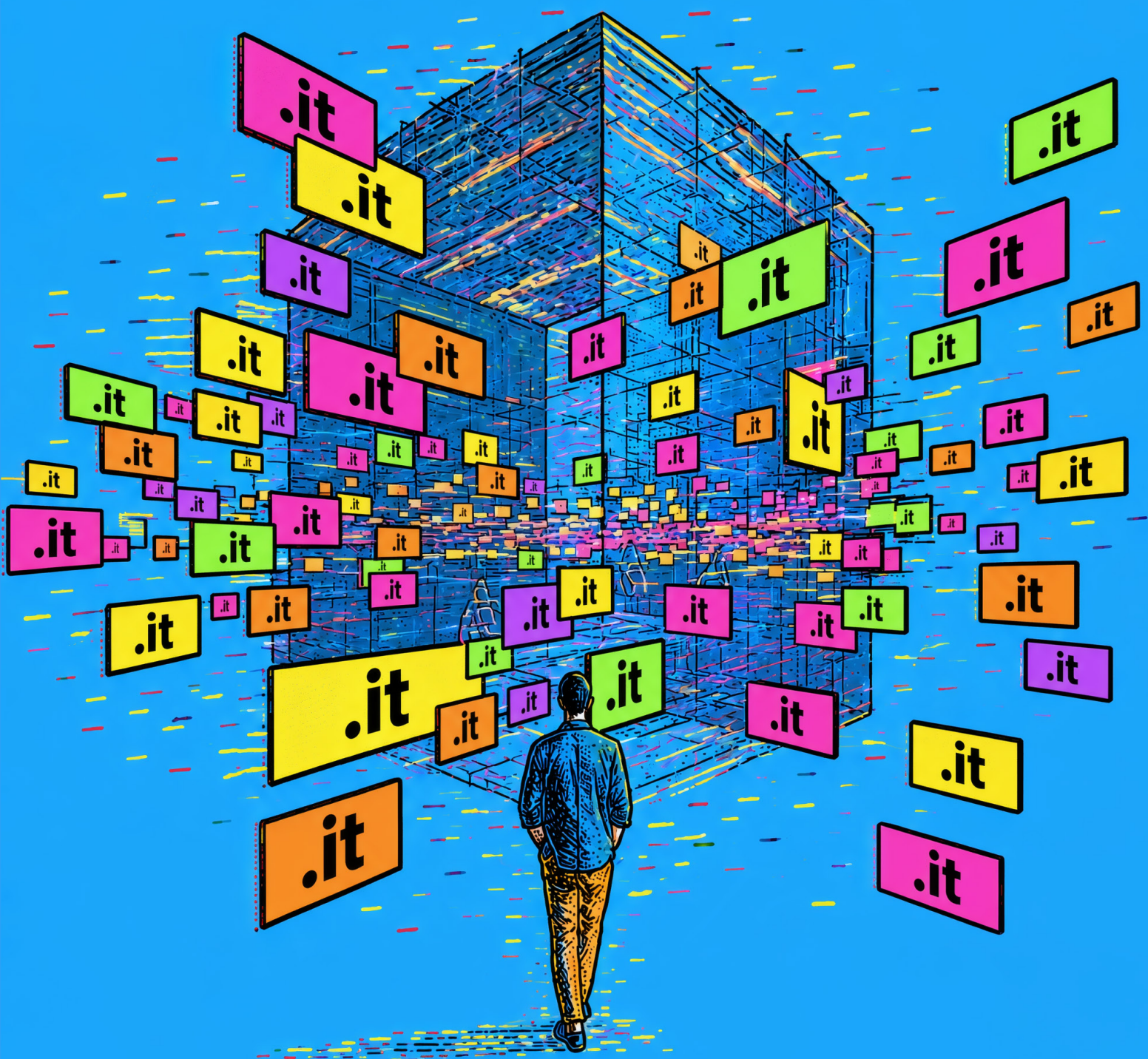


# dot it

DOMAINS • OPINIONS • TRENDS



**Registro.it**

L'ANAGRAFE DEI DOMINI .IT

#### EDITORIAL COORDINATION

Chiara Spinelli

#### EDITORIAL COMMITTEE

Valentina Amenta, Maurizio Martinelli,  
Chiara Spinelli

#### GRAPHIC DESIGN

Coesiva

#### EDITORIAL BOARD

Francesca Nicolini  
(editorial coordinator),  
Stefania Fabbri, Chiara Spinelli

#### PARTICIPANTS

Giorgia Bassi, Beatrice Lami,  
Gino Silvatici, Chiara Spinelli,  
Luca Albertario  
con Sonia Sbrana e Daniele Pancrazi  
(legal captions)  
Michela Serrecchia  
(technical captions)  
Silvia Giannetti (operational captions)

#### DATA SOURCE

Systems and Technological Development  
Unit of the .it Registry

#### DATA PROCESSING

Lorenzo Luconi Trombacchi,  
Michela Serrecchia  
(Systems and Technological Development  
Unit of the .it Registry)  
Luca Albertario, Daniele Pancrazi,  
Sonia Sbrana  
(Legal Aspects and Litigation Unit)  
Silvia Giannetti (Operations and Registrars  
Services Unit)

#### EDITED BY

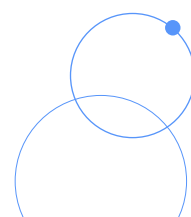
External Relations, Media, Communication  
and Marketing Unit

Via G. Moruzzi, 1  
I-56124 Pisa  
tel. +39 050 313 98 11  
e-mail: [info@registro.it](mailto:info@registro.it)  
website: [www.registro.it](http://www.registro.it)

#### HEAD OF REGISTRO .IT

Andrea Passarella

Registro .it è gestito da:



|           |                                                                                                                              |    |
|-----------|------------------------------------------------------------------------------------------------------------------------------|----|
| <b>01</b> | <b>Preview   4</b>                                                                                                           |    |
|           | • Understanding change, building the digital future                                                                          | 5  |
| <b>02</b> | <b>Statistics   8</b>                                                                                                        |    |
|           | • Annual growth of .it                                                                                                       | 9  |
|           | • Four-month growth of .it                                                                                                   | 10 |
|           | • Top 10 regions with the most .it domains                                                                                   | 11 |
|           | • The types of .it domain assignees                                                                                          | 12 |
|           | • Reasons for oppositions                                                                                                    | 13 |
|           | • Opposition report - reassignments                                                                                          | 14 |
|           | • Annual trend of oppositions - reassignments                                                                                | 15 |
|           | • Resolution of Oppositions                                                                                                  | 16 |
|           | • Domain verification by the Registro                                                                                        | 17 |
|           | • Authinfo requests                                                                                                          | 18 |
|           | • Requests by competent Authorities                                                                                          | 18 |
|           | • Reserved Domain Names for Italian Municipalities                                                                           | 19 |
| <b>03</b> | <b>News   20</b>                                                                                                             |    |
|           | • Cybersecurity, from research to training: a day dedicated to digital security at the Internet Festival                     | 22 |
|           | • Registrar courses: training and updating on the technologies and processes of the Registro .it                             | 25 |
|           | • Scientific dissemination and educational game: two new initiatives for the Ludoteca of Registro .it                        | 29 |
| <b>04</b> | <b>Insights   28</b>                                                                                                         |    |
|           | • NIS2 and the future of the Italian Registro.<br>Interview with Andrea Passarella                                           | 33 |
|           | • From data to strategy: understanding .It to envision its future                                                            | 41 |
|           | • The Ludoteca of Registro .it, cybersecurity and digital education: with 'Train the Trainer', training starts with teachers | 46 |
|           | • NIS2: certification, harmonisation and 'report once' on the agenda of the European Parliament                              | 51 |
| <b>05</b> | <b>Events   66</b>                                                                                                           |    |
|           | • International events from the Internet world                                                                               | 67 |

01

Preview  
Statistics  
News  
Insights  
Events

# UNDERSTANDING CHANGE, BUILDING THE DIGITAL FUTURE

*From the growth of .it domain names to the transformations introduced by artificial intelligence, from the new challenges of cybersecurity to the training of operators and teachers: this issue of DOT describes an evolving digital ecosystem and the commitment of the Registro .it to interpret its changes, strengthen its security and promote new skills*

by Francesca Nicolini

**T**he digital ecosystem is undergoing a profound transformation. Artificial intelligence changes the way we search for and use information, the evolution of cyber threats imposes new defence strategies, while the European regulatory framework assigns increasingly specific responsibilities to those who manage essential infrastructures and services. Technologies change, but so do behaviours, the skills required and the value placed on one's own online presence.

It is in this scenario that the content of the new issue of DOT takes shape, examining change from different perspectives and connecting trends in .it domain names, infrastructure security, the training of operators and the education of the new generations.

The starting point is the data. At the end of the second four-month period of 2026, registered .it domain names reached 3,623,902, representing an increase of 2.44% compared to the same period in 2025. The balance for the four months is also largely positive: new registrations exceed cancellations by more than 45 thousand units. Numbers that testify to the vitality of .it, but that also require looking beyond growth to understand how the transformations of the digital ecosystem are changing the role and value of domain names.

What does it mean today to choose a domain name and build an independent online presence? What value do enterprises, professionals, and users place on .it? And how are these perceptions changing in an environment where AI-based search engines and conversational systems redefine how online content is accessed? The **strategic research promoted by the Registro .it and entrusted to The Fool** aims to answer these questions. **The survey**, which is dedicated to one of the issue's insights, **analyses the perception of domain names and the positioning of .it in relation to other extensions**, involving the different actors in the supply chain and combining qualitative and quantitative research tools. The aim is to **build a knowledge base to understand new behaviours, to identify priority targets and to guide future strategies** for communication and positioning.

In the new digital environment, **the domain name continues to serve as a means of safeguarding one's own online identity**. It is a resource that enables businesses and professionals to build a recognisable and lasting presence, through an autonomous space in which to present themselves, provide services and develop relationships with their communities of reference. Understanding how this value is perceived today is a necessary step to **interpret change** without relying on assumptions but **starting with data and testimonies**.

Alongside the changes affecting the online presence, there is the other major topic covered by this issue: **digital security**. **The NIS2 Directive strengthens the European cybersecurity framework** and directly involves organisations responsible for essential services and infrastructure. This topic is particularly relevant in view of the deadline, scheduled for October 2026, by which those included in the NIS list in 2025 are required to have implemented the basic cybersecurity measures. **In the interview with Andrea Passarella, Director of CNR-IIT and Head of the Registro .it, we address the transformations introduced by the legislation** and their impact on a central infrastructure for the functioning of the Internet. The interview also deepens the **path taken by the Registro .it** in terms of organisation, technology and processes, the value of collaboration between the actors in the supply chain and the need to build a culture of security capable of accompanying the evolution of technologies.

Standards, research, innovation and skills will also be at the heart of the **Cybersecurity Day**, organised by CNR-IIT as part of Internet Festival 2026, in collaboration with Fondazione SERICS, Registro .it and Unione Industriale Pisana (Industrial Union of Pisa). **The day**

will bring together representatives of institutions, research, universities and businesses to explore some of the most current topics in the sector: from the evolution of the European regulatory framework to secure quantum communications, from new device authentication systems to the relationship between artificial intelligence and cybersecurity, to the opportunities and vulnerabilities linked to connected cars.

An **important part of the event** will be dedicated to **training**, because the ability to address digital risks does not depend only on the availability of advanced technologies. It requires well-trained people, informed organisations and programmes capable of transferring knowledge and turning it into concrete actions. This need gave rise to ‘**Train the Trainer**’, a **new project developed by the Ludoteca of Registro .it together with the CINI Cybersecurity National Lab**, which will be presented during the afternoon session of Cybersecurity Day. The project was created to strengthen teachers’ skills and foster a shared culture of digital security.

Conceived as a **regional experiment** in Tuscany, the project aims to develop a model that can be replicated in other school settings and, in the long term, on a national scale.

The initiative **will involve a first network of teachers from Tuscany** in a 25-hour course, which will combine the contents curated by CINI with the experience of the Ludoteca in didactic methodologies and game-based learning. **The aim is to provide teachers with knowledge, methodologies and tools to tackle cybersecurity issues in the classroom**, integrating them into digital citizenship pathways and adapting them to the needs of students: the teacher is not only the target of the initiative but plays an active role in the dissemination of a shared culture of digital security.

**The training also concerns accredited Registrars:** the **list of courses** follows the technological, regulatory and organisational evolution of the sector, offering opportunities to update on the tools and processes of the Registro .it. The programme ranges from **RDAP** service for access to registration data to the **accuracy principle and operational management** through **DARWIN**, from **quality management systems** to the **security of Linux systems**, up to the use of **Moodle** for online training.

