MNEMO

NEGOCIO
CIBERSEGURIDAD
CONECTIVIDAD

RFC 2350
MNEMO-CERT

Date: 28/02/2024, Version 1.0

CHANGE CONTROL

Version	Description	Elaborated by	Approved by	Date
1.0	Establishment of main team in Spain	Mariano Lázaro Jusdado	Mariano Lázaro Jusdado	28/02/2024

1. DOCUMENT INFORMATION

This document contains a description of the **MNEMO-CERT**, according to the model recommended in the IETF RFC 2350, which provides basic information about the CERT of MNEMO Evolution & Integration Services S.A., the ways in which it can be contacted, description of the responsibilities and services offered.

1.1.1 DATE OF LAST UPDATE

1.0 version, published on 28 february 2024, as reflected in the **Change control** section of this document.

1.2.1 DISTRIBUTION LIST FOR NOTIFICATIONS

Currently, **MNEMO-CERT** has a distribution list for notifications of security bulletins, in case you are interested, please contact us by email at info.cert@mnemo.com

1.3.1 LOCATIONS WHERE THIS DOCUMENT CAN BE FOUND

The current version of this **MNEMO-CERT** description document is available from the MNEMO website: https://cert.mnemo.com/rfc-2350/.

1.4.1 AUTHENTICATION OF THIS DOCUMENT

This document has been signed with the PGP key of **MNEMO-CERT**. The image of the signature is shown in section 2.8 of this document.

2. CONTACT INFORMATION

2.1.1 TEAM NAME

Mnemo Evolution & Integration Services CERT (**MNEMO-CERT**)

2.2.1 ADDRESSES

Spain
C/ *Cardenal Marcelo Spínola 14, 5ª planta,*
28016 Madrid, Spain

Colombia
Calle 100 #8 A-37 Of. 704
WTC Torre A Bogotá, Colombia.

2.3.1 TIME ZONE

MNEMO-CERT operates mainly in Spanish Standard Time, GMT +01:00.

2.4.1 TELEPHONE NUMBERS

Spain: +34 (91) 417 67 76
Colombia: +57 (601) 552 72 10

2.5.1 FAX NUMBER

Fax number not available.

2.6.1 E-MAILS

For general purposes, the preferred method of contact is through: info.cert@mnemo.com.
To report a security incident, it is preferable to do so through: cert@mnemo.com.

2.7.1 OTHER TELECOMMUNICATIONS SERVICES

Not available.

2.8.1 PUBLIC KEYS AND ENCRYPTION INFORMATION

MNEMO-CERT uses a PGP key, with:

- UserID: MNEMO-CERT <cert@mnemo.com>
- KeyID: A38E028F
- Fingerprint: 51F9279977411BA6C2AA395CE36698DEA38E028F

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (MingW32)

mQINBFN0u+gBEADWOdoEZ38BvrcaQmUic+8589dCv+3NFAEG4+29N2WKTMvkaJ60
qUPmzIGxtfrqaMHiuy82dB5uh1BkDJ80JK1hqU56CV07/byuYXSCbqIcyIxVenNv
s5nj8ktzoqxn/2T++fuXCGz4CgTdA9m6phDmJO63CV+zBpYccnWO96kzhyswJSOY
k2zIOVFc+ls109sNS7opANb1yv8JxbAO3P4tmD//uHEfa7sZNMYyuoOgHRpSAUH2

