

Incident Summary and Response Statement

April 13, 2026

To: SISTEMAS Y SERVICIOS DE COMUNICACIÓN, S.A. DE C.V.

Subject: Cybersecurity Incident

Incident

The event was a cybersecurity-related incident involving targeted activity affecting part of our environment.

Preventive Measures during the Incident

As part of our immediate response and containment measures, we isolated affected systems and temporarily suspended portions of the platform to protect overall system integrity and limit potential impact.

We do have multiple redundancy mechanisms in place. However, in this case, the security measures applied during containment impacted the normal behavior and speed of failover processes. The temporary service disruption was therefore primarily a result of controlled actions taken to secure the platform, rather than a failure of redundancy as such.

Following the incident, we have already implemented additional security controls, including an extra security layer, enhanced monitoring, and improvements to detection and response mechanisms.

We are also working on further platform segmentation to allow more targeted isolation in similar scenarios, while optimizing fallback to secondary systems.

General Incident Timeline

The event was detected on April 2nd at approximately 09:00 pm EST, followed by immediate internal escalation and containment actions.

Throughout April 3, remediation activities were carried out, and a controlled restoration of services was initiated, prioritizing event reporting.

Events reporting was gradually restored on April 3rd, around and after 5:00 pm EST.

Full restoration of web and application services was completed on April 4 at approximately 11:30 am EST.

Controls & Improvements

We currently operate a range of controls across detection, response, access management, logging, redundancy, and backup.

As part of the post-incident actions, we are enhancing these further, including:

- Strengthened monitoring and alerting capabilities
- Additional security control layers
- Improved segmentation of platform components
- Optimization of failover and fallback procedures
- Review and improvement of communication and escalation processes
-

We understand the importance of transparency and the need for clear information in managing your stakeholders and market confidence.

We remain fully committed to strengthening our platform resilience, improving response capabilities, and ensuring the reliability and security of the services we provide.

RESIDENCE CONTROL EOOD DBA M2M SERVICES