rete (VLAN, DMZ, micro-segmentazione)
- [ ] Configurati firewall perimetrali con regole restrittive (deny-by-default)
- [ ] Implementata protezione degli endpoint (EDR/XDR)
- [ ] Configurata la crittografia delle comunicazioni (TLS 1.2+, VPN IPSec/SSL)
- [ ] Implementato il controllo degli accessi basato sui ruoli (RBAC)
- [ ] Configurata l'autenticazione multi-fattore (MFA) per accessi privilegiati e remoti
- [ ] Implementata la gestione delle vulnerabilita con scansioni periodiche
- [ ] Definita la procedura di patch management con tempistiche di applicazione
- [ ] Implementato il monitoraggio continuo della sicurezza (24/7 o NearTime)
- [ ] Protetti i sistemi DNS, NTP e altri servizi infrastrutturali

5.5 Gestione degli accessi e identita

- [ ] Implementata politica di gestione delle credenziali (complessita, scadenza, riuso)
- [ ] Implementata autenticazione multi-fattore (MFA) per tutti gli accessi critici
- [ ] Definita procedura di provisioning/deprovisioning degli account utente
- [ ] Implementato il principio del minimo privilegio (least privilege)
- [ ] Implementata la revisione periodica dei diritti di accesso (access review)
- [ ] Gestiti e monitorati gli accessi degli account privilegiati (PAM)
- [ ] Implementata la gestione sicura delle credenziali di servizio e delle API key

5.6 Crittografia

- [ ] Definita la politica di utilizzo della crittografia
- [ ] Implementata la crittografia dei dati a riposo per i dati sensibili/critici
- [ ] Implementata la crittografia dei dati in transito (TLS, VPN)
- [ ] Gestite le chiavi crittografiche secondo best practice (rotazione, custodia)

SEZIONE 06

Sicurezza della supply chain

Gestione dei rischi legati ai fornitori e alla catena di approvvigionamento

La NIS2 pone particolare attenzione alla sicurezza della **supply chain**. Le organizzazioni devono valutare e gestire i rischi derivanti dai rapporti con i fornitori diretti e con i prestatori di servizi. Questo include la valutazione della qualita e della resilienza dei prodotti e servizi ICT dei fornitori.

Checklist: Sicurezza della catena di fornitura

- [ ] Inventariati tutti i fornitori critici di servizi e prodotti ICT
- [ ] Valutato il livello di rischio cyber per ciascun fornitore critico
- [ ] Inserite clausole di sicurezza informatica nei contratti con i fornitori
- [ ] Richiesta e verificata la conformita NIS2 dei fornitori soggetti
- [ ] Definite procedure di due diligence per la selezione di nuovi fornitori ICT
- [ ] Implementato il monitoraggio continuo del rischio dei fornitori critici
- [ ] Definite procedure per la gestione degli accessi dei fornitori ai propri sistemi
- [ ] Inclusi i fornitori nei test di sicurezza e nelle esercitazioni di incident response
- [ ] Definito piano di contingenza in caso di indisponibilita di fornitori critici
- [ ] Verificata la sicurezza dello sviluppo software dei fornitori (secure SDLC)

Rif. normativo: Art. 24(2)(d) D.Lgs. 138/2024; Art. 21(2)(d)(3) Direttiva NIS2

SEZIONE 07

Gestione incidenti e notifiche obbligatorie

Obblighi di notifica al CSIRT Italia e all'ACN secondo tempistiche stringenti

OBBLIGO GIA IN VIGORE - Notifica incidenti

L'obbligo di notifica degli incidenti significativi e gia attivo dal 1 gennaio 2026. La pre-notifica deve avvenire entro 24 ore e la notifica completa entro 72 ore. La relazione finale deve essere trasmessa entro 1 mese dall'incidente.

