CYBERSECURITY IN DATA COMMUNICATIONS AND RELATIONS WITH MIBGAS SYSTEMS

The activity carried out by MIBGAS as Market Operator and Guarantees Manager contains a high degree of technological communications and the use of electronic means for the proper performance of its work. Exposure to this technological environment implies obvious connectivity advantages for users, but also exposure to the threats derived from the use of information technologies.

The MIBGAS group relies on OMIE, as a service provider in technological systems and cybersecurity, which has developed the market platform and offers technological support for the management of these services. MIBGAS makes these means available to agents and users for their access and participation in the markets it operates.

The use of these systems implies the observation and absolute compliance with the established rules on cybersecurity included in this release, as well as the measures and procedures mentioned below, and requires the use of the best practices contained in the applicable national and European regulations. Compliance with these policies and best practices is mandatory for users and is a necessary condition for access and participation in MIBGAS platforms. Failure to comply with them therefore entails the indemnity of MIBGAS with respect to damages that may arise from the actions of users who fail to observe these precautions.

Below, we indicate the procedures and protocols established by OMIE, which are applicable in the access and use of the gas market platforms, to act in a preventive manner, to ensure the best operation of the system and a guide for action in case of possible fraudulent actions, in section 3 of this document.

It is an obligation of the agents to take all reasonable and appropriate professional due diligence precautions to protect their IT infrastructure and to prevent fraudulent or unauthorized use or access to market data and platforms.

Link to Instruction 3/2021 on Cybersecurity in Data Communications and Relations with OMIE

MIBGAS platforms and IT communications with MIBGAS

OMIE has established cybersecurity measures of a technical, procedural, and organizational nature that guarantee the correct and secure operation of its information systems and market platforms. Compliance with these measures is mandatory for all agents and users accessing MIBGAS systems.

Access to the market platforms used by the agents (www.market.mibgas.es) is done through a secure connection, requiring the use of personal digital certificates that guarantee the user's identity, preventing access if the user does not have an authorized certificate. The digital certificate is also used for the signature of the operations carried out by the agent in the Market Platform and allows the traceability of such operations. The actions performed by the agents in their relationship with the market must exclusively be carried out through said platforms and through the appropriate use of personal certificates. All confidential information supplied by agents or required for their actions in the market is accessible exclusively through the Market Platform (www.market.mibgas.es) using MIBGAS digital certificates.

In case of modification of the content of the information, OMIE shall replace the information accessible through the website, and may notify the agents of the modification, indicating that they should access the website again to obtain the new values, but never sending the modified values via e-mail. Neither MIBGAS nor OMIE provides sensitive information (orders data, market results, energy delivery invoices or credit or debit notes) via e-mail.

In the event that the agent receives e-mails, which may apparently have been sent by MIBGAS or OMIE, in which atypical, unusual, exceptional or emergency actions are required to be performed, the agent shall properly review the message and, if it has any suspicion as to its authenticity, it must immediately contact MIBGAS or OMIE by the means set forth in section 3 of this notice, to confirm the authenticity thereof.

Obligations of agents

Agents and users are responsible for the management and protection of their own information systems and must employ the measures they deem necessary in their activity with adequate professional diligence to protect their IT infrastructure and prevent fraudulent or unauthorized use or access to data and market platforms.

They must also contact MIBGAS immediately if they have reason to suspect that there has been improper access to their IT infrastructure that may have compromised the information exchanged with the market, the broker's IT equipment that communicates with the market, the digital certificates of access to the market, or that confidential or security data of access to market platforms has been improperly disclosed.

In case of doubt regarding information apparently received from MIBGAS or OMIE, the agent must always refer to the information published on the Market Platform, or if necessary, proceed to confirm the authenticity of such information by calling the MIBGAS or OMIE contact telephone numbers, which are listed on the market platform and in the Annex to this notice.

In relation to the digital certificates issued by MIBGAS for the agents' access to the market website, the agent is obliged to keep custody and maintain them, and must revoke and request the issuance of new digital certificates in case of loss of the certificate, in case of doubt that unauthorized external access is being made with any of the agent's certificates or in case of suspicion that they may have been improperly accessed.

Regarding the access infrastructure and digital communications with MIBGAS, the agent must have established mechanisms and procedures for cybersecurity and monitoring of the use and exchange of sensitive information, taking into account the best practices in cybersecurity, which guarantee that the aforementioned processes are carried out in a secure manner. Agents must guarantee at all times that their IT infrastructures do not cause any impact on the correct operation of the market platforms, as well as collaborate with MIBGAS and OMIE to manage and solve these situations.

Response to an internal cybersecurity incident at an agent's premises

In the event that a market agent detects any internal cybersecurity incident that may put at risk the information exchanged with MIBGAS, the agent's IT equipment that communicates with the market, or the digital certificates for access to the trading platforms, apart from the internal processes it has in place for handling cybersecurity incidents, the agent must cooperate with MIBGAS and OMIE throughout the incident management process.

As soon as the incident is detected, the agent shall immediately notify MIBGAS and OMIE through the official means of communication established, as indicated in the "Contact Information" accessible at www.market.mibgas.es, described in the Annex. MIBGAS has an email dedicated to these matters: notificacion_incidentes_ciberseguridad@mibgas.es.

The notification must contain details of the incident in those relevant aspects that may affect the market. Particularly in everything related to the agent's equipment that communicates with the market or in which market information is stored, with special reference to the digital access certificates.

The agent is obliged to provide the additional relevant information that may be required by MIBGAS or OMIE in relation to the incident and the possible actions in the agent's infrastructure related to the market, so that, in a coordinated manner, progress is made in the establishment of the necessary measures until the complete resolution of the incident, or, until the absence of any risk to the market is completely assured, at which time MIBGAS or OMIE must be informed again, providing the information associated with the total or partial closure of the incident. The agent must communicate the relevant information associated with the detection, containment, and mitigation and, finally, recovery of the incident.

During this process, in case of risk to the market, MIBGAS or OMIE may at any time interrupt the agent's access or require actions such as revocation of certificates, renewal or modification of encryption keys or similar elements used by the agent in order to protect the correct functioning of the market.

In order for the whole incident management process to be carried out in an appropriate manner and for communication between MIBGAS or OMIE and the agent to be agile and effective, the agent is obliged to keep updated, on the Market Platform, the details of the contact persons designated by the agent for interlocution with MIBGAS or OMIE, accessible from www.market.mibgas.es.

> Registration and Consultation Platform -> Participant Data -> Modification of reference data -> Contact persons

ANNEX

Contact Information

ADDRESS

MIBGAS

Alfonso XI, 6. Madrid 28014 – España
T +34 916 598 900 F +34 915 240 806

24h Service every day

Market Operation

T +34 916 598 960
T +34 916 598 967
trading@mibgas.es

Attention during office hours

ISSUES RELATED TO:

Agents Access Procedures, Maintenance of Agents Data, Information Systems, etc.

agentes@mibgas.es

Invoicing, Collection and Payments, and Guarantees, RSL

liquidaciones@mibgas.es

Reporting Service(REMIT)

remit@mibgas.es

Cibersecurity incidents notifications

notificacion_incidentes_ciberseguridad@mibgas.es