These are different areas but linked by a common need: to develop skills capable of translating innovations, standards and technological tools into effective practices. **The quality and security of the domain name ecosystem also depend on the ability of its operators to keep up-to-date and face changes that affect the**

entire supply chain.

Finally, a look at the **European debate** is offered by an **in-depth study that draws on the main themes at the heart of the NIS2 revision process**: the possible certification of the ‘**cyber posture**’ (the overall level of security) of the organisation, the **harmonisation of technical requirements** and the ‘**report once**’ principle, which aims to reduce the duplication of incident reporting requirements. The contents of this issue thus return a **dynamic ecosystem**, in which growth, innovation and security cannot be considered separately. Understanding the impact of artificial intelligence, strengthening the resilience of infrastructure, supporting operators and investing in digital education are all part of the same strategy. **For the Registro .it, interpreting the change means continuing to guarantee the quality and security of the service, but also observing the evolution of the Internet**, producing knowledge, supporting its ecosystem and contributing to the dissemination of increasingly necessary skills. Because the digital future will depend not only on available technologies but on the ability to understand them, use them responsibly and govern their evolution.

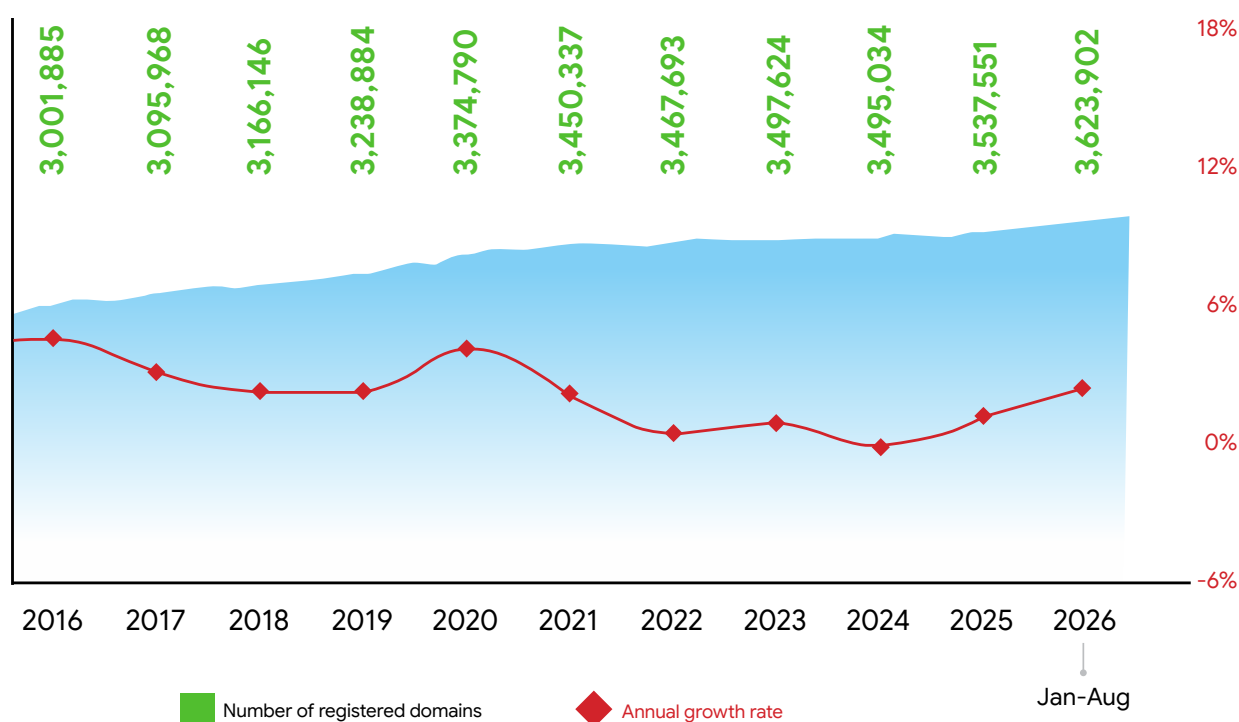
2

Preview  
**Statistics**  
News  
Insights  
Events

## ANNUAL GROWTH OF .IT

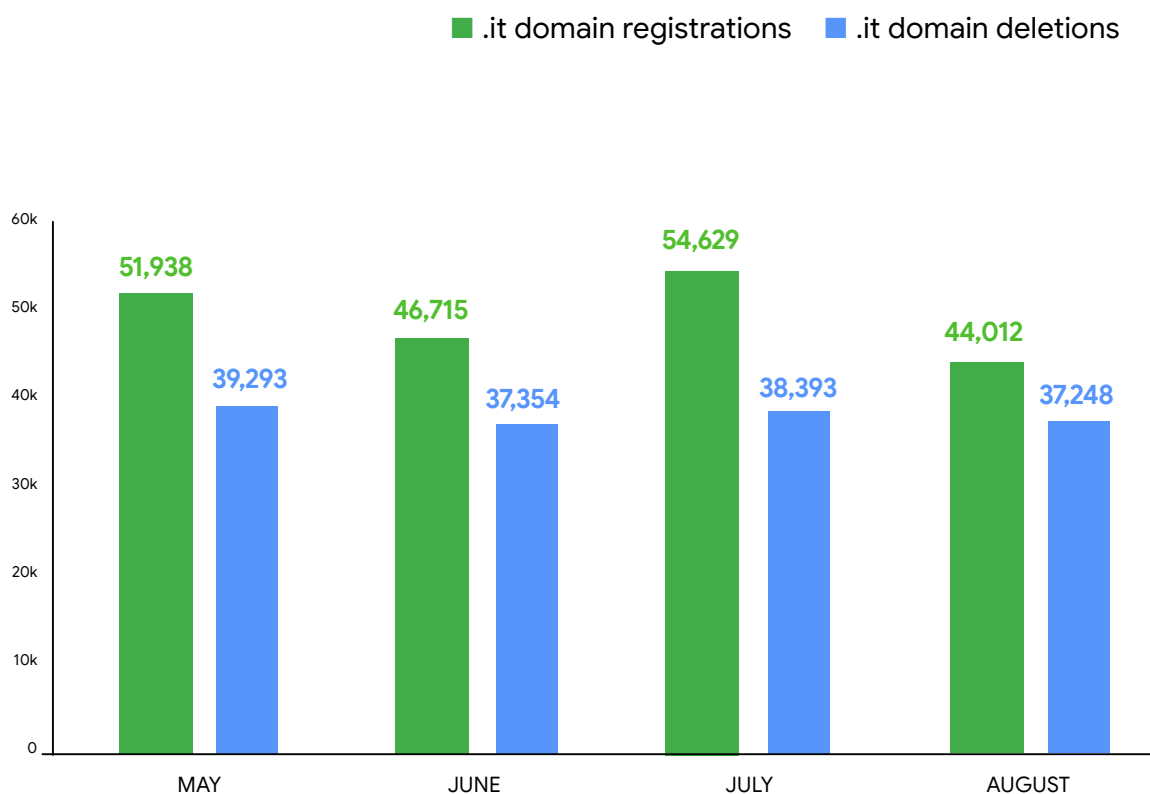
A sharp rise in .it domains: by the end of the second four-month period of 2026, **the total number of registered names had reached 3,623,902**. This significant leap forward represented an **increase of 2.44% (+86,351 domains)** compared with the same period in 2025, a year in which growth had stood at just 0.31% (+10,853 domains compared with the end of 2024).

May–August 2026



## FOUR-MONTH GROWTH OF .IT

An analysis of .it domain name registrations in the second four-month period shows a positive trend compared with the same period of the previous year. **New registrations have exceeded 197,000** (compared with over 145,000 in 2025). Furthermore, whilst in 2025 cancellations exceeded new registrations by around 8,000, **in 2026 the balance is largely positive, with new domains outnumbering cancellations by over 45,000**. The trend is positive in two respects: an increase in new registrations and a simultaneous decrease in cancellations compared to the previous year.



## TOP 10 REGIONS WITH THE MOST .IT DOMAINS

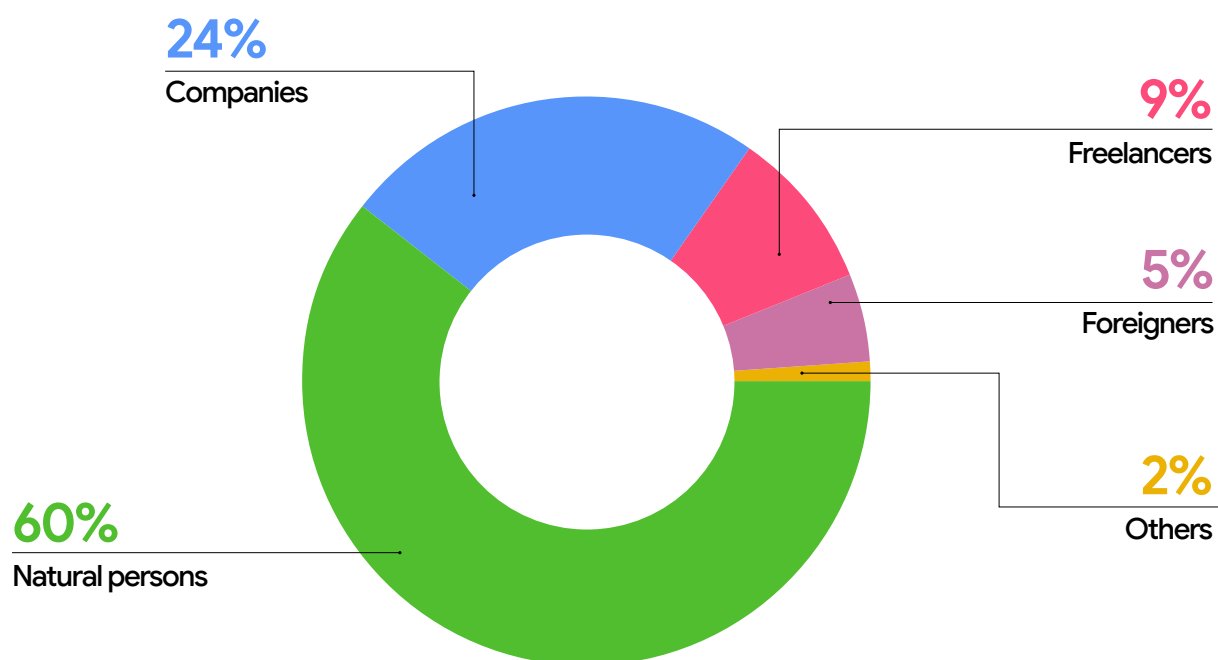
In the four-month period from May to August, **Lombardy and Lazio** retained their **first and second places** in terms of the volume of new domains, **accounting for 21% and 13% of the national total respectively**. It is worth noting the excellent performance of the Veneto region, which has climbed three places **to take third place on the podium with 9%**. By contrast, Piedmont has slipped back, losing two places to settle at 7%, whilst Sicily has slipped three places in the regional rankings compared with the same period in 2025, coming in 7th place.

| Region         | Recordings | Percentage |
|----------------|------------|------------|
| Lombardy       | 31,283     | 20.57%     |
| Lazio          | 19,087     | 12.55%     |
| Veneto         | 13,683     | 9.00%      |
| Campania       | 11,953     | 7.86%      |
| Piedmont       | 10,727     | 7.05%      |
| Emilia-Romagna | 10,589     | 6.96%      |
| Sicilia        | 9,843      | 6.47%      |
| Tuscany        | 9,796      | 6.44%      |
| Apulia         | 7,841      | 5.15%      |
| Sardinia       | 4,065      | 2.67%      |



## THE TYPES OF .IT DOMAIN ASSIGNEES

Compared with May–August 2025, the percentage of new .it domains registered by natural persons increased by ten percentage points in May–August 2026, reaching 60%. This growth came at the expense of businesses and self-employed professionals, which saw a decline (of seven and one percentage point respectively), settling at 24% and 9%.