+eclxRtdd2yDAj/BfvjC2HMcBSkd3CWCtCNPcmdYOdYdXLUdc3PPXTsrIh7koDhO
wyI3G+gZdCxM/ZVvMCGeVUhbQuRlgyyUc2NfqFs9skBiLB3tEaSrd9IdE1TQJrdm
I1mRp2+9y3dQvmdug6VyAfRejhtYLB7mCT1gQEhUb6A+8UrRKf56CzlFcjbchAIX
n2iqk5KqycDJhD0RbP2MrSSPPsP9K3r/lRD87/X3Jth/GcbvLj4pt8UakP12c/aY
d0hHEzeC7gEFQcWboKuL8cbPIt396VFhYMr5835MyX44eNqQxO8CO3o7NI5km+vc
3T+PyTv2qrGjGk+49+ieCpI9G7Na8VsHXfqpqIz/zmk2Fd3i1QwmjjxBVoVx1H0U
Yrr51GPNKN2zwhiRfYsFFEdBKnrggS1RRt5l0kh/AnDtoomSI9uIyFLL/wARAQAB
tBtNbmVtby1DRVJUIDxjZXJ0QG1uZW1vLmNvbT6JAjkEEwECACMFAlN0u+gCGw8H
CwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRDjZpjeo44Cj+LYD/4u+t6OxeR4
7l8wZr6G4VylgzPcXeeHr4YBDgw1biPnCXz31rrRysePyfkw6ku45GRP6oI1z8c9
Y2GZv2bgHROpnMcVj0XbMYCvcBJGmWXlZot0BvMwNLrVaudPe6bUiz2tHhW/stn1
7bClcbw8oKq1o16OBAnRN0sXhuvxqvC4FZgqTsjiA+FAtQXfY8x1zqG/lHqlrpo2
VFVe+jPBUtwyeizh8ev3m2/Hqzr+6h+eYR/uw03Wn+SDknotTqN1MIy6Kv7aZlq0
lENAxed8MEnL1dPObdrC3Y4bMxcXFQssX9u3Ue5T65xs9rqctFByoVCdiCT6hyZ+
CR0f88ysjRTUlZm+QB3T+26kp0ow28NwIdEW6qf3w1w7ZQDxBe/uf2IMLefakvG6
fDXID0iQwgYoclgnq33ppjbdb4GxV+ntlF8JQiMQiSSfBJNUq9kA+hpYCdFpOGET
3nEN4Q+EdXT+/rEB8ORnQ9dP02fA8uZ9QdIQmmddd34F4eJ7akckwVtflnm1FLYR
W97vNl9alSLYq3aeKGzweg5kqhPvsj6fVIBi2SPQ+LK0RQiLkonHHbUfvlDZHCET
iDa2mLHGjySwp6x542lTldEwnHmjC8G//W9jQ3yYWoj9HJrz9xVjE5PuOzy0Ih9u
taRsDPSEnpD4ATSVJTq4EHJ8k0+gMgp35w==
=0Ljh
-----END PGP PUBLIC KEY BLOCK-----

2.9.1 TEAM MEMBERS

The team is composed of security experts with more than 10 years of experience, performing various cybersecurity services, security alerts, incident reporting, incident management, cyber intelligence, digital forensics, digital surveillance, to name a few.

2.10.1 ADDITIONAL INFORMATION

Any other information about **MNEMO-CERT** can be found at http://cert.mnemo.com/.

2.11.1 CONTACT POINTS

For general purposes, the preferred method of contact is via email:

- info.cert@mnemo.com.

To report a security incident, preferably via the email address cert@mnemo.com. If you require urgent assistance, please include the word [URGENT] in the subject line.
If not possible (or not desirable for security reasons) using email, you can contact **MNEMO-CERT** by telephone: +34 (91) 417 67 76.
When submitting a report, if possible, use the above mentioned format called “Incident Report Form”, located at the website: https://mnemo.com/wp-content/uploads/2024/02/Formulario-CERT.pdf

2.12.1 OPERATING HOURS

The hours of operation of **MNEMO-CERT** are 24 hours a day, 7 days a week.

3. MNEMO-CERT

3.1.1 MISSION

To provide a reliable single point of contact for effective response to technology and ICT (Information and Communications Technology) related incidents in different economic and financial sectors and Critical Infrastructure in the public and private sector.

3.1.2 Vision

To encourage cooperation and information exchange between members of the financial sector to jointly develop projects, as well as to provide a high level of expertise in the field of critical infrastructure and cyber security to improve their protection and incident response capabilities.

3.1.3 Objectives

- Provide specialized cyber security services to reduce the risk level of your target community.

  - Standardize security strategies to serve as a reference framework for improving prevention, protection and response capabilities to new and emerging threats.
  - Define methods for the identification and analysis of the main cyber threats in order to understand the incident and establish an effective global response capability.
  - Promote security forums and integrate working groups for the exchange of knowledge, experiences, tools and techniques related to cybersecurity and the latest attack trends among members of the sector.
  - Build a national e-crime observatory for the collection, analysis and dissemination of information that provides qualitative and quantitative measurements related to security incidents in order to develop prevention and protection strategies.
  - Use new technologies, techniques and specialized training to prevent, detect and assist in the investigation and prosecution of electronic and white-collar crime, in accordance with applicable laws and regulations.
  - Disseminate useful and timely information that is related to security incidents of member financial institutions in order to assist in decision making to know where to focus their resources and attention.
  - Generate threat intelligence that can be used to identify tools, tactics and procedures used in cyber-attacks, in order to integrate security mechanisms and provide technical solutions in a customized manner that best suits your defensive posture.
  - Manage incident response through effective detection as well as coordination of the handling of all critical infrastructure related incidents using best practices, services and tools.

