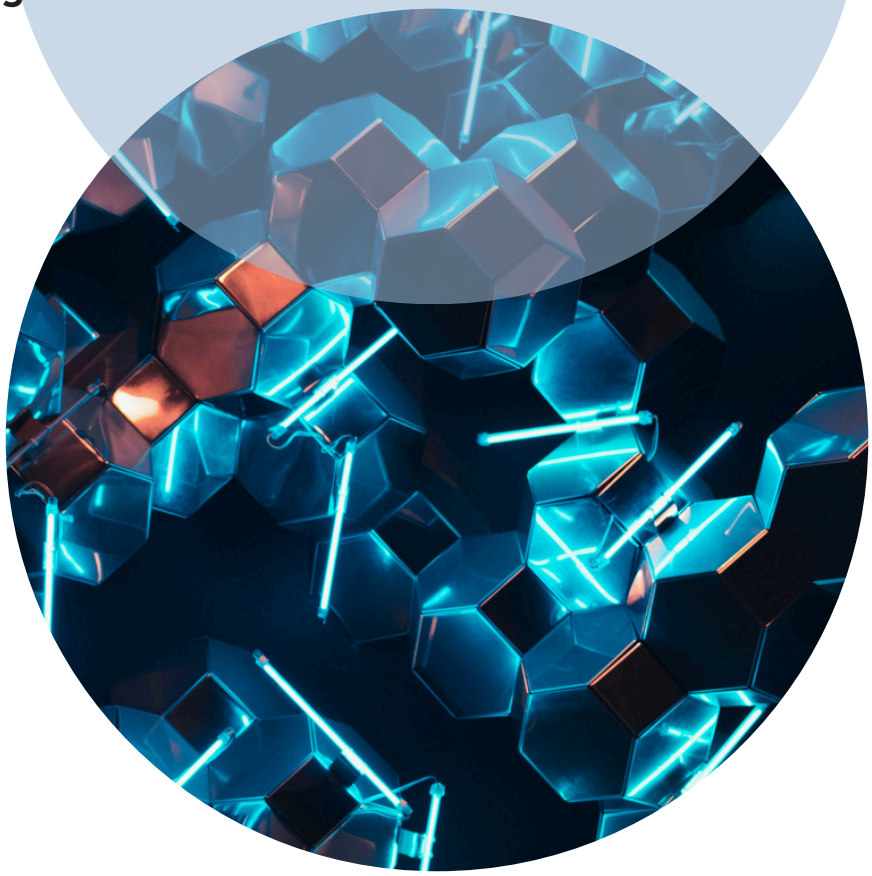
Abreu advogados

Implementing Regulation of the Cybersecurity Legal Framework

info@abreuadvogados.com
abreuadvogados.com



On June 22, 2026, Regulation No. 756/2026 was published, implementing the Cybersecurity Legal Framework ("RJC"), approved by Decree-Law No. 125/2025, of December 4, establishing essential operational rules for essential entities, important entities, and relevant public entities.

The Regulation defines, among other matters, the operation of the new electronic platform of the National Cybersecurity Center ("CNCS"), the procedures for self-identification and classification of covered entities, the rules for reporting cybersecurity incidents, and the structural instruments that will serve as a reference for the implementation of the obligations set forth in the RJC.

A) MyCiber Platform and Qualification of Entities

One of the main new features of the Regulation is the launch of the CNCS's electronic platform, already available with a simulation feature – MyCiber - which will now serve as the primary channel for interaction between covered entities and the competent cybersecurity authority. The platform will ensure, in particular:

- Self-identification of covered entities;
- The procedure for classifying entities as essential, important, or relevant public entities;
- The designation of the Cybersecurity Officer and the Permanent Point of Contact;
- The submission of mandatory and voluntary notifications;
- Receipt of electronic notifications from the CNCS;
- The submission of reports and other information required under supervisory powers.

Self-Identification and Classification Procedure

The process begins by completing an electronic form on the MyCiber platform, which will result in provisional registration. Following review by the CNCS, the entity's qualification procedure will be initiated.

Following the public consultation process, the right to a prior hearing for the entities in question was established. This right is exercised upon notification by the CNCS, and the entities have 10 business days to comment on the draft decision. Once this period has elapsed, the CNCS will issue the final qualification decision, which will include, where applicable:

- The entity's category;
- The applicable compliance level;
- The mandatory cybersecurity measures to be implemented.

Following qualification, the provisional registration becomes definitive, and the entity becomes subject to the ongoing obligations set forth in the RJC and the Regulation.

B) Cybersecurity Officer and Permanent Point of Contact

The Regulation also specifies the requirements regarding the designation and notification of the Cybersecurity Officer and the Permanent Point of Contact, which must be reported through the restricted area of the MyCiber platform.

C) Incident Reporting

The Platform will also serve as the central hub for submitting mandatory notifications of incidents with a significant impact.