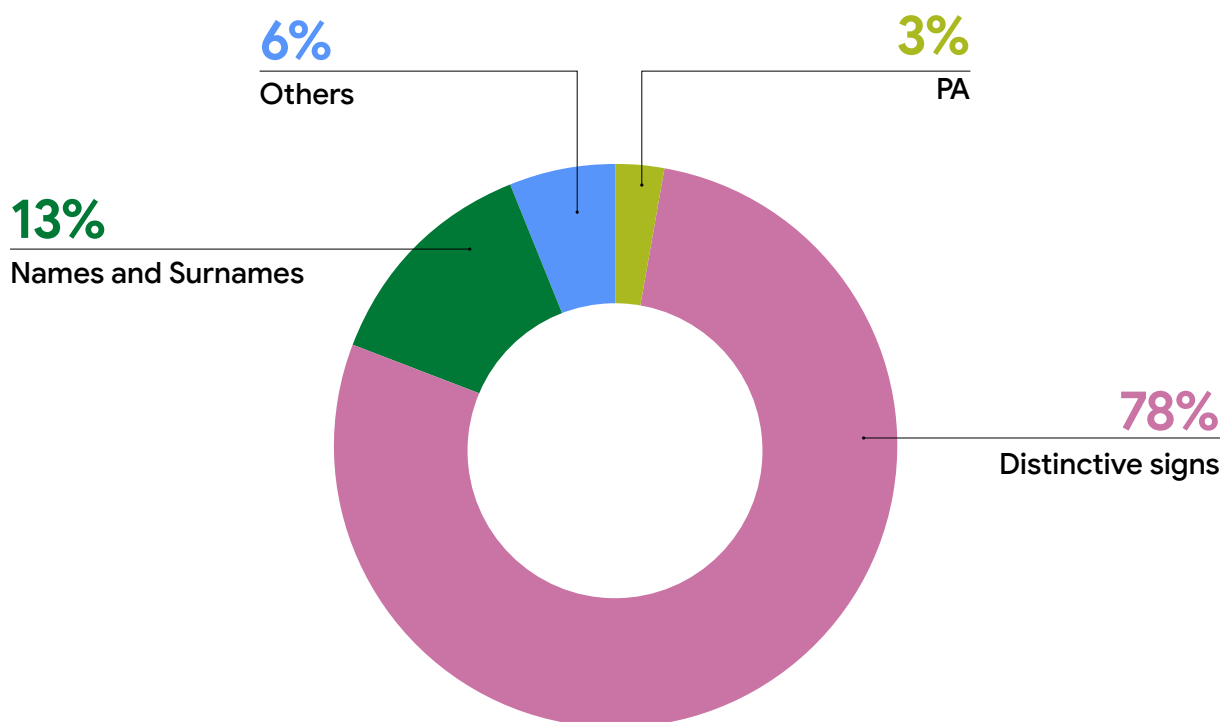


## REASONS FOR OPPOSITIONS

In the middle four-month period of 2026, opposition proceedings launched to protect **distinctive signs continued to account for the predominant share of the total**, with an impact of 78%. Compared with the same period in 2025, when such oppositions accounted for 89% of requests, there has, however, been a decline in their percentage impact.

Oppositions to **names and surnames** are on the rise, **increasing from 1% in 2025 to 13% in 2026**. Oppositions lodged by **public administrations stand at 3%**, down from the 5% recorded in the corresponding period of 2025.

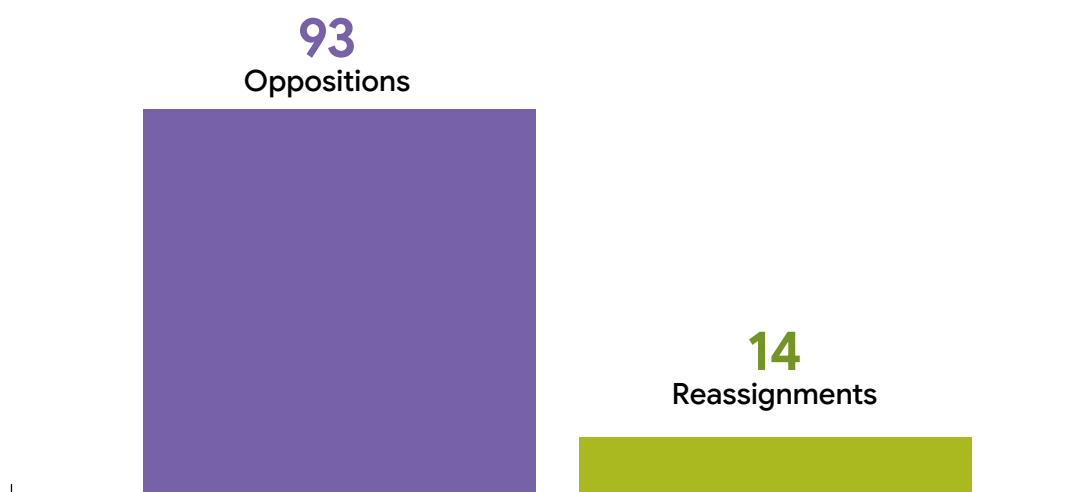
The number of requests attributable to **other reasons (miscellaneous) remains virtually unchanged**, rising from 5% in the second four-month period of 2025 to **6%** in 2026.



## OPPOSITIONS AND REASSIGNMENTS REPORT

**B**etween May and August 2026, **93 oppositions were lodged, (+29) compared with the 64 recorded in** the corresponding period of **2025**. The monthly average stood at 23 oppositions. May saw the highest number of activations (38), followed by July (22) and June (21), while August recorded the lowest figure, with 12 oppositions. From a geographical perspective, **39 oppositions involved exclusively Italian parties**. The North accounts for the majority of assignees/respondents (23), followed by the Centre (9) and the South (6); there is also one case involving an Italian citizen resident in a non-EU country. Among the opponents/complainants, the South has 15, while the North and the Centre both have 12. The picture is completed by **44 oppositions brought by Italian parties against foreign assignees**, 5 initiated by foreign parties against Italian assignees and, finally, 5 procedures involving exclusively foreign parties.

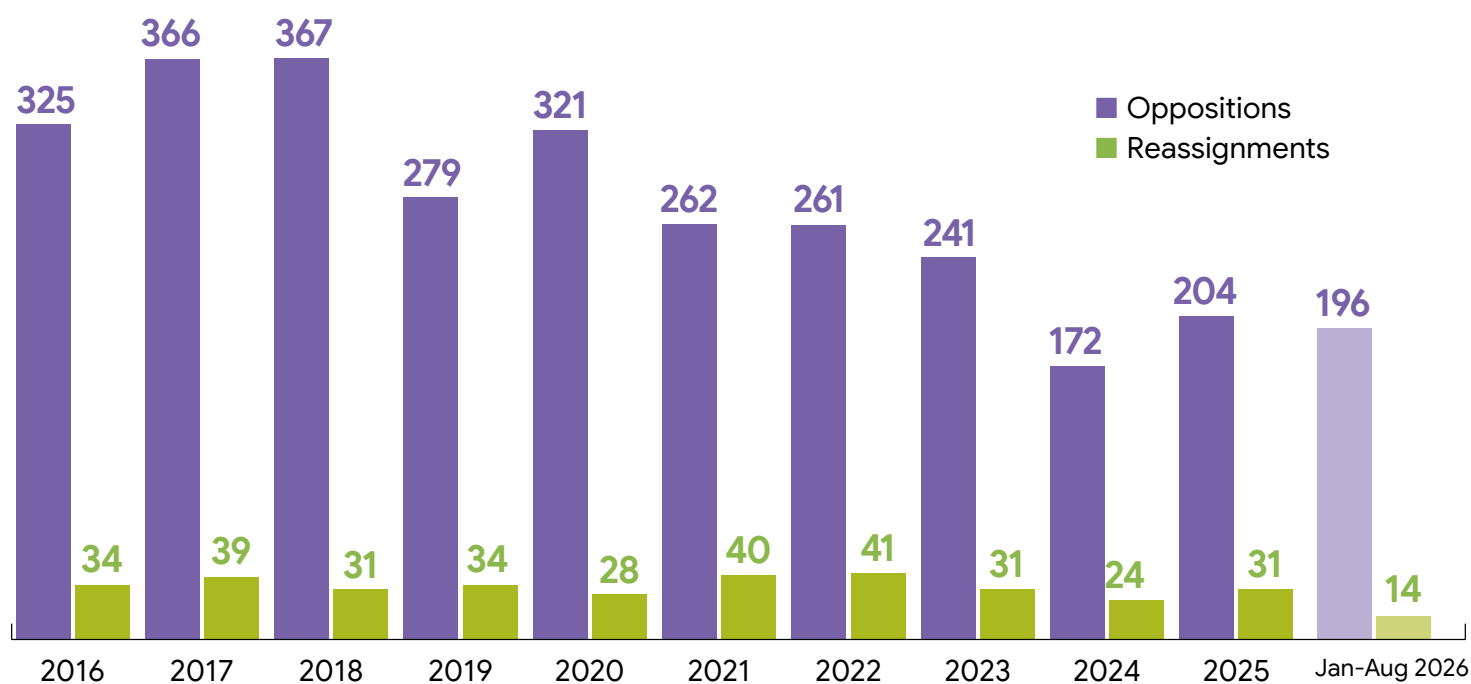
During the same period, **14 reassignment procedures** were initiated at a Dispute Resolution Service Provider (PSRD), **an increase (+6) compared with the 8** recorded in the corresponding four months **in 2025**. The highest number of procedures was initiated in July (6), followed by June (4) and May (3), while only one reassignment procedure was initiated in August.



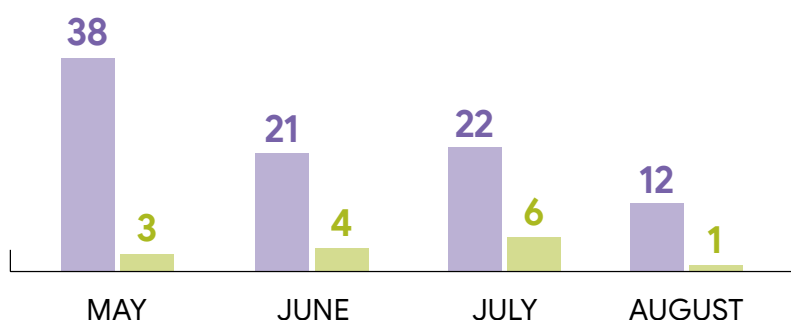
## ANNUAL TREND OF OPPOSITIONS - REASSIGNMENTS

**C**ompared with the corresponding four-month period in 2025, the period from May to August 2026 saw an increase in the number of oppositions from 64 to 93. The increase was recorded in all the months under consideration, peaking in May (+16 oppositions, from 22 to 38), followed by June (+6, from 15 to 21), July (+5, from 17 to 22) and August (+2, from 10 to 12).

The **reassignment procedures are increased from 8 to 14 (+6)**. Of these, 12 resulted in the transfer of the domain name to the opponent/complainant, while only one was concluded due to the proceedings being closed. Finally, one procedure remains pending, still awaiting a decision from the Board.



Four-month trend



## RESOLUTION OF OPPOSITIONS

**55%** of the 93 oppositions lodged during the four-month period **are still pending**. Among the oppositions concluded, the revocation of domain names – following verification of the subjective requirements – accounts for the largest proportion, representing 23% of cases. These are followed by the initiation of a reassignment procedure at a PSRD (10%), the domain name holder's waiver of the allocation (5%), the opponent's withdrawal of the opposition (4%) and the cancellation of the domain name by the Registrar (3%).

