1 DOCUMENT INFORMATION

1.1 Date of last update

03/04/2026

1.2 Distribution list for Notification

csirt@kio.tech

1.3 Document location

https://kio.tech/csirt

2 CONTACT INFORMATION

2.1 Team name

KIO Cyber Security Incident Response Team

2.2 Address

Calle Guillermo Haro, Santa Fe, Zedec Sta Fé, Álvaro Obregón, 01376 Ciudad de México, CDMX

2.3 Phone

+52 5579061458

2.4 Preferred contact method

Email csirt@kio.tech (please use our cryptographic key)

2.5 Website

https://kio.tech/csirt

2.6 Time zone

UTC / GMT - 6 hours

2.7 Hours of operation

24x7

2.8 Public keys and encryption

The CSIRT uses PGP for secure communications; the key is available at https://kio.tech/csirt

3 CHARTER

3.1 Mission

Manage the full incident response lifecycle to minimize the impact of cyber threats on our constituency, ensuring operational resilience. Our mission includes acting as a trusted node in the international community, actively contributing intelligence and best practices to strengthen the collective defense of the digital ecosystem.

3.2 Constituency

The target constituency of the KIO Cyber Security Incident Response Team is internal and external, as KIO ITS is one of the most important MSP/MSSPs in Mexico, therefore it needs to protect its own digital ecosystem, that of its clients, and that of the region against cybersecurity incidents.

- Internal Constituency: Comprises all technological infrastructure, information systems, networks, and digital assets that are owned by, or operated by KIO ITS for its corporate operations and service provision.
- External Constituency: Comprises all technological infrastructure, information systems, networks, and digital assets of public and private sector organizations or the FIRST community that request incident response services from the KIO Cyber Security Incident Response Team.

3.3 Sponsorship

KIO Cyber Security Incident Response Team belongs to KIO IT Services.

3.4 Authority

The authority and technical autonomy of the KIO Cyber Security Incident Response Team are granted by the KIO ITS Management team for the internal constituency; on the other hand, authority and autonomy in the external constituency are established under the terms of the FIRST community.

Within this framework, the team is authorized to:

- Direct and coordinate all security incident response activities.
- Perform technical analyses on affected systems, including forensic and malware analysis, as permitted by the agreement with the constituency.
- Recommend and, when applicable, execute immediate containment actions, such as isolating systems or blocking indicators of compromise in the security infrastructure.

- Interact directly with technical and administrative personnel of the constituency for effective incident management.

4 POLICIES

4.1 Information sharing and confidentiality

The KIO CSIRT manages all information under strict confidentiality criteria, using it exclusively for the prevention, detection, analysis, and mitigation of incidents. To guarantee the integrity, authenticity, and safeguarding of data at all times, we comply with KIO's Information Classification policy, use the TLP (Traffic Light Protocol) protocols, and PGP encryption.

PGP Key:

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGlqZhYBEADGvqtobcoUuUKF51B/TJHyBZ04xzVCEpKx1vCRDFwZp+mOBBa4
Dr8aeRXdaL23lumenC1bBnUosbNZQ/jlQBIcaj+0X+U4xUBvaDT5QGay5jH9thpy
Od7jpDkEjdeN7Mzkif2sGBQ193vDXkZFmEJcoHDKsKS2fVDw8Pd+yVML3oeCveSk
8SDYwC0wr9eoZaR+WuGQFKJmXE6nhfkcZL6B//BxnpOici+k/oGn0uUPsVh/fW1i
R7Vy/SVNLqIHqfcV0SrJpI3y5xyRR7oBmDwqCceAkxI4skekz3ARySW2jFCqabXx
dxIZliEfZSvTJBm0+W9TrQtZCZTvgCET3uZUENH8uXux9ChMOS9e7jf0MeaPMsVj
RWswh/ixO4UKsVAYZNN6ARbJayxbcuP8fIJVtbD4RQRUIW+2Yy8IRub1r/J4Jlml
xL/WIxakoN5SQ+lahnH9Nv8IsuIzUW5pUPN/1sob6w+RQcJUnn9DwPumHvS+drP8
WTQOpUqwOwkvJDkHLidajVn3O3wnqO/vJWeysx5JLDg61mSaaEukSJLDa82GvIL4
xLbgQlU2EjC9u5wyRbK6W7zn9y5VBCugxuKMID1V+TSNZgSI703kkdN8QVwZ96u3
HFbaFzRiUw8WKs1X4b3GoCyWo5Bz8H4xgnYhGAq/4p8AilZmHQlJ8KQKgQARAQAB
tDZDeWJlciBTZWN1cml0eSBJbmNpZGVudCBSZXNwb25zZSBUZWFtIDxjc2lydEBr
aW8udGVjaD6JAlcEEwEIAEEWIQSy8h0eE2QV/vCkveCRrSD/fCvwVAUCaWpmFgIb
AwUJAeFKCgULCQgHAgIiAgYVCgkICwIEFgIDAQIeBwIXgAAKCRCRrSD/fCvwVI1D
D/sFEf8QQmrm1HMX7e4xbdRJ92Oxo37tm9jJJV7/h5EkuesHKqrkYkdVouXSi2uR
8sKq4bTiqgUMVvvr2ntikqBVAebbyniXwdY9v4q5BwB/TtPOVPT0mPFXL2vKGXs0
13tJ5Bk5aW2o4Z8Jr8g7PAgYSFDEL/U5JG8HPcZCbMmHYe0s5gm86/VhXIPgwxmq
OYvooGuWssg8B3aS6b9HZPI4UGkzoLslyUCfOgQnjset/CaLjpp9s6ViVGjwzd1z
3rHny5cqIa0vxesrslkgN7+JLUCjN6usiic2+wFQhS3d0+hLUsnVFwgf++w79sQ4
oO2qrpMKsxOC+73ZgYJ+xxj+/J41Kqqt/ujqwTGYkd40/MBiNn/sbf7SFPGceFTN
Dnsb3CQ2jexPvHkGjfIKLfOr+RuCXGtg62wscaMEkW1+21QNDhWzuiuAzAYrCtSl
Rlg9UtE3OvO1ratemfI02klyIWdTA8Vl9LLWmSLU5SsCFvuGZN7onb+fxx7yGa+a
hYvI0yZwTs/jJFjDpt8P8hFFr4ubPQaGNQkQadWYdRYBPbkx81WjsqSbt3Il+ynb
L2Y5SuabauHNxuLzVQvFmBFx0mRM/0C5OX06jb11y/7xuT+73uiyLdc0Xjp1loWQ
HmGDjrzfvqMy49x6bIJIqxnEuTy/jQIqrPsre3JYIZd8fbkCDQRpamYWARAA4Qnn
CfKYjcH0Xmx/yrsRC0HF8Ab4FR2W2uYnGPOzZDXD47ybhnFZSeIMkhxDUI+wNZZN
LNmh2zj33Ve0Eye2qDKKBOyUbrNWpKqNfxhfFfkZBGBEBy3kaonasbXeW