INFORMATIVE NOTE

PLMJ ADVOGADOS, SP, RL

50 YEARS By your side.

TELECOMMUNICATIONS, MEDIA AND TECHNOLOGY

CYBERSECURITY LEGISLATION

The RJSC establishes the structure for cybersecurity security and requires compliance with security requirements and notification of incidents to the National Cybersecurity Centre, whenever there is an incident having a relevant or substantial impact on networks and information systems.

Law 46/2018 of 13 August 13 has now been published. This law approves the **Legal Framework of Cybersecurity** (Regime Jurídico da Segurança do Ciberespaço, referred to here by its Portuguese initials, "RJSC"), implementing Directive (EU) 2016/1148, of the European Parliament and of the Council of 6 July 2016, on measures to ensure a high common level of network and information security across the Union.

The RJSC establishes the structure for cybersecurity security and requires compliance with **security requirements** and **notification of incidents** to the National Cybersecurity Centre, whenever there is an incident having a relevant or substantial impact on networks and information systems.

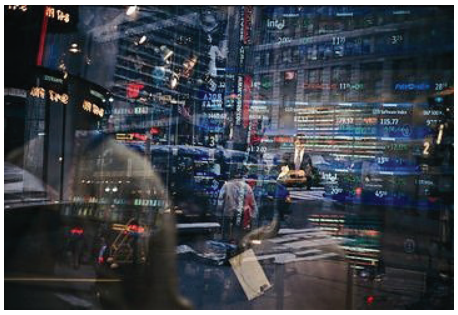
The RJSC applies to:

- The Public Administration
- Critical infrastructure operators
- Essential services operators
- Digital service providers whose registered office is located in Portugal, and provide (i) online market services, (ii) online search engine services and (iii) cloud-computing services;
- Any other entities that use information networks and systems.

This RJSC requires these entities to comply with **security requirements** that entail compliance with appropriate, proportionate technical and organisational measures, and management of the risks inherent to the security of the networks and information systems they use.

With regard to digital service providers, in order to provide a security level appropriate to the risk inherent in the security of the information networks and systems they use within the context of the provision of digital services, the RJSC requires that the following factors be considered: (i) security of the systems and facilities, (ii) processing of incidents, (iii) business continuity management, (iv) monitoring and auditing of the tests conducted, and (v) compliance with international standards.

This RJSC requires these entities to comply with security requirements that entail compliance with appropriate, proportionate technical and organisational measures, and management of the risks inherent to the security of the networks and information systems they use.



FUNDAÇÃO PLMJ

ANDRÉ PRÍNCIPE
S/ Título da série Tunnels, 2005
Prova de branqueamento de corante
66 x 100 cm
From the Collection of the PLMJ Foundation

With regard to the obligation of **notification of incidents** to the National Cybersecurity Centre, digital service providers must notify an incident only when faced with an incident having «substantial impact» and to the extent to which they have access to the information needed to assess the impact of the accident on the basis of the factors listed above. In relation to other entities covered by the RJSC, in order to determine the relevance of the impact of the incident, the number of users affected, the duration of the incident and the geographical distribution are taken into account. Over and above the parameters listed above, digital service providers are also required to assess the seriousness of the disruption of the operation of the service, and the extent of the impact on economic and corporate activities.

It is also possible for any entity to report an incident voluntarily if the incident in question has a major impact on the continuity of the services provided.

In order to comply with the provisions of the RJSC, **digital service providers and digital infrastructure sector entities (traffic exchange points, domain name systems (DNS) providers and group domain-name registers) must immediately report the activity they carry on to the National Cybersecurity Centre**. This obligation does not apply to essential services operators, to the extent that identification of these entities is reserved to the National Cybersecurity Centre (a process that is scheduled for conclusion on 9 November 2018). Breach of the obligation to report constitutes a serious infringement punishable with fine of up to €9000 in the case of companies and other legal entities.

Security requirements applicable to the Public Administration, critical infrastructure operators and essential service providers, as well as the reporting requirements, will be further developed in complementary legislation to be enacted within 150 days of the entry into force of the RJSC.

Although the obligation to implement technical and organisational security and incident-reporting measures only becomes mandatory 6 (six) months after the publication of the RJSC, that is, as from 13 February 2019, companies should now begin to plan and create the necessary in-house mechanisms allowing them to meet the new legal requirements.

An administrative offence framework is established, and supervision and enforcement are the responsibility of the National Cybersecurity Centre. The maximum fines amount to €50,000 in the case of the case of companies or other legal entities.

Lastly, the following are excluded from the scope of application of the RJSC: (i) micro and small enterprises, (ii) undertakings providing public-communications networks or publicly available electronic communications services, (iii) trust service providers (iv) information networks and systems directly related to the command and control of the General Staff of the Armed Forces, and (v) networks and information systems that process classified information.

Although the obligation to implement technical and organisational security and incident-reporting measures only becomes mandatory 6 (six) months after the publication of the RJSC, companies should now begin to plan and create the necessary in-house mechanisms allowing them to meet the new legal requirements.