- Coordinate communication between internal, national and international incident response teams for the exchange of information and best practices related to computer security incidents.
- Issue timely alerts of vulnerabilities affecting critical infrastructures in order to act quickly to prevent or limit potential negative impacts.
- Analyze critical infrastructures to identify threats and risks that could affect their operation in order to develop effective protection strategies and measures.
- Obtain information on a permanent basis and generate intelligence mechanisms to prevent incidents, reduce risks and improve decision making.
- Build a knowledge base to improve understanding of key critical infrastructure security issues.
- Research and analyze trends and patterns of incident activity to provide in-depth knowledge about cyber threats and improve security infrastructure.

3.2.1 TARGET COMMUNITY

MNEMO-CERT is responsible for providing cybersecurity services to all organizations in different economic and financial sectors, critical infrastructure in the public and private sectors, as well as internal and external customers.

3.2.2 Target community countries

MNEMO-CERT provides cybersecurity services in the following countries:

- Spain
- Colombia
- Other Latam countries

3.3.1 SPONSORSHIP AND/OR AFFILIATION

MNEMO-CERT is an initiative of MNEMO Evolution & Integration Services. Since1998, the staff of MNEMO has worked together with Red.es for the management of information security incidents in both the academic and governmental sectors. In addition, they participated in the organization of congresses from 1999 to 2008, including different activities (conferences and courses) aimed at raising awareness and training in information security. In addition, they developed a network of cooperation projects with different universities.
Since 2001, this team has been involved in the definition and establishment of the UNAM-CERT (Computer Security Incident Response Team), which is in charge of responding to possible computer security incidents. They also coordinated several security projects in support of academic institutions such as UNAM-RENASEC (National Security Network of UNAM), NRIE (National Research and Education Network) and CLARA Network (Latin American Cooperation of Advanced Networks).
Since 2011, MNEMO staff has collaborated with e-LeCaixa CSIRT by exchanging information on information security incident handling.

3.4.1 AUTHORITY

MNEMO-CERT provides assistance and response for cybersecurity incidents that occur in all organizations in different economic and financial sectors and critical infrastructure in the public and private sectors.

4. SERVICES PROVIDED

The following table shows the services offered by **MNEMO-CERT**:

SERVICIOS	
Monitoring and detection of events and cyber-attacks.	- Security Operations Centers (SOCs). - Threat Hunting. - Use cases. - Monitoring.
Cyber Defensa – Digital Forensics and Incident Response (DFIR)	- Incident response. - Threat triage. - Malware analysis. - Digital Forensics Analysis. - Information recovery. - Cyber crisis management.

Cyber Protection	- Digital surveillance.
	- Alerts.
	- Takedowns.
	- Attack surface management.
	- Special reports.
	- Cyber investigations.
	- VIP monitoring.
	- Deepweb, Darknet, underground forums.
	- Threat intelligence.
	  ○ Threat profiling.
	  ○ Security bulletins.
	  ○ Vulnerabilities.
	- Attack Surface Reduction (ASR).
	  ○ Vulnerability assessment.
	  ○ Pentesting.
	  ○ Red Team.
	  ○ Adversary simulation.

Governance and Technology Risks - Training	- Implementation of information security standards.
	- Data protection compliance.
	- Analysis and development of processes.
	- Compliance audits.
	- Risk analysis.
	- Training and knowledge acquisition.
	  ○ Cyber exercises (Table TOP).
	  ○ Adversary simulation exercises.
	  ○ Awareness.

	○ Cybersecurity training. ○ Security Incident Response Process Maturity.

5. INCIDENT REPORT FORM

MNEMO-CERT has created a local format designed for incident reporting. The current version of the incident report format is available at: https://cert.mnemo.com/reporte-de-incidentes-ciberneticos/
Preferably to report an incident use encrypted email, using PGP keys.
In case of an emergency or crisis please provide MNEMO-CERT with at least the following information:

- Contact details and organization information:
  - Name of person.
  - Name and address of the organization.
  - E-mail address.
  - Telephone number.
- Brief description of the incident.
- Evidence available (documents attached).
- Estimated date and time of the incident.
- Relevant information to solve the incident.
  - Resources affected (number of devices affected).
  - Services affected.
  - Operating systems.

6. EXCLUSION OF LIABILITY

While every precaution will be taken in the preparation of information, notifications and alerts, MNEMO-CERT assumes no liability for errors or omissions, or for damages resulting from the use of the information contained therein.