Entro 24 ore	Pre-notifica	Segnalazione iniziale al CSIRT Italia con indicazione se l'incidente possa avere impatto transfrontaliero
Entro 72 ore	Notifica completa	Aggiornamento con valutazione iniziale, gravita, impatto, indicatori di compromissione (IoC)
Su richiesta	Report intermedio	Aggiornamenti sullo stato della gestione dell'incidente
Entro 1 mese	Relazione finale	Descrizione dettagliata, causa, misure adottate, impatto transfrontaliero

Checklist: Gestione e notifica incidenti

- [ ] Definita la procedura di gestione degli incidenti (Incident Response Plan)
- [ ] Costituito l'Incident Response Team (IRT) con ruoli e responsabilita
- [ ] Configurato il canale di comunicazione con il CSIRT Italia
- [ ] Definiti i criteri per determinare un "incidente significativo" ai fini della notifica
- [ ] Predisposto il template di pre-notifica (24 ore) secondo il formato ACN
- [ ] Predisposto il template di notifica completa (72 ore)
- [ ] Definita la procedura per la relazione finale (entro 1 mese)
- [ ] Testate le procedure di notifica con esercitazioni periodiche (almeno annuali)
- [ ] Implementato il processo di raccolta delle evidenze forensi (chain of custody)
- [ ] Definita la procedura di comunicazione verso gli utenti/clienti impattati

Rif. normativo: Art. 25, 26 D.Lgs. 138/2024; Art. 23 Direttiva NIS2

SEZIONE 08

Continuita operativa

Business continuity, disaster recovery e resilienza dei sistemi critici

Checklist: Continuita operativa e resilienza

- [ ] Identificati i processi e i servizi critici dell'organizzazione (BIA - Business Impact Analysis)
- [ ] Definiti RTO e RPO per ogni servizio critico
- [ ] Documentato il Business Continuity Plan (BCP) aggiornato
- [ ] Documentato il Disaster Recovery Plan (DRP) con procedure di ripristino
- [ ] Implementata infrastruttura di backup conforme (regola 3-2-1, backup off-site/cloud)
- [ ] Implementata ridondanza per i sistemi critici (alta affidabilita, clustering)
- [ ] Testato il ripristino completo da backup almeno una volta all'anno
- [ ] Condotte esercitazioni di disaster recovery con simulazione di scenario
- [ ] Definita la gestione delle crisi con catena di comando e comunicazione
- [ ] Documentate le procedure di ripristino per ciascun sistema critico
- [ ] Verificata la capacita di operare in modalita degradata durante un incidente
- [ ] Integrato il piano di continuita con i fornitori critici

Rif. normativo: Art. 24(2)(c) D.Lgs. 138/2024; Art. 21(2)(c) Direttiva NIS2

SEZIONE 09

Formazione e sensibilizzazione

Obbligo di formazione per gli organi di gestione e per tutto il personale

La NIS2 impone che gli **organi di gestione** seguano una formazione specifica sulla cybersecurity e che sia garantita una formazione analoga ai **dipendenti**, per aumentare la consapevolezza dei rischi informatici e delle pratiche di igiene digitale.

Checklist: Formazione e awareness

- ☐ Definito un piano di formazione annuale sulla cybersecurity
- ☐ Organi di gestione (CdA) hanno completato formazione specifica NIS2
- ☐ Personale tecnico IT formato su gestione incidenti e risposta alle minacce
- ☐ Tutti i dipendenti hanno completato formazione base sulla cybersecurity
- ☐ Implementato programma di security awareness continuo (phishing simulation, newsletter)
- ☐ Formazione specifica per il personale con accesso a dati/sistemi critici
- ☐ Documentate le sessioni formative con registri di partecipazione
- ☐ Verificata l'efficacia della formazione con test/quiz periodici
- ☐ Aggiornata la formazione in base alle nuove minacce e incidenti rilevati
- ☐ Inclusa la formazione sulla sicurezza nel processo di onboarding dei nuovi dipendenti