Covered entities must submit:

- Initial notification;
- Notification of the end of the significant impact;
- Final or interim report.

The platform will allow users to track the status of notifications, link different reports related to the same incident, and receive automatic alerts regarding legal reporting deadlines.

The Regulation also provides for the possibility of submitting voluntary notifications regarding incidents, cyber threats, vulnerabilities, or near-incidents, even by entities or individuals not registered on the platform.

According to the final text of the Regulation, information regarding the occurrence of significant incidents will be published on the Platform.

D) Structural Instruments

The Regulation establishes a set of key instruments for implementing the new cybersecurity regulatory framework.

i. National Cybersecurity Reference Framework (QNRCS)

The QNRCS now serves as the national reference framework for identifying norms, standards, and best practices in the areas of cybersecurity and information security management.

ii. Risk Matrix

The Risk Matrix establishes the risk scenarios applicable to different sectors and subsectors of activity and determines the respective compliance levels:

- Basic;
- Substantial;
- High.

The classification obtained will directly influence the cybersecurity obligations applicable to each entity.

iii. Minimum Cybersecurity Measures

Annexes III and IV establish the sets of minimum cybersecurity measures applicable to:

- To essential and important entities;
- To relevant public entities.

These measures now constitute the mandatory minimum standard for compliance with the RJC.

Next Steps

The Regulation's entry into force on June 23 marks the start of the operational phase of the new Cybersecurity Legal Framework.

Entities potentially covered by the Regulation should, effective immediately:

- Assess whether they fall within the scope of the RJC;
- Prepare their self-identification on the MyCiber platform;
- Review their cybersecurity governance mechanisms;
- Appoint a Cybersecurity Officer and a Permanent Point of Contact;
- Assess their level of compliance and the applicable cybersecurity measures;
- Prepare internal incident management and reporting procedures.

The timely implementation of these measures will be crucial to ensuring compliance with the new regulatory obligations and reducing the risk of supervisory action and administrative liability.

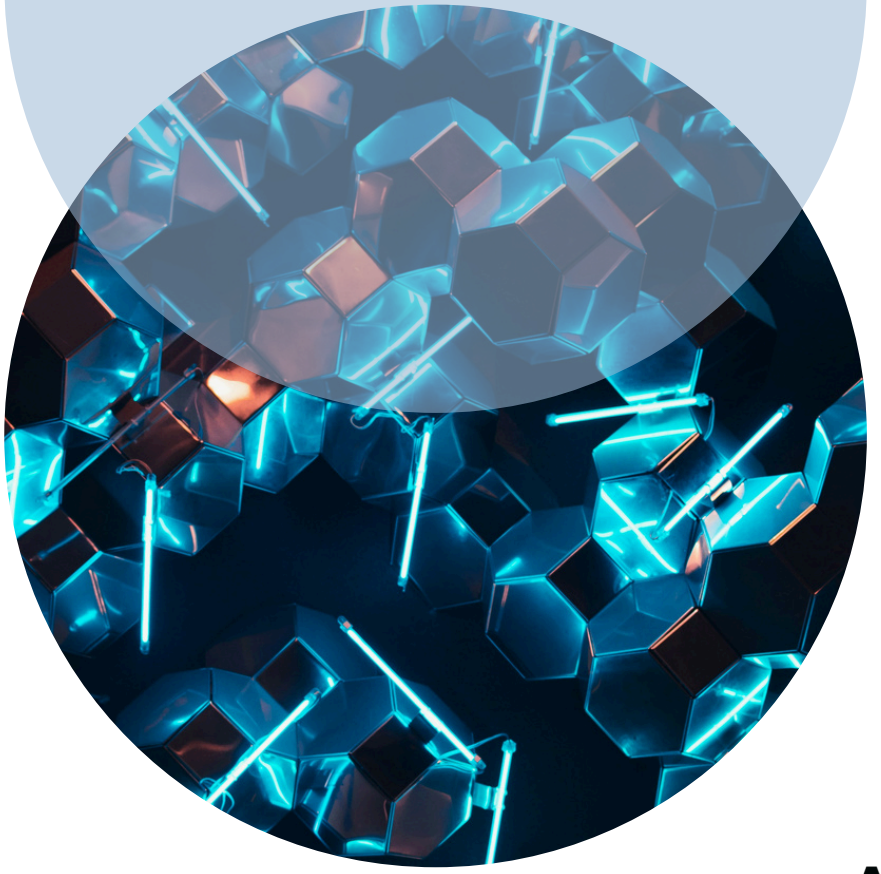
For more information, please contact our Data Protection and Cybersecurity Service.

Thinking about tomorrow? Let's talk today.

Ricardo Henriques
ricardo.henriques@abreuadvogados.com

Catarina Mascarenhas
catarina.mascarenhas@abreuadvogados.com

Marta Boura
marta.boura@abreuadvogados.com



info@abreuadvogados.com
abreuadvogados.com

Abreu advogados