APPLOGIC S.R.L.S

Dichiarazione delle Misure di Sicurezza Cyber

ai sensi della Direttiva (UE) 2022/2555 – NIS2 | D.Lgs. 4 settembre 2024 n. 138

Documento pubblico per la verifica della supply chain ICT

Versione 1.0 – 3 Dicembre 2025

1. Informazioni sul Soggetto

Ragione Sociale	Applogic S.r.l.s.
Sede Legale	Via Rocco di Cillo 5, 97100 Ragusa (RG)
Settore	Servizi ICT – Fornitura e gestione servizi Internet
Classificazione NIS2	Soggetto Importante (art. 3, comma 1, D.Lgs. 138/2024)
Autorità di Riferimento	ACN – Agenzia per la Cybersicurezza Nazionale
Data Documento	Dicembre 2025
Contatto Sicurezza	info@applogic.it

2. Scopo e Campo di Applicazione

Il presente documento è pubblicato da Applogic S.r.l.s. in qualità di soggetto importante ai sensi del D.Lgs. 138/2024 (recepimento della Direttiva NIS2) e illustra le misure di sicurezza adottate nell'ambito della propria catena di approvvigionamento ICT (supply chain).

Il documento è destinato a:

- Clienti soggetti NIS2 (essenziali o importanti) che devono verificare i fornitori ICT nella propria supply chain
- Pubbliche Amministrazioni (scuole, comuni, enti) tenute al rispetto delle disposizioni di sicurezza ICT
- Aziende private che richiedono evidenza delle misure di sicurezza dei propri fornitori
- Autorità di vigilanza e organismi di audit

I perimetri di servizio coperti sono:

- Registrazione e gestione nomi a dominio (.it, .edu.it, internazionali) in modalità reseller
- Hosting web (VPS e shared hosting su infrastruttura multi-cloud)
- Posta Elettronica Certificata (PEC) – in modalità reseller
- Email tradizionale – in modalità reseller
- Certificati digitali SSL/TLS – in modalità reseller
- Realizzazione e manutenzione siti web e applicativi SaaS

3. Perimetri di Servizio e Classificazione del Rischio

La tabella seguente illustra i perimetri di servizio erogati da Applogic, la modalità operativa e il livello di sicurezza assegnato secondo la classificazione interna L1–L4, adottata in coerenza con i principi di gestione del rischio della Direttiva NIS2 e del D.Lgs. 138/2024.

Perimetro di Servizio	Modalità di Erogazione	Livello Sicurezza
Domini .it / .edu.it	Reseller tramite registrar accreditato CNR	BASSO (L1)
Domini internazionali	Reseller tramite registrar accreditati ICANN	BASSO (L1)
Hosting Web (VPS/Shared)	Cloud: Aruba, OVH, Hetzner, AWS, IONOS, Applogic - titolarità mista per contratto	MEDIO (L2)
Email tradizionale	Reselling caselle Mail	BASSO (L1)
Certificati SSL/TLS	Reseller Certification Authority riconosciute	BASSO (L1)
Realizzazione siti web	Sviluppo su infrastruttura cliente o Applogic	BASSO (L1)

Nota metodologica: La classificazione L1–L4 è uno strumento interno di valutazione del rischio, non uno standard normativo. L3 indica responsabilità diretta e controllo pieno; L2 indica responsabilità amministrativa con componente infrastrutturale demandata a provider certificati.

4. Misure Tecniche e Organizzative Adottate

4.1 Controlli di Sicurezza Attivi

Controllo di Sicurezza	Descrizione	Stato	Evidenza
Monitoring uptime automatico	Attivo su tutti i servizi critici gestiti	**Attivo**	✓ Doc. interna
Web Application Firewall (WAF)	Attivo sui server web gestiti da Applogic	**Attivo**	✓ Doc. interna
Log retention e analisi	Conservazione log di accesso e sistema	**Attivo**	✓ Doc. interna
Autenticazione forte (2FA)	Attiva sui sistemi critici interni (pannelli di controllo, registrar, hosting admin)	**Attivo**	✓ Doc. interna
Firewall perimetrale VPS	Delegato a provider certificati (Aruba, Hetzner, AWS, OVH, IONOS)	**Delegato**	↗ Provider
Vulnerability detection	Implementato su perimetro gestito (SIEM)	**Attivo**	✓ Doc. interna
Backup e disaster recovery	Procedure attive con retention documentata per contratto	**Attivo**	✓ Doc. interna
Gestione incidenti (P02)	Procedura formalizzata conforme D.Lgs. 138/2024	**Attivo**	✓ Doc. interna

4.2 Gestione degli Incidenti di Sicurezza

Applogic ha adottato una procedura formalizzata di gestione degli incidenti (Procedura P02) conforme ai requisiti del D.Lgs. 138/2024. La procedura disciplina:

- Identificazione e classificazione degli eventi di sicurezza (tassonomia secondo le determinazioni ACN)
- Notifica tempestiva al cliente entro 24 ore dalla conoscenza dell'evento
- Notifica all'ACN nei casi previsti dalla normativa
- Analisi dell'incidente, mitigazione del rischio e ripristino dei servizi
- Documentazione e tracciabilità completa degli eventi

4.3 Continuità Operativa e Backup

Applogic garantisce la continuità dei servizi gestiti attraverso:

- Procedure di backup documentate con retention definita per contratto
- Monitoraggio automatico dell'uptime su tutti i servizi critici
- Procedure di disaster recovery per i servizi di gestione domini
- Possibilità di migrazione rapida verso altro provider su richiesta del cliente, con rilascio di AuthCode, dati di registrazione e accesso senza ritardi ingiustificati

4.4 Controllo degli Accessi

I sistemi critici (pannelli di controllo hosting, interfacce registrar, accessi amministrativi) sono protetti da:

- Autenticazione forte a due fattori (2FA) per tutti gli accessi privilegiati
- Principio del privilegio minimo (least privilege) nella gestione degli accessi
- Procedure di onboarding/offboarding del personale con revoca accessi

4.5 Sicurezza della Rete e dei Sistemi

I servizi web gestiti direttamente da Applogic sono protetti da:

- Web Application Firewall (WAF) attivo sui server web gestiti
- Firewall perimetrale sui VPS, delegato ai provider certificati (Aruba, OVH, Hetzner, AWS, IONOS)
- Log retention e analisi degli accessi con conservazione per il periodo minimo di legge
- Monitoraggio uptime automatico con alerting in tempo reale

5. Catena di Fornitura (Supply Chain) e Provider Certificati

Applogic eroga i propri servizi avvalendosi esclusivamente di provider e fornitori terzi che dispongono di certificazioni di sicurezza riconosciute a livello internazionale. La selezione dei fornitori è effettuata valutando le certificazioni disponibili, la conformità normativa e l'affidabilità operativa.

Provider / Fornitore	Servizi Forniti	Sede
Aruba S.p.A.	Hosting shared	Italiana
OVH SAS	VPS, Dedicated Server, Cloud Hosting	Francese
Hetzner Online GmbH	VPS	Tedesca
Amazon Web Services (AWS)	Cloud hosting	USA/UE
IONOS SE	VPS	Tedesca
Gestori PEC (AgID)	Posta Elettronica Certificata	Italiana
Teknadoc Italia S.r.l.	Registrazione domini .it / edu.it	Italiana
Cloud DNS Ltd	Gestione DNS	Bulgara

Per tutti i servizi erogati in modalità reseller (PEC, SSL, Email, hosting), Applogic mantiene il controllo amministrativo e di provisioning, mentre la responsabilità infrastrutturale è demandata ai provider certificati sopra indicati, in conformità al modello di responsabilità condivisa previsto dalla Direttiva NIS2.

L’organizzazione adotta un modello multi-provider finalizzato alla mitigazione del rischio di concentrazione, alla prevenzione del fenomeno di vendor lock-in e alla riduzione della dipendenza da singoli fornitori.

La distribuzione dei servizi su più provider e su diverse regioni geografiche consente di aumentare la resilienza operativa, garantire maggiore continuità del servizio e limitare l’impatto di eventuali disservizi o incidenti, in coerenza con i principi di gestione del rischio e sicurezza della supply chain previsti dalla Direttiva (UE) 2022/2555 e dal Decreto Legislativo 4 settembre 2024 n. 138.

I fornitori sono selezionati sulla base di criteri di affidabilità, conformità normativa, livelli di servizio (SLA) e garanzie di sicurezza. Sono inoltre previste procedure di exit strategy e migrazione dei servizi, al fine di assicurare la continuità operativa e la sostituibilità dei fornitori in caso di criticità o cessazione del rapporto.

6. Limitazioni Strutturali e Perimetro di Responsabilità

Applogic dichiara che i seguenti ambiti esulano dal proprio perimetro di controllo diretto:

- DNS autoritativi (gestiti dai provider di infrastruttura)
- Infrastruttura di trasporto PEC (gestita dai gestori AgID accreditati)
- Infrastruttura delle Certification Authority per i certificati SSL/TLS
- Infrastruttura hardware dei datacenter dei provider cloud

Per i servizi erogati su infrastruttura del cliente (titolarità del cliente per contratto), la responsabilità di Applogic è limitata agli aspetti di configurazione, sviluppo e gestione applicativa concordati contrattualmente. La sicurezza dell'infrastruttura rimane in capo al cliente.

7. Conformità Normativa e Dichiarazioni

Applogic S.r.l.s. dichiara di operare in conformità a:

- Direttiva (UE) 2022/2555 – NIS2
- D.Lgs. 4 settembre 2024 n. 138 (recepimento NIS2)
- Regolamento (UE) 679/2016 – GDPR
- Regole tecniche e operative del Registro .it (CNR) per i domini nazionali
- Normativa AgID per i servizi PEC
- Best practice di sicurezza ICT

Applogic accetta eventuali verifiche documentali richieste dai propri clienti nell'ambito degli obblighi NIS2 sulla supply chain, ai sensi dell'art. 21 della Direttiva NIS2 e del D.Lgs. 138/2024.

8. Aggiornamento del Documento

Il presente documento è soggetto a revisione annuale o in caso di modifiche significative ai servizi, all'infrastruttura o al quadro normativo di riferimento. La versione aggiornata sarà pubblicata sul sito web aziendale www.applogic.it

Per informazioni, richieste di audit documentale o chiarimenti in merito alle misure di sicurezza adottate, contattare:

Applogic S.r.l.s. | applogic@gov.ecert.it
info@applogic.it | www.applogic.it

Ragusa, 3 dicembre 2025
Il Legale Rappresentante
Dott. A.Lazzara
Applogic S.r.l.s.