10%

Activation of reassignment procedure

23%

Domain names revocation

3%

Cancelled by the Registrar

5%

Renunciation by the assignee

4%

Opposition abandonment

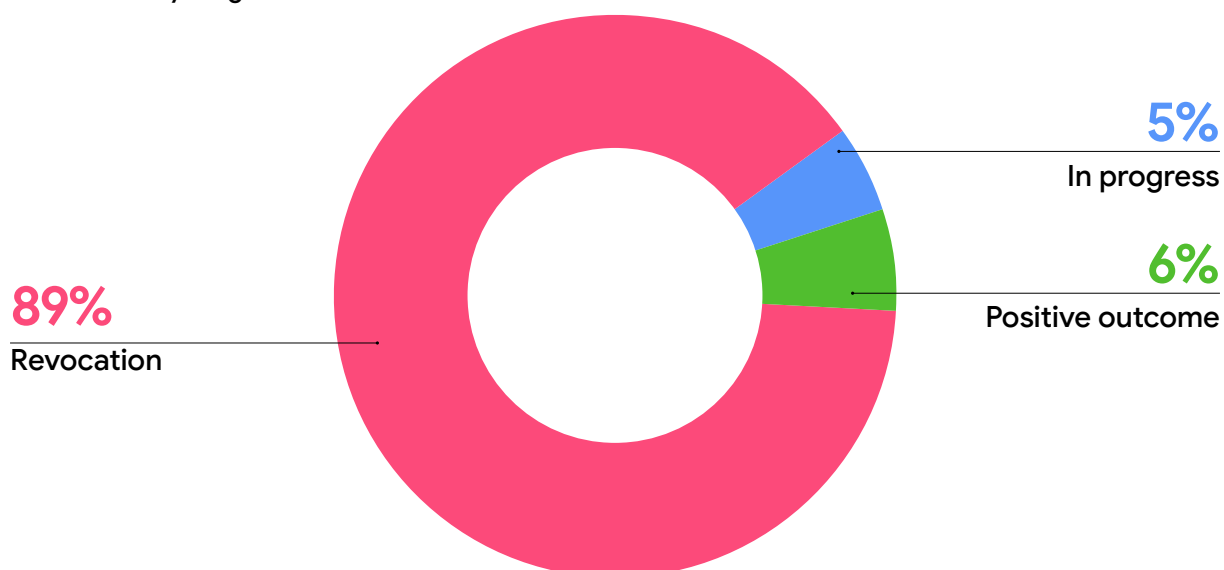
55%

Pending oppositions

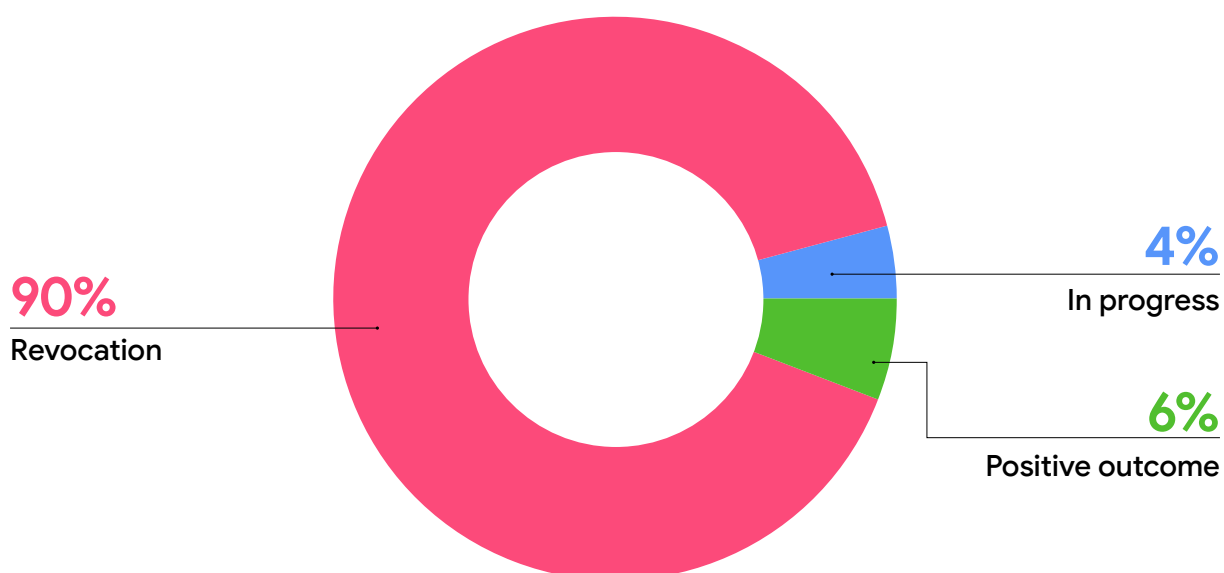
## DOMAIN VERIFICATION BY THE REGISTRO

In order to verify the accuracy of the Registrants' details held in the Whois database, the Registro .it initiated **98 verification requests involving 114 domain names**: of these, **103** were **revoked** and only **6** were **successful**. For **5** domain names, **verifications** are still **in progress**.

### Checks May-August 2026



### Domains involved May-August 2026



## AUTHINFO REQUESTS

In the second four-month period of the year, **the Registro .it issued 15 AuthInfo codes** directly to Registrants, to protect them in cases where the Registrar was no longer active. There were 6 Registrars involved.

15



Authinfo code  
requests

22



Domains

6



Registrars involved

## REQUESTS BY COMPETENT AUTHORITIES

The competent Authorities, in compliance with legal prerogatives, have requested information regarding certain assignees of domain names registered in the ccTLD .it: in the second four-month period, **there were 39 requests relating to the same number of domain names**.

39



Requests

39



Domains involved

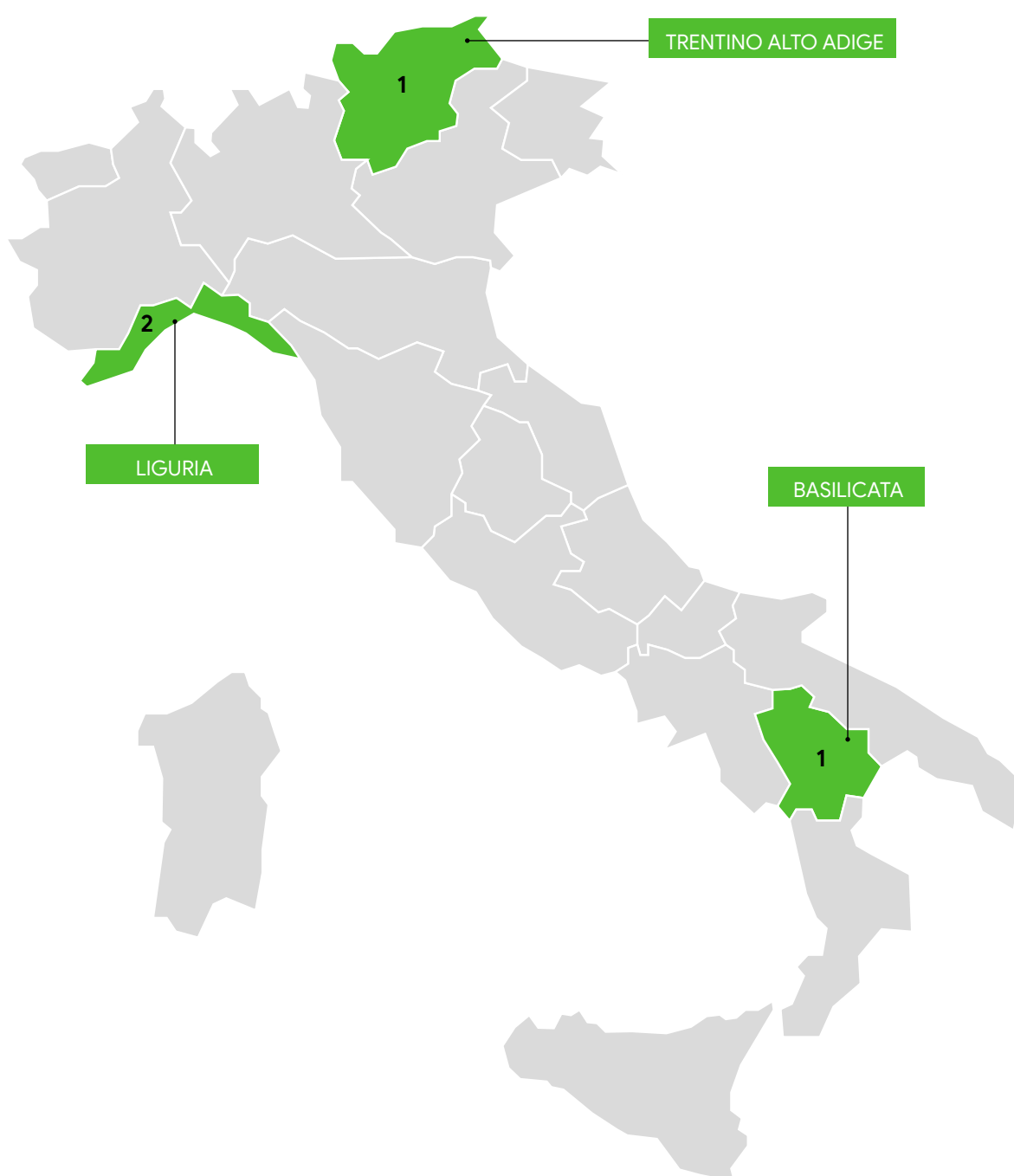
4



Reserved names

## RESERVED DOMAIN NAMES FOR ITALIAN MUNICIPALITIES

**D**uring the period under review, **there were 4 registrations of reserved names** (in this case, for Italian municipalities), namely: `comune.grigno.tn.it`, `comune.vallecrosiaalmare.im.it`, `comuneditrivigno.it` and `comune.pontinvrea.sv.it`.



03

Preview  
Statistics  
**News**  
Insights  
Events

# CYBERSECURITY, FROM RESEARCH TO TRAINING: A DAY DEDICATED TO DIGITAL SECURITY AT THE INTERNET FESTIVAL

The usual **Cybersecurity Day**, organised by the Institute of Informatics and Telematics (CNR-IIT), in collaboration with the Fondazione SERICS, Registro .it and Unione industriale Pisana (Industrial Union of Pisa), returns on **9 October**, as part of the 2026 edition of the **Internet Festival**.

The initiative is part of the programme of the Internet Festival 2026, now in its sixteenth edition. This year is dedicated to the **keyword #wisdom**. A concept that is particularly relevant in the field of cybersecurity as well: faced with the increasing complexity of digital technologies, the spread of artificial intelligence and the evolution of cyber threats, **security depends not only on technological tools, but also on the ability to make informed and responsible choices**. In this sense, wisdom can be read as the ability to navigate change, assess risks and opportunities, and manage innovation with balance and vision.

The event, scheduled at the **Auditorium of the headquarters of the Industrial Union of Pisa**, will bring together representatives of institutions,



research, universities and businesses to take stock of emerging threats and strategies needed to build a more secure digital ecosystem. At the heart

of the event, an increasingly topical awareness: **cybersecurity is not only a technological issue, but a challenge that requires skills, collaboration and training.**

The **morning** will open with the **institutional greetings** of **Alberto Lenzi**, Councillor of the Tuscany Region with responsibility for cybersecurity, **Andrea Passarella**, Director of CNR-IIT and Head of the Registro .it, **Alessandro Armando** of Fondazione SERICS, **Francesco Palmieri**, Director of CINI (National Interuniversity Consortium for Informatics) Cybersecurity National Lab, and **Andrea Madonna**, President of Industrial Union of Pisa.

**Andrea Rigoni** (Altirium Srl) will open the session dedicated to the most topical issues in digital security with a **keynote speech** focusing on the **evolution of the European regulatory framework on cybersecurity**. Particular attention will be given to the **NIS2 Directive**, which expands the number of those involved and introduces new requirements in the areas of risk management, incident prevention and business continuity. This focus is particularly relevant in view of the **October 2026 deadline**, by which entities included in the national NIS list will be required to implement the baseline cybersecurity measures. This talk will therefore provide an opportunity to deepen the **impact of the legislation on Registrars, organisations and digital operators**, who will be required to adopt an increasingly structured approach to security and strengthen the resilience of the services offered.

Next, the so-called “**cyber information**

**capsules**”, short and targeted speeches, designed to offer in a few minutes ideas and perspectives on innovative technologies and solutions in an ever-changing environment. **Alessandro Zavatta** (QTI Srl) and **Sara Nocentini** (INRiM) will offer two insights on technologies that will play an increasingly important role in digital security. The first will accompany the public in the field of **secure quantum communications**, explaining its principles and possible applications for future cybersecurity; the second will focus on **unclonable physical functions**, used to develop authentication systems that take advantage of the unique features of the devices.

The **morning** will continue with the **keynote speech** by **Stefano Zanero** of Politecnico di Milano, dedicated to the complex **relationship between artificial intelligence and cybersecurity**: two increasingly interconnected areas where AI can be both a tool for strengthening defence capabilities and a factor for expanding and transforming risk scenarios. The session will close with the participation of **Stefano Di Carlo** of Politecnico di Torino, who will analyse **opportunities and vulnerabilities linked to the growing number of connected cars**, systems in which innovation, cybersecurity and digital infrastructure protection are of central importance.

In the **afternoon** the focus will move on one of the crucial issues for the future of cybersecurity: **training**. A **round table**, moderated by **Ilaria Matteucci** of the CNR-IIT, will bring together **Paolo Prinetto** of the CINI Cybersecurity National Lab, **Giuseppe Lettieri** of the University of Pisa and **Mirko Tribastone** of the IMT

School of Advanced Studies of Lucca. The discussion will deepen the **role of training** in developing the specialist skills required by the sector and in defining pathways that can accompany the evolution of cybersecurity.

The event will continue with the presentation of “**Train the Trainer**”, the project born from the **collaboration between the Ludoteca of Registro .it and CINI Cybersecurity National Lab** to promote the diffusion of a culture of cybersecurity through training courses aimed at teachers. The meeting will be introduced by **Alessandra Nardini**,

Councillor of the Tuscany Region for Training and Education, and **Luciano Tagliaferri**, Director General of the Regional School Office for Tuscany. The project will be illustrated by **Giorgia Bassi** of CNR-IIT and **Gabriele Costa** of the IMT School of Advanced Studies of Lucca.