Rif. normativo: Art. 23(3)(4) D.Lgs. 138/2024; Art. 20(2) Direttiva NIS2

SEZIONE 10

Audit, monitoraggio e miglioramento continuo

Verifica periodica dell'efficacia delle misure implementate

Checklist: Audit e miglioramento continuo

- [ ] Definito un programma di audit interno della sicurezza (almeno annuale)
- [ ] Condotti vulnerability assessment periodici su tutti i sistemi esposti
- [ ] Condotti penetration test periodici (almeno annuali) su perimetro esterno e interno
- [ ] Implementato monitoraggio continuo dello stato di sicurezza (dashboard, KPI)
- [ ] Definiti KPI di sicurezza e reportistica periodica per la direzione
- [ ] Implementato un processo di gestione delle non-conformita e azioni correttive
- [ ] Mantenuto un registro delle azioni correttive e del loro stato di avanzamento
- [ ] Verificata periodicamente la conformita alle politiche di sicurezza interne
- [ ] Aggiornate le politiche e procedure in base ai risultati degli audit
- [ ] Documentata la valutazione della conformita per eventuali ispezioni dell'ACN
- [ ] Predisposta la documentazione per cooperare con le attivita di vigilanza dell'ACN

Rif. normativo: Art. 31, 33, 34, 35, 36 D.Lgs. 138/2024; Art. 32, 33 Direttiva NIS2

SEZIONE 11

Scadenze e roadmap

Calendario degli adempimenti NIS2 in Italia

Data	Adempimento	Stato
17 Gen 2023	Entrata in vigore Direttiva NIS2	Completato
18 Ott 2024	Recepimento in Italia - D.Lgs. 138/2024	Completato
1 Gen 2026	Inizio obbligo notifica incidenti significativi	In vigore
1-28 Feb 2026	Registrazione annuale piattaforma ACN	In scadenza
Apr 2026	Pubblicazione requisiti tecnici definitivi ACN (FNCS)	In arrivo
1 Ott 2026	**Conformita obbligatoria alle misure di sicurezza**	**DEADLINE**

REGIME SANZIONATORIO

Soggetti essenziali: Sanzioni fino a 10.000.000 EUR o 2% del fatturato annuo mondiale (il maggiore dei due). Possibile sospensione temporanea dei dirigenti responsabili.

Soggetti importanti: Sanzioni fino a 7.000.000 EUR o 1,4% del fatturato annuo mondiale (il maggiore dei due).

Ulteriori conseguenze: Esclusione da gare pubbliche, revoca di certificazioni e autorizzazioni, pubblicazione delle violazioni, ordine di conformita con termine perentorio.

COME UNIT SISTEMI PUO AIUTARTI

Il tuo percorso verso la conformita NIS2

Unit Sistemi Technology e il partner MSP che accompagna le PMI italiane dalla valutazione iniziale alla conformita completa. Con oltre **30 anni di esperienza** nella gestione delle infrastrutture IT e **6.000+ endpoint protetti**, offriamo un percorso strutturato in 4 fasi:

1	2	3	4
Assessment	**Roadmap**	**Implementazione**	**Monitoraggio**
Gap analysis completa: dove sei oggi vs dove devi essere	Piano di remediation prioritizzato con tempi e costi	Firewall, MFA, SIEM, backup, policy, formazione	Compliance continua, audit readiness, aggiornamenti

Tecnologie che implementiamo per la conformita NIS2:

- Fortinet (Firewall, FortiSIEM, FortiEDR)
- Bitdefender (Endpoint Protection)
- Zabbix (Monitoraggio 24/7)
- Cisco Catalyst / Meraki (Networking)
- Veeam / Acronis (Backup & DR)
- TacticalRMM (Gestione Endpoint)
- Palo Alto Networks (Next-Gen Firewall)
- Microsoft 365 Security & Compliance
- VMware (Virtualizzazione & HA)

Richiedi il tuo NIS2 Assessment Gratuito

In 30 minuti ti diciamo se sei obbligato, a che punto sei, e cosa devi fare.

Tel. 02 2660 0445 | info@unitsistemi.it | www.unitsistemi.it/nis2

Unit Sistemi Technology S.r.l.
Milano: Via Del Gonfalone 3, 20164 | Lecco: Corso Promessi Sposi 23/D, 23900
Tel. 02 2660 0445 | Fax 02 2660 0445 | info@unitsistemi.it
P.IVA 11139950965 | www.unitsistemi.it