

# Information Security Policy in Supplier Management

Madrileña Red de Gas, hereinafter MRG, hires suppliers and contractors to carry out various services and activities; both operational, development or maintenance, etc. and that they contribute their technical capabilities and specialized knowledge for adequate performance towards the client and society in general.

## Principles:

- Due diligence in the processing of information during the development of activities, and especially in relation to clients; and taking as reference the requirements related to the protection of personal data and cybersecurity.
- Equal opportunities and non-discrimination of suppliers/contractors.
- Transparency, objectivity and protection of information in purchasing and contracting processes.
- Communication and feedback between MRG with its suppliers/contractors on the performance of contractual compliance, including the requirements described in the clauses related to personal data protection and cybersecurity.
- Supervision, review, evaluation and monitoring of suppliers.
- Loyalty, trust and mutual respect in the bilateral relationship and with the market.

## Commitments:

- Comply with the Code of Ethics and MRG's internal rules defined in the integrated management system, including the areas of data protection and information security.
- Comply with the provisions of the internal regulations that regulate the relationship with suppliers / contractors; and especially, in relation to punctuality and accuracy in the delivery of the documents required for the purchase of goods and provision of services.
- Communicate to MRG any incident that occurs in the information systems. Improve the capacity for prevention, detection, reaction, analysis, recovery, response, investigation and coordination against incidents and activities that affect cybersecurity.
- Use information systems following MRG guidelines, as well as destroy or return assets owned by MRG upon completion of the contract.
- Implement the necessary security and resilience measures to protect the confidentiality, integrity and availability of information, as well as operating systems based on their criticality, existing risks and new threats, following a risk-based approach. that considers changes in the technological environment.
- To allow the performance of Security reviews and/or audits for the investigation of incidents and the maintenance of MRG certifications.

In Pozuelo de Alarcón, November 3<sup>th</sup>, 2023

Alejandro Lafarga Ibran  
General Director