Digital security depends not only on evolving technologies, but also on the ability to develop skills, spread awareness and create connections between research, schools, institutions and businesses. And **investing in training today means preparing for the digital challenges of tomorrow**.



**INTERNET FESTIVAL 2026**  
FORNIRE DI FUTURO

**9 OTTOBRE 2026** | ORE 10-16

# CYBERSECURITY DAY

**MATTINA**

10.00 | WELCOME COFFEE E REGISTRAZIONE

10.30 | SALUTI ISTITUZIONALI E INTRODUZIONE  
Alberto Lenzi, Assessore Regione Toscana alla Cyber sicurezza  
Andrea Passarella, CNR-IIT  
Andrea Madonna, Unione Industriale Pisana  
Giorgia Giacinto, Fondazione SERICS  
Gianluigi Ferrari, Università di Pisa  
Francesco Palmieri, CINI Cybersecuritylab

11.00 | KEYNOTE  
IL FUTURO DELLA SICUREZZA TRA REGOLAMENTI, MINACCE AI E NUOVE TECNOLOGIE  
Andrea Rigoni, Altirium Srl

11.30 | COMUNICAZIONI QUANTISTICHE SICURE: DALLA FISICA ALLA CYBERSECUREZZA DEL FUTURO  
Alessandro Zavatta, QTI Srl

11.40 | AUTENTICAZIONE SICURA CON FUNZIONI FISICHE NON CLONABILI  
Sara Nocentini, INRIM

11.50 | KEYNOTE  
UNA TORMENTATA LOVE STORY: AI E CYBERSECURITY  
Stefano Zanero, Politecnico di Milano

12.20 | IL FUTURO CORRE VELOCE: LE AUTO CONNESSE TRA INNOVAZIONE E VULNERABILITÀ  
Stefano Di Carlo, Politecnico di Torino

Light lunch a seguire

**POMERIGGIO**

14.00 | LA FORMAZIONE IN CYBERSECUREZZA  
Tavola rotonda, modera Ilaria Matteucci, CNR-IIT  
Paolo Primetto, CINI | Giuseppe Lettieri, Università di Pisa  
Stefano Chessa, Università di Pisa | Mirko Tribastone, IMT Lucca

14.45 | IL PROGETTO TRAIN THE TRAINER  
Alessandra Nardini, Assessora Regione Toscana a Educazione e Istruzione  
Luciano Tagliaferri, Direttore Generale Ufficio Scolastico Regionale Toscana  
Giorgia Bassi, CNR-IIT  
Gabriele Costa, IMT Lucca

**AUDITORIUM UNIONE INDUSTRIALE PISANA | Via Volturmo 43, Pisa**

**ISCRIVITI QUI**

ORGANIZZATO DA

IIT ISTITUTO DI INFORMATICA E TELEMATICA CNR

Consiglio Nazionale delle Ricerche

Registro.it

SERICS

Unione Industriale Pisana

# REGISTRAR COURSES: TRAINING AND UPDATING ON THE TECHNOLOGIES AND PROCESSES OF THE REGISTRO .IT

**T**he Registro .it has organised a **calendar of courses dedicated to Registrars**, partly started last months, which will continue **until December**.

**Updating the technical and operational skills of Registrars, increasing their knowledge of the tools made available by the Registro .it and accompanying operators in the regulatory and technological evolution of the domain name system:** these are the objectives of the training programme that the Registro .it dedicates to accredited operators.

An activity that contributes to enhancing quality, security and efficiency in domain name management, through moments of in-depth analysis on technical, organisational and regulatory issues and useful tools for daily activities and updates affecting the sector. The 2026 edition proposes a programme that ranges from the evolution of data access protocols to information accuracy management, from process quality to the security of Linux systems, to online training tools.

## FULL 2026 COURSE CALENDAR

|                                                                                             |                                     |                                                                 |
|---------------------------------------------------------------------------------------------|-------------------------------------|-----------------------------------------------------------------|
| THE RDAP SERVICE                                                                            | 25 September, from 9 a.m. to 1 p.m. | Course completed                                                |
| THE PRINCIPLE OF DATA ACCURACY: REGULATORY FRAMEWORK AND OPERATIONAL MANAGEMENT WITH DARWIN | 19 October, from 9 a.m. to 1 p.m.   | Streaming                                                       |
| THE QUALITY MANAGEMENT SYSTEM                                                               | 10 November, from 10 a.m. to 1 p.m. | Streaming                                                       |
| HARDENING LINUX SYSTEMS AND SERVICES                                                        | November (date to be confirmed)     | Streaming                                                       |
| MOODLE, AN ONLINE TRAINING PLATFORM                                                         | Scheduled until 30 December         | On-demand course, available in the Registro .it Academy section |

## THE RDAP SERVICE

**25 September 2026, from 9 a.m. to 1 p.m. - Streaming**

The course **focused on the Registration Data Access Protocol (RDAP) service**, the international standard developed by IETF for access to domain name and IP address information.

For decades, the **WHOIS** protocol has been the universal tool for querying and obtaining information from Internet registries. However, WHOIS is now revealing all its operational limitations: lack of structured formats, total lack of internationalisation, inability to manage data privacy (as required by the GDPR - General Data Protection Regulation) and a chronic lack of security and authentication.

Based on a modern **HTTP/REST** architecture and responses in JSON format, RDAP is not just an upgrade, but a real infrastructure revolution. **This protocol allows** registries (such as the Registro .it) and Registrars **to provide a secure, scalable data consultation service, which is easily integrated with other software and natively designed for access control and protection of sensitive data.**

The aim of the course was to guide participants through a path that starts from the fundamentals of the protocol – architecture, data model, query types, structure of responses and errors, bootstrapping mechanism – to the most advanced aspects: some of the extensions already standardised or being standardised, the operational and security implications for registries and Registrars.

## THE PRINCIPLE OF DATA ACCURACY: REGULATORY FRAMEWORK AND OPERATIONAL MANAGEMENT WITH DARWIN

**October 19, 2026, from 9:00 AM to 1:00 PM – Streaming**

In today's digital ecosystem, the quality and truthfulness of information is no longer just a management requirement but a fundamental pillar of cybersecurity and legal compliance. **This training module aims to deepen the principle of data accuracy by analysing its evolution and central role within the new European regulatory framework.**

From theory to practice, the second part of the module will provide a technical and operational analysis of **DARWIN** (Data Accuracy Registrar Web Interface), the strategic web application developed by the Registro .it to support Registrars in verifying, updating, and improving the quality of data associated with domain names.

## THE QUALITY MANAGEMENT SYSTEM

**10 November 2026, from 10 a.m. to 1 p.m. - Streaming**

The course will provide an **overview of the principles and requirements of the ISO 9001 standard, with particular reference to their application in the domain name sector**. The main aspects of process management, performance monitoring, customer satisfaction and continuous improvement will be explored through **practical examples and case studies**.

## HARDENING LINUX SYSTEMS AND SERVICES

**(date to be confirmed)**

**November 2026 - Streaming**

The course will focus on the **security of Linux systems and services**, with a path that will address access and authentication management, file security and permissions, network protection through firewalls and VPNs, and hardening of critical services. Container **hardening, monitoring and logging** for security, **auditing** and **security compliance** will also be covered, with reference to tools and standards such as Lynis, CIS Benchmarks and OpenSCAP, in addition to encryption and data protection at rest and in transit, with examples of technologies such as LUKS.

## MOODLE, AN ONLINE TRAINING PLATFORM

**On-demand course, already available in the Academy section of the Registro .it (<https://academy.nic.it/login/index.php>) and will be open until 30 December 2026**

The course is **intended for Registrars who intend to use Moodle for the delivery of online learning activities**.

It is divided into two main sections:

1) The **first section** covers the installation and administration of the Moodle platform:

Module 1: Installation

Module 2: Administration

2) The **second section** involves the teachers setting up and managing an online course, and providing participants with the materials they need to complete the course and the tools required for active participation:

Module 3: Setting up and managing an online course

Module 4: Activities and Resources

### Enrolment and information

Registrars interested in attending the courses **can register through the [RAIN portal](#)** For courses delivered via **streaming**, the link to join will be sent to registered Registrars **one week before the course begins**.

The **Registrar 2027 course programme is currently being prepared**. Topics, modalities and dates of upcoming events will be defined and communicated at a later date.



# SCIENTIFIC DISSEMINATION AND EDUCATIONAL GAME: TWO NEW INITIATIVES FOR THE LUDOTECA OF REGISTRO .IT

Education, research and dissemination are fields that are increasingly called upon to engage in dialogue and to experiment with new ways of communicating and learning. Against this backdrop, the **Ludoteca of Registro .it brings its expertise and approach to play to bear in its engagement with the worlds of education, research and training.**



On the right, **Giorgia Bassi**, coordinator of the Registro .it Ludoteca project

Between May and August 2026, this programme took the form of **two events**, each with a different focus and format.

Last **May**, the Ludoteca of Registro .it took part in the **conference ‘Education and Research: public engagement for the scientific culture of the future’** (Ischia, 10–13 May). The initiative, which was also aimed at teachers and organised by the research bodies INFN (National Institute for Nuclear Physics), INAF (National Institute for Astrophysics), INGV (National Institute of Geophysics and Volcanology) and CNR (National Research Council), provided an **important opportunity for reflection and discussion on the role of scientific dissemination in society**.

Among the topics addressed during the panel discussions, round-table discussions and workshops, particular attention was paid to innovative formats for scientific dissemination, educational resources and programmes for schools, teacher training, and bridging the gender gap in STEM (Science, Technology, Engineering and Mathematics). These are the areas that have characterised the work of the Ludoteca of Registro .it for many years. These are areas that have long been central to the activities of Ludoteca del Registro .it, which was a key contributor to the session.



The “Internetopoli” game

**‘Tools/content/resources for schools’**, presenting its educational offering and its approach to game-based learning.

In **June**, the Ludoteca of Registro .it took part in the **‘Board Game Research Meeting’** (Genoa, 11-13 June), a scientific and interdisciplinary conference entirely **dedicated to the analysis of board games** as a subject of study, a cultural practice and a tool also used in an educational context, presenting the floor game **‘Internetopoli - The Game’**, designed for primary and lower secondary schools.

The game, which has been used in recent years mainly during participation in festivals and scientific dissemination events, is inspired by the traditional Game of the Goose and has been designed to be flexible and adaptable, so as to suit both the time available and the age and skills of the players. Along the way, the teams are faced with games, challenges and unexpected situations that encourage discussion, collaboration and critical thinking. The setting is one of the central elements of the game: the Internet is described as a city in its own right, made up of addresses, places and the people who live there every day. The topics covered range from how the Internet works to social networks, from online privacy to smart cities and the Internet of Things, up to online content and fake news.



The “Internetopoli” game



4

Preview  
Statistics  
News  
Insights  
Events

# NIS2 AND THE FUTURE OF THE ITALIAN REGISTRO

## Interview with Andrea Passarella

The new regulatory framework derived from the NIS2 Directive has been in force in Italy since 16 October 2024. Two years after its entry into force, implementation enters a decisive phase: digital security increasingly concerns the organisation, processes and collaboration between interdependent actors, as well as technologies. We talk about it with Andrea Passarella, director of the Institute of Informatics and Telematics (IIT) of the CNR and Head of the Registro .it, to understand what is changing for the domain name system, how the Registro has prepared itself for the operational deadlines of 2026 and what prospects are opened up by artificial intelligence and, in the medium term, by quantum technologies

Interview by Francesca Nicolini

**1** NIS2 marks an important evolution in the European cybersecurity strategy. Why is this directive so important, and what changes from the past?

NIS2 is based on a very concrete observation: **digital services are now part of the essential infrastructure of our societies**. An incident involving a network, cloud service or domain name system can spread rapidly and have consequences that go far beyond the target. That is why the European Union has widened the scope of the organisations involved and strengthened the level of responsibility required. **The**

**aim is to bring cybersecurity into the ordinary decisions of governance and management of organisations.**

The most important change is the **risk-based approach**. Security is not treated as a static list of technical requirements, which is the same for everyone and valid once and for all. **Each organisation must be aware of the services it provides, identify the systems and dependencies that make them possible, assess threats and the potential impact of incidents, and then choose appropriate and proportionate measures.** This requires a continuous cycle: analysis, prevention, monitoring, response and improvement. Compliance thus becomes the result of

verifiable organisational capacity, not a separate document-based exercise from daily operations.

This setting is particularly important for Internet services. The Internet is a distributed system in which no single operator controls all the components necessary for service continuity. Interdependencies, supply chain, external services, vulnerability management and the ability to share relevant information in a timely manner should also be considered. NIS2 also introduces a more direct involvement of administrative and management bodies: **security responsibilities, priorities and resources must be clear and attended to at the appropriate level.**

In my view, the strategic value of the directive lies precisely here. **NIS2 creates a common framework between**

*Compliance becomes the result of verifiable organisational capacity, not a separate document-based exercise from daily operations*

**different organisations and calls for security to be measurable, governed and updated over time.** For an Internet infrastructure, it means constantly assessing risk, taking appropriate



**Andrea Passarella**, Director of CNR-IIT and Head of Registro .it, at the celebration marking 40 years of the Internet in Italy, organised by CNR-IIT

measures, strengthening the ability to continue to deliver the service even under adverse conditions, limiting the effects of an incident and quickly restoring full operation.

## **2** The Registro .it is directly involved in the evolution of the European framework on Internet security. What are the main challenges that NIS2 poses to an infrastructure such as the Registro?

A country code top-level domain registry, or ccTLD, performs a specific, and the same time systemic, function. **The Registro .it maintains the database of Italian domain names and ensures the proper functioning of the services that make those names accessible on the Internet.** Availability, integrity and correctness of information are therefore essential. **A disruption would not affect a single organisation but could impact a very large part of the national digital ecosystem.**

*The accuracy of the data is an essential element in preventing abuse, effectively managing incidents and ensuring the reliability of the system*

The **first challenge** is to **translate the principle of risk management into a non-disruptive**, high-volume, and evolving attack surface **environment**. Attempts to alter or misuse data, credential compromise, technology and delivery dependencies, operational errors, and physical events that can impact continuity must be considered as attacks on DNS services. For each scenario, prevention measures, detection capabilities, response procedures and continuity plans are needed, verified with regular exercises.

A **second challenge** concerns the **traceability of decisions and responsibilities**. Mature infrastructures such as ours already have advanced technical controls, but NIS2 calls for them to be brought back to a unified framework, linking risks, measures, evidence and roles. It means documenting what is being done in a more structured way, verifying the effectiveness of controls, managing incidents according to defined flows and driving improvement with what is learnt from day-to-day operations.

Then, there is a **dimension of the domain name industry**. The legislation requires operators of top-level registries and entities providing registration services to **collect and maintain accurate and complete data**, applying proportionate verification procedures and making policies publicly available. The accuracy of data is not just an administrative issue: it helps to prevent abuse, makes incident management more effective and increases the overall reliability of the system, while respecting the protection of personal data.

**3** With the 2026 operational deadlines approaching, how has the Registro

.it prepared for them, and what have been the most significant changes in terms of organisation, technology and processes?

The Registro does not start from scratch. **The infrastructure has always been designed and upgraded to ensure high levels of security, availability and reliability.** The technological work required by NIS2 is therefore part of a continuous path: strengthening the monitoring, access protection, vulnerability management, responsiveness, redundancy and business continuity. **The compliance** does not coincide with a single project ending at a certain date; **it is part of the ordinary evolution of a critical infrastructure for the country.**

**The most profound intervention concerns the organisation and the processes.** We reviewed how we identify and assess risks, relating threat scenarios to relevant services, assets and dependencies. On this basis, we are making responsibilities, decision-making flows and operational steps even more explicit. **The aim is that, under normal conditions such as during an incident, each function knows what actions to take, what information to share and what decisions should be taken at the different levels** in a precise and documented manner.

Another **key element** is **people accountability.** Procedures are effective only if the person applying them understands the reasons for them and recognises anomalous situations in a timely manner. That is why we have invested in **specific staff training** and in **fostering a shared understanding**, including amongst those who do not hold

*The Registry has made itself available to the national domain name ecosystem to share actions and measures and act as a “hinge” between institutions and the business community*

strictly technical roles. Security, in fact, involves purchasing, contracts, human resources management, communication, vendor relationships and data governance. Finally, **NIS2 has given further impetus to work on the accuracy of data associated with the registration of domain names.** It is a process that requires clear rules, sustainable controls and collaboration across the entire supply chain, from the Registro to Registrars up to registrants. The Registro, even before the entry into force of NIS2, has launched a fundamental process to improve the accuracy of data related to domain name registration, including investing in automated procedures that generate “alerts” in suspicious cases that need to be investigated in detail. **We are working to ensure that the verification mechanisms are effective and proportionate**, without introducing unnecessary complexity for legitimate users. **The deadline for October is therefore a verifiable step in a path that has already begun, not the point of arrival.**

*If applied strictly, NIS2 can therefore produce an advantage beyond compliance: a Registro better organised in its processes, more aware of its dependencies and better prepared to respond to change*

**4 NIS2 is geared towards the resilience of the entire digital ecosystem. How important is it that the Registro, Registrars, providers and others in the supply chain work in a coordinated manner?**

It is essential because, within the domain name system, the quality of service depends on a chain of subjects. The Registro manages the top-level domain and registration platform; Registrars work in the relationship with registrants; providers and technology vendors make connectivity, hosting, DNS and other services available. An incorrect entry, a compromised credential or an uncoordinated response procedure can affect other components as well. **The resilience of the system is therefore also determined by the quality of the relations between the actors.**

**NIS2 makes this interdependence more visible. The Registro must govern its own risks but it must also include those arising from shared suppliers and processes.** Similarly, Registrars are

called upon to contribute to the security and accuracy of data according to their role. This requires understandable requirements, reliable communication channels, consistent procedures for managing incidents and technical confrontation moments. In case of a significant event, the speed and quality of the information exchange can make the difference between a localised problem and a wider disruption.

**Coordination must be concrete and sustainable.** It is not a question of passing on obligations across the chain but of **giving each subject responsibilities commensurate with the assets it controls and the risks it can manage.** The Registro may provide tools, guidelines, training and verification mechanisms; Registrars may contribute with knowledge of the customer relationship and the correct application of procedures; providers must ensure the reliability of the services on which the chain depends.

**This collaboration also produces a system benefit.** Shared standards and regular dialogue reduce ambiguity, facilitate incident response and enable better practices to be disseminated more quickly. For the end user, the result must be a simple experience, supported by a chain that recognises risks and manages them in a coordinated way.

Also on the basis of these considerations, the Registro has made itself available to the national ecosystem of domain name registration, both to share actions and measures to be implemented, and as a “hinge” between the institutional level (the articulations of the state responsible for regulating the NIS2) and the productive fabric of related companies. The

collaboration between all these actors, within the limits of their respective competences and prerogatives, is helping to manage the shift in the operational paradigm brought about by the entry into force of NIS2.

**5** The process of compliance goes beyond simply meeting regulatory obligations. What implications might this have for the Registro .it, and how do security standards and requirements provide tangible value for Registrars, businesses and users?

**We consider NIS2 as a lever to further improve the way the Registro operates.** Systematic risk analysis helps to set priorities, clarify processes and link investments to scenarios that may have the greatest impact. The provision of the evidence required by the legislation is also of operational value: it allows verification of whether the measures are applied, whether they work and whether they need to be updated. **Compliance**, in this perspective, **consolidates the quality of management**.

**For Registrars**, smoother processes and better defined channels mean **greater predictability**. Transparent rules on data accuracy, clear escalation procedures and reliable tools reduce uncertainty and facilitate day-to-day work. **For companies and entities** that choose a .it domain, **continuity of services and the robustness of the supply chain are elements of their digital presence**. **For citizens**, trust stems mainly from the **possibility of using stable services and responsible data management**.

In this regard, we would like the .it domain to be increasingly seen as a mark of

*The domain name remains a stable point of identity and recognisability in an increasingly algorithmic-mediated information environment*

quality and reliability. However, we must avoid absolute promises: no top-level domain alone can guarantee that every website is safe or that every content is reliable. **The value of .it derives from the way the Registro governs the infrastructure and registration data, the quality of the Registrars and the ability of the entire supply chain to prevent and address abuses.**

The pathway includes technological evolution of the infrastructure, the adoption and verification of recognised standards, the review of internal processes and the strengthening of data accuracy. These elements make the system more transparent and controllable. If applied strictly, NIS2 can therefore produce an advantage beyond compliance: a Registro better organised in its processes, more aware of its dependencies and better prepared to respond to change.



From left: **Rita Cucchiara**, Rector of the University of Modena and Reggio Emilia; **Andrea Lenzi**, President of CNR; and **Andrea Passarella**, during the celebration marking 40 years of the Internet in Italy

## 6 Security also depends on people and skills. How important is it to build a culture of digital security?

It is an essential requirement. Many incidents exploit ordinary behaviours: a mismanaged credential, a misleading message, a postponed update, an unreported anomaly. Technology can reduce risk but it does not replace people's attention and judgement. For this reason, **individual accountability is part of the security model of the Registro**: each person must know their role, the expected behaviours and the channels to be activated when a problem is detected. **Training must be continuous and linked to real activities. For the staff of the Registro .it means exercises, updates on threats and specific insights** for the different roles. **For Registrars and other operators in the supply chain it means**

**understanding new responsibilities, applying procedures correctly and developing a common prevention and response capacity.** A one-off training session is not enough, because technologies change, attacks change, and the ways in which people use digital services change. Then there is the broader issue of users. **Internet security improves if citizens and businesses know how to recognise risks and make informed choices. The Registro has been working on this for years, also through the Ludoteca of Registro .it, with initiatives aimed at young people** from the first school cycles. Bringing children and young people closer to digital citizenship means providing practical tools to protect identities, data and relationships online, without fuelling fear or mistrust of technology.

We are also consolidating a **strategic partnership with the Cybersecurity National Lab of the CINI** to contribute to **training programmes** that accompany the entire educational chain, **from primary to secondary school, also involving teachers**. It is a long-term investment. Technical skills are necessary, but a culture of security also requires critical thinking, the ability to assess sources and awareness of the consequences of one's own digital actions.

**7** Looking to the future, what is the most important challenge for the Internet system in the coming years, also in light of the rapid evolution of artificial intelligence?

The main challenge will be to integrate very rapid innovations without losing control, transparency and the ability to make choices. **Artificial intelligence is already changing the way we produce content, look for information and design services**. For those who build an online presence, traditional search engine rankings go hand in hand with the need to be correctly interpreted and cited by generative systems, a step often referred to as the transition from SEO to GEO. However, the domain name remains a stable point of identity and recognisability in an increasingly algorithmic-mediated information environment.

**Generative tools also reduce the time and cost of creating websites and content**. This can encourage a greater digital presence of professionals, businesses, associations and citizens, and can be reflected in demand for domain names. At the same time, it makes it

easier to produce misleading content, credible imitations and automated campaigns. **Quantitative growth must therefore be accompanied by means of verification, accurate registration data and a better ability of users to recognise risk signs**.

**Artificial intelligence will also change the management of the Registro**. It can help automate repetitive tasks, detect anomalies, correlate weak signals and support risk analysis. However, these tools must be introduced with clear criteria: data quality, human supervision, error measurement, information protection and the possibility of reconstructing decisions. **AI must strengthen people's abilities, not create opaque addictions or new vulnerabilities**.

**The placement of the Registro within the CNR-IIT represents a concrete advantage**. **The day-to-day dialogue with research enables advanced results to be evaluated in a timely manner and mature results to be transformed into solutions for infrastructure and services**. This applies to AI and, in the medium term, to quantum technologies. On this second issue, it will be important to prepare in time, adopting a cryptographic agility logic and evaluating the transition to solutions that are resistant to quantum attacks.

NIS2 also provides a useful way for us to address these transformations: understanding assets, assessing risks, assigning responsibilities, verifying measures and updating choices. Technologies will change; the ability to govern them, by collaborating with the supply chain and investing in skills, will remain the foundation of a reliable Internet.

# FROM DATA TO STRATEGY: UNDERSTANDING .IT TO ENVISION ITS FUTURE

by Chiara Spinelli

“**D**omain names have now become useless”. “With social media, nobody’s going to bother building a website anymore – it’s futile”. **In the debate on digital marketing, the demise of websites and domain names has been predicted time and again for years, yet websites continue to exist as well as thrive,**

**and individuals, professionals and businesses continue to register domain names to secure a distinctive and credible online presence of their own.** What was the most recent of these warnings? “You’ll see that artificial intelligence will replace search engines, and the website will become superfluous.” Yet the figures in this DOT report show that a drop in the number of domain names registered in Italy has not materialised, instead numbers have indeed risen steadily in the first few months of 2026.

**This does not mean that the market is immune to the AI revolution.** On the contrary, we know that it is changing rapidly: generative artificial intelligence is transforming the way we build websites and produce content, and above all, it is irreversibly changing the way people search for information – shifting from a generic query to a dynamic conversation; a transformation in which the quality of our online presence, thanks to our website, seems to have taken centre stage once again. Internet users seem to have become aware, even before the industry’s key players had, that in uncertain and turbulent times, **the website always provides a safe haven**



WMF 2026: presentation of the Registro .it survey on the perception of .it domains. From left: **Mirko Bruni**, CEO of “The Fool”; **Alessandra Scomparin**, Senior Market Consultant at “The Fool”; and **Chiara Spinelli**, Head of Communications at CNR-IIT and Registro .it

### for web browsing.

In such a rapidly changing landscape, however, we cannot rely solely on impressions, experience or recorded data, which show growth but do not disclose its underlying causes. That is why, as Registro .it, we decided to gain a better and more comprehensive understanding of the issue and to commission a survey on the perception of .it domain names in the Italian market.

The ultimate aim of the survey is to equip ourselves with an **increasingly data-driven strategy** to guide our communication decisions and tailor our messages: **to understand how the .it domain is perceived today, what values are attributed to it, who influences the choice to use it, and what factors might support – or hinder – its future development.** A knowledge base that is essential for interpreting the market in which we operate, anticipating trends and working with our Registrars to develop increasingly effective communication strategies to promote the .it domain.

But there is also a deeper reason: **the desire to listen in order to understand.** We want to listen **to those who manage and distribute domain names, those who support businesses and professionals in building their digital presence, and, finally, those who choose, purchase or encounter a .it address every day** – not by looking to the data for confirmation of what we already thought, but by putting our beliefs to the test.

### NOT A PHOTOGRAPH, BUT A REEL

The survey, commissioned to the company **TF – The Fool** following

*In a rapidly changing landscape, registration data alone is not enough to understand how the .it domain is perceived and what factors influence the choice to use it. That is why Registro .it has commissioned a survey on how it is perceived in the Italian market*

numerous expressions of interest from various industry players, convinced us first and foremost because it does not stop at providing a snapshot of the current market situation. **The research also examines what is changing and reshaping the digital ecosystem:** user behaviour, supply chain dynamics and the new forms of visibility generated by systems of artificial intelligence – in short, a constantly evolving landscape.

The project followed a step-by-step process structured around three actions (**listening, observing and validating**), with each stage paving the way for the next. **The qualitative interviews served to bring themes, tensions and hypotheses to the surface; the analysis of the digital context made it possible to compare these with what happens online; finally, the quantitative survey assessed the extent to which these perceptions are widespread amongst the general public, professionals and micro-enterprises.**

Another aspect that we, as Registro,

*The internal review highlighted the relationship between the actual value and the perceived value of the .it domain: a significant part of its assets remains largely invisible to the outside world*

were keen to explore was **how the .it domain is perceived by the various stakeholders involved**. Its ecosystem extends far beyond the scope of our day-to-day activities: it includes Registrars, who distribute domain names and have a direct relationship with the market; web agencies and digital professionals, who often influence business decisions; and, ultimately, all the organisations and individuals who build or use an online presence. Looking at the .it domain from these different perspectives also allows us to gauge the gap between the value we attribute to it, the value perceived by the supply chain, and the value that actually reaches the end user.

## START WITH US, BUT DON'T STOP WITH US

The work began with an **in-house workshop involving senior figures from Registro .it**, a useful exercise for identifying expectations, priorities and areas of awareness. **The issue that emerged from this discussion is the relationship between the domain's actual value and**

**its perceived value**. For us at Registro, the .it domain carries strong symbolic, technical and institutional significance, based on a number of strengths upon which we have built our institutional image and our communications over time: the guarantee of Italy's digital identity; a stronger legal point of reference in the event of disputes; and a reliable infrastructure, supported in part by our presence within the CNR, which ensures innovation and a rigorous focus on data security and quality. However, some of these assets may not be very visible to the outside world, or may be difficult to translate into benefits that are immediately apparent.

**The next stage of the analysis involved nine operators representing the Registrar sector, including members of the Registro's Steering Committee (CIR) and representatives of the trade associations AssoTLD and ASSODN.** The interviews explored market developments, the **relationship between .it and .com, the role of intermediaries, commercial strategies, the impact of NIS2 and expectations regarding Registro**. We are in constant contact with the Registrars, thanks in part to the work of the Registro Steering Committee (CIR), but The Fool's external perspective has enabled us to re-examine this dialogue from a different angle.

## OBSERVING THE DIGITAL CONTEXT

**The listening phase was followed by an analysis of the digital context**, comprising three complementary activities: **web and social media listening, SEO** (Search Engine Optimisation) **analysis and GEO** (Generative Engine Optimisation) **analysis**.



From left: **Mirko Bruni** and **Alessandra Scomparin** of “The Fool”, and **Chiara Spinelli** of CNR-IIT and Registro .it

Web and social media listening analysed public online conversations relating to .it, identifying the most recurring themes, the parties involved and whether the sentiment was positive or negative. The SEO analysis, on the other hand, identified the main questions users ask search engines: how to register a domain, how to choose a domain extension, what the differences are between .it and .com, how to check the availability of a domain name, and how to transfer a domain. Finally, the GEO analysis examined how the topic is addressed in users’ conversations with generative artificial intelligence systems. This final step has helped make the research truly forward-looking: if an increasing proportion of decisions are already being made today (and will increasingly be made in the future) through a conversation with an AI assistant, understanding which sources inform those responses becomes essential.

## USERS’ VIEWS

The final stage ultimately took the investigation beyond the specialist supply chain and towards the end users.

The qualitative part involved professionals, micro-business owners, web agencies and digital operators through interviews, focus groups and conversational tools. This was followed by a quantitative CAWI survey of 2,500 people: 2,000 interviews representative of the Italian adult population and 500 specifically for professionals and owners of micro-enterprises. The opinions gathered in the focus groups were obviously not regarded as automatically representative of the entire market, but they were useful in formulating hypotheses to be tested in the final, quantitative phase, in order to ascertain whether and to what extent they are widespread, and amongst which audiences.

*Web and social media listening, SEO and GEO enable us to observe how the .it domain is discussed in online conversations, searched for on search engines and represented in the responses of artificial intelligence*

*The challenge is to ensure that the national dimension is not perceived as a limitation and to promote the .it domain as an expression of an Italian identity also capable of competing on international markets*

## THE RESULTS? A STRONG ASSET, BUT ONE THAT IS NOT WIDELY KNOWN

The initial stages of the analysis provided us with a complex picture.

**The .it domain undoubtedly possesses a strong sense of identity that is associated with Italy**, proximity, familiarity and trust, with the meaning attributed to the domain being further expanded: it is not merely a technical address, but **the primary asset of a proprietary digital presence**.

Nowadays, particularly for industry professionals (web agencies), a domain name is not only the cornerstone of a website (the ideal place to host content and build relationships that do not depend entirely on the rules and algorithms of platforms), but also **a useful tool that is well worth recommending, for example, to establish a professional email address**. Having your own domain means safeguarding your name, presenting yourself in a more credible way and

maintaining **greater control over your online identity**: this is valuable not only for medium-sized and large companies, but also for professionals, freelancers, micro-businesses, start-ups and digital creators.

However, **the research also highlights a critical issue**: whilst the “Italian” nature of the .it domain is recognised, this does not always translate into a conscious reason for choosing it, whereas the .com domain retains an advantage in terms of aspiration (“if I choose it, I will be more highly regarded on the international market”), even amongst companies that operate predominantly in Italy. This therefore presents a significant challenge for Registro and the Registrars: to ensure that the “national” dimension is not interpreted as a limitation – in the sense of being “provincial” – and to promote the .it domain as an Italian root capable of supporting even the most ambitious projects. **In many market sectors – from tourism to food, and from fashion to high-quality craftsmanship – Italy is synonymous with excellence, history and prestige**: qualifying oneself as Italian can be an advantage even – and perhaps above all – on the international market.

Then there is the issue of security: the .it domain is often perceived as more reliable, but a domain extension alone cannot guarantee the reliability of every website that uses it. Security cannot, therefore, be presented as a vague promise, but must be translated into clear rules, checks, traceability, clearly defined responsibilities and the supply chain’s ability to take action against abuses.

## THE LAST PIECE OF THE JIGSAW: THE FINAL FIGURES

The final phase of the survey, which will focus on the views of the Italian public, professionals and micro-enterprises, will round off the process. This will be the decisive step in determining whether the values attributed to the .it domain by Registro and the Registrars are reflected in the market, to what extent they influence consumer choice, and which aspects remain internal to the supply

chain. Only once we have this data will we be able to transform the body of evidence gathered into practical guidelines for the positioning and communication of Registro .it, as well as for our relations with the various stakeholders in the ecosystem. Because a *data-driven* strategy is not simply about having a lot of data, but about being willing to listen to what the data tells us, even when it challenges what we thought we knew.

# THE LUDOTECA OF REGISTRO .IT, CYBERSECURITY AND DIGITAL EDUCATION: WITH ‘TRAIN THE TRAINER’, TRAINING STARTS WITH TEACHERS

A new project carried out in collaboration with CINI (the National Interuniversity Consortium for Informatics) Cybersecurity National Lab aims to provide teachers with the tools and skills to bring digital security into the classroom. ‘Train the Trainer’ involves an initial network of teachers in Tuscany in a 25-hour programme combining theory and practice, with the aim of developing a model that can be replicated nationwide

by **Giorgia Bassi**

**T**he Internet, digital platforms, social networks, video games and, in recent years, tools based on artificial intelligence have now become part of our everyday lives.

Familiarity with and proficiency in using technology, however, do not necessarily equate to the ability to use it in an informed, safe and responsible manner. This naturally applies to the so-called ‘digital natives’, as defined by Marc Prensky (‘Digital Natives, Digital Immigrants’) in 2001, but also to users who are more ‘mature’ in terms of age, those whom the American scholar refers to as ‘digital immigrants’. Prensky himself subsequently moves beyond this

dichotomy by introducing the concept of ‘digital wisdom’, understood as the ability to use technology in an informed way, to enhance one’s own abilities, solve problems and make better decisions.

Educating digitally aware and responsible citizens, who are not merely consumers of services but are able to navigate the online environment critically, is now a strategic objective for society as a whole and has always been one of the core missions of the Registro .it Ludoteca project.

From this perspective, **digital education** is not only about the ability to use tools and technologies to their full potential. It **also involves an understanding of the**

risks involved, the protection of one's own data and online identity, as well as the ability to recognise threats and adopt safe online behaviour.

Cybersecurity is therefore a key component of online education and digital citizenship training; for this reason, it is essential to set up training programmes aimed at the younger generation. Building on this understanding, in recent years the range of resources of the Ludoteca has been expanded to include materials, tools and play-based educational activities focused on safety, designed primarily for children aged 8-13.

It is against this backdrop that the new **"Train the Trainer" project was launched, in collaboration with CINI (National Interuniversity Consortium for Informatics) Cybersecurity National Lab**, which is working towards the full realisation of Italy's national cybersecurity ecosystem and which, for many years, has been supporting training and awareness-

*Fostering digitally aware and responsible citizens, who are not merely consumers of services but are able to navigate the online environment critically, has always been one of the core missions of the project of the Ludoteca of the Registro .it*

raising activities on cybersecurity issues in upper secondary schools and universities. The collaboration, which began last academic year with the design and creation of the board game 'Nel Mezzo dei Maghi' (Among the Wizards) (successfully tested by around 170



Video game "Nabbovaldo e il ricatto dal cyberspazio": a serious video game created by the Ludoteca of Registro .it to introduce young people to cybersecurity

*Cybersecurity is a key component of online education and digital citizenship training; for this reason, it is essential to set up training programmes aimed at very young people*

lower secondary school pupils), will therefore continue in the new 2026/27 academic year with 'Train the Trainer', an interdisciplinary training initiative aimed at teachers.

### TRAINING TEACHERS TO MAXIMISE THE IMPACT OF TRAINING

Schools are one of the best places to foster a culture of digital safety, as they enable us to reach large sections of the young population by addressing these issues during lessons on digital citizenship that are part of the curriculum.

For this to happen, however, it is not enough simply to provide schools with materials or to organise one-off workshops run by external experts: **it is important to involve teachers so that they can gain a proper understanding of cybersecurity topics and learn how to use the most appropriate tools**, integrating them into their lesson planning according to the needs of their classes. This is something that the Ludoteca has

always sought to achieve, through the publication of specific resources for teachers, such as guides to using apps, activity sheets, video tutorials and training sessions.

The 'Train the Trainer' programme was developed precisely to meet this need, with the aim of training a group of teachers from primary schools (years 4 and 5) and lower secondary schools, so that they can become independent in using all the tools and methodologies for cybersecurity education made available by the Ludoteca in their classrooms.

This **approach** therefore **focuses** not only on the immediate impact of the training, but also on **its replicability and sustainability** over time: the teacher who has undertaken the training is not regarded simply as a recipient of the programme but as an active participant in building a shared culture of digital safety and a teaching approach capable of incorporating it.

### A 25-HOUR COURSE COMBINING THEORY AND PRACTICE

**The project comprises a training programme totalling 25 hours**, divided into eight synchronous online sessions and one face-to-face workshop, with the aim of gradually guiding a group of teachers from an understanding of digital security issues to their practical application in the classroom.

**The training programme is co-designed by the Ludoteca of Registro .it and CINI**, drawing on each organisation's specific expertise: the Ludoteca is responsible for the educational aspects, while CINI, with the support of **Ilaria Matteucci**, a researcher at the Trust Security Privacy

Unit of the **CNR-IIT**, is responsible for the content relating to cybersecurity.

## FROM CYBERSECURITY TO GAME-BASED LEARNING: TOOLS FOR TEACHING

The section organised by the **Ludoteca** focuses on teaching methods for **digital education**, with a particular emphasis on game-based learning, that is, the design of game-based workshop activities. Teachers have the opportunity to discover all the main resources in the Ludoteca dedicated to cybersecurity, such as the **video game “Nabbovaldo and the blackmail from cyberspace”**, the board game **“Among the Wizards”** (developed in collaboration with CINI and IMT School of Lucca), card games such as **“Think first, then share”** and many other group games, including **“Caesar cipher”** and **“The password acronym”**. The training programme also includes the presentation and trialling of **lesson plans**, that is, lesson activity sheets tailored to different age groups, with the aim of providing **specific teaching resources that can be used and adapted to suit the needs of individual classes**. Part of the programme is also dedicated to the **“SuperCyberKids”** platform, developed as part of the European Erasmus+ project, in which the Ludoteca took part, and designed as a resource-rich tool for cybersecurity education aimed at teachers.

## CYBERSECURITY CONTENT: FROM THEORY TO PRACTICE

As regards **cybersecurity issues, which are covered by CINI**, the programme begins with some introductory topics,



Comic strips from the game “Cyberquiz”

such as how the Internet and networks work and secure communications, before moving on to digital hygiene practices and the protection of school data, the main attack vectors and AI-related threats, and finally incident management. **Each**

*“Train the Trainer” provides teachers with the tools and skills to address cybersecurity in the classroom, adapting the content to their students’ needs*

**module combines theoretical elements with practical activities**, with the aim of developing the ability to identify risks and to prevent and manage threats.

At the end of the theoretical section, there will be an **in-person workshop** (one for primary school teachers and one for lower secondary school teachers), during which participants can try out the tools and lesson plans presented in the theoretical section, simulating teaching activities with the **support of the Ludoteca staff**.

The programme concludes with a webinar for discussion and evaluation, during which participants can share their experiences, challenges and potential ways forward, with a view to gathering feedback to resolve issues and improve specific aspects.

### **AN INITIAL REGIONAL TRIAL**

The project is designed as an initial pilot scheme at regional level, involving only the region of Tuscany for this school year. The aim is to develop and validate, through structured support for the schools involved and the collection of data and feedback, a replicable intervention model capable of adapting to different school contexts and of being

*The project starts in Tuscany with the aim of developing and validating a training model that can be replicated in other school settings and, in the longer term, at national level*

progressively rolled out nationwide, while identifying the most effective conditions for its wider implementation.

The project could also help to create a community of trained teachers who are able to share experiences, adapt activities to their own contexts and gradually become multipliers of skills within their own schools.

The **'Train the Trainer' project will be presented during "Cybersecurity Day" as part of the Internet Festival 2026**, in a session dedicated to training and educational initiatives.

# NIS2: CERTIFICATION, HARMONISATION AND 'REPORT ONCE' ON THE AGENDA OF THE EUROPEAN PARLIAMENT

The European Parliament is examining the targeted revision of NIS2: among the amendments under consideration are the role of 'cyber posture' certification, the harmonisation of technical requirements and the 'report once' principle. An ongoing debate of particular relevance to top-level domain registries (TLD registries) and other Internet infrastructure operators

by Gino Silvatici

**T**he process of targeted revision of the NIS2 Directive is entering a new phase. The European Parliament's **Committee on the Internal Market and Consumer Protection (IMCO)** published on 1 July **a series of amendments relating to the proposal through which the European Commission intends to modify certain aspects of the directive**, primarily with the aim of simplifying its application, in line with the new European framework on cybersecurity certification. It should be noted that **the amendments in question do not yet represent the European Parliament's position**: the committee responsible for examining this dossier is the Committee on Industry, Research and Energy (ITRE), while IMCO is issuing an opinion which ITRE may take into account when finalising the Parliament's negotiating position.

The dossier, identified as legislative procedure 2026/0012(COD), is still at the parliamentary scrutiny stage.

The proposals put forward in the IMCO Committee are nevertheless interesting because they show that a number of key issues remain unresolved within Parliament: to what extent use **the 'cyber posture' certification** (i.e. the organisation's overall level of computer security), **how much leeway to allow Member States to introduce national requirements** in addition to those defined at European level, and **how to reduce the proliferation of incident reporting obligations**.

These issues are also particularly relevant to organisations involved in the Internet infrastructure, including Top Level Domain (TLD) registries.

*In January 2026, the European Commission presented a proposal to amend the NIS2 directive with the aim of reducing compliance burdens, increasing legal certainty and ensuring a more uniform application of the rules across the internal market*

In January 2026, the European Commission presented a proposal to amend the NIS2 directive as part of a wider package of revisions to European cybersecurity legislation. The stated aim is not to rewrite the directive, which came into force in October 2024, but to make changes to certain aspects in order to reduce compliance burdens, increase legal certainty and ensure a more uniform application of the rules within the internal market. **The proposed measures include changes to the definition of entities falling within the scope of NIS2:** new provisions for companies operating in several Member States, a greater role for ENISA (the European Network and Information Security Agency) in coordinating cross-border supervision, and greater use of European certification as a means of demonstrating compliance with risk management measures. The proposal confirms that ccTLDs will continue to be treated differently: **top-level domain registries would continue**

**to be regarded as essential entities,** regardless of their size.

However, **one of the key issues** in the dossier remains **the relationship between European harmonisation and national requirements**. For this reason, one of the most hotly debated issues in the IMCO amendments concerns the certification of what is known as ‘cyber posture’. **The IMCO Committee’s original proposal adds** to Article 24 of NIS2 **the possibility** for Member States to require essential and important entities **to obtain a certificate regarding their ‘cyber posture’** under a European certification scheme. Where the certificate demonstrates compliance with certain NIS2 requirements, the competent authorities should also take this into account in their supervisory activities, avoiding duplication of checks on aspects already covered by the certification. The idea ties in with the proposed **‘Cybersecurity Act 2’**, which expands the European certification framework to allow not only the certification of ICT products, services and processes, but also the ‘cyber posture’ of organisations. The IMCO Committee regards this possibility as an effective tool for assisting, in particular, businesses that operate in several countries and have to deal with different authorities and supervisory procedures.

**One of the amendments** tabled in the IMCO Committee would move **towards a more binding model, requiring certification for entities subject to NIS2 that provide services in more than one Member State**. In this way, a single European certificate could become a sort of ‘cybersecurity passport’ for

organisations operating across borders.

Other amendments, however, take the opposite approach: **Member States could encourage, but not require, essential and important entities** to obtain **certification of their 'cyber posture'**. The difference is not insignificant: in the first case, certification could become a structural component of NIS2 compliance for certain categories of operators, while in the second case it would remain primarily a voluntary tool through which an organisation can more easily demonstrate its compliance. At present, however, these are merely options for negotiation: **IMCO has not yet adopted a definitive position.**

For TLD registries, the debate over the extent to which technical requirements should be harmonised is probably even more significant. NIS2 provides, in fact, that the European Commission shall lay down – by means of implementing acts – the technical and methodological requirements relating to risk management measures for certain categories of digital operators. These specifically include DNS Service Providers and TLD registries, alongside, amongst others, cloud providers, data centres, content delivery networks and managed service providers. This provision led to the adoption of Implementing Regulation (EU) 2024/2690, which lays down common technical and methodological requirements for these categories of entities.

The European Commission's 2026 proposal aims to go one step further: where a European implementing act has been adopted pursuant to Article 21(5), **Member States should not be able to impose further technical,**

*As regards TLD registries, perhaps even more important is the debate on the extent to which technical and methodological requirements relating to risk management measures for certain categories of digital operators should be harmonised*

**methodological or sector-specific requirements on the entities concerned in relation to those same measures.**

**The rationale is one of maximum harmonisation.** If an operator is already subject to technical requirements defined uniformly at EU level, the introduction of different or more stringent obligations in individual countries risks recreating the regulatory fragmentation that the EU legislation is intended to eliminate.

**For a sector as inherently cross-border as that of domain name infrastructure, this principle may be of particular relevance.** Different national rules could, in fact, result in higher compliance costs and inconsistent interpretations of the NIS2 framework itself. However, several IMCO amendments call for this restriction to be removed or relaxed, thereby allowing Member States greater scope to introduce additional national requirements even where a European implementing act is already in place. This debate reflects two requirements that are not easily reconciled: on the one hand,



the desire to **establish uniform rules within the single market**; on the other, the need to **allow Member States to adopt higher levels of protection** where their national circumstances or specific threats so require.

Another element featured in several amendments is the **'report once'** principle, which **aims to reduce duplication in incident reporting** and forms part of a wider European effort to streamline reporting obligations. Today, a single cyber incident can simultaneously trigger reporting obligations under several European regulations, each directed at different authorities: NIS2, the GDPR,

DORA, the 'Cyber Resilience Act', eIDAS and legislation on the resilience of critical entities may, in certain circumstances, overlap. The model towards which the EU is moving is that of 'report once, share many', with the aim of enabling the entity concerned to submit information just once, via a single point of entry, and subsequently allowing the competent authorities to share the necessary information in accordance with their respective remit. **The European Commission had already proposed – as part of the Digital Omnibus – the creation of a 'single entry point' within ENISA for this type of notification.**

**As regards European ccTLDs, this**

**dossier is particularly worthy of attention because of the potential final balance between harmonisation and national autonomy.** On the one hand, a uniform European framework for technical requirements can facilitate compliance and reduce the risk that operators carrying out similar activities will be subject to different requirements in different Member States. This aspect is particularly significant for TLD registries, which are already subject to Implementing Regulation 2024/2690. On the other hand, if the approach advocated by certain IMCO amendments were to prevail in the final text, Member States would retain greater scope to introduce additional requirements. For operators, this could mean a greater need to monitor not only European legislation, but also its subsequent national implementations.

The future of certification will also need to be monitored closely. A European **certification scheme capable of attesting to compliance with NIS2 measures** could be a **useful tool for streamlining audits and supervision**; however, making such certification a mandatory requirement would entail new costs and compliance obligations, which would need to be assessed in terms of proportionality.

**The legislative process is still ongoing.** IMCO examined the compromises on the amendments by 28 September, while the vote on its opinion is scheduled for 15

*The model towards which the EU is moving is that of 'report once, share many', with the aim of enabling the entity concerned to submit information just once by using a single point of entry*

October 2026. It will then be primarily ITRE, as the committee responsible, that will define the Parliament's position to be taken into the subsequent legislative negotiations. **As far as the domain name sector is concerned, therefore, there are no immediate new obligations on the horizon at present.** However, the ongoing debate is important because it will help to determine how consistent the application of NIS2 will be across Europe in the future, what role the 'cyber posture' certification might play, and to what extent it will be possible to avoid duplication in both technical requirements and reporting obligations. Three aspects which, for essential digital infrastructure such as TLD registries, may have far more significant operational consequences than a review formally described as 'targeted' might initially suggest.

05

Preview  
Statistics  
News  
Insights  
Events

# INTERNATIONAL EVENTS FROM THE INTERNET WORLD



6 OCTOBER

\* **CENTR Leaders Day 2026** |  
Bruxelles (Belgium)



7 OCTOBER

\* **CENTR General Assembly (GA 76)** |  
Bruxelles (Belgium)



8 OCTOBER

**TLD ISAC Conference 2026** |  
Bruxelles (Belgium)



13-14 OCTOBER

\* **30th CENTR R&D** |  
Riga (Latvia)



17 – 22 OCTOBER

**ICANN 87 - 28th Annual General Meeting** |  
Bali (Indonesia)



26- 30 OCTOBER

**RIPE 93** | Sofia (Bulgaria)



3-4 NOVEMBER

**SMAU** | Milan

*The Registry  
is here with  
a dedicated  
stand!*



14-20 NOVEMBER

**IETF 127** |  
San Francisco (USA)



25 NOVEMBER

\* **14th CENTR Academy** |  
Online

\* Events reserved for CENTR members



è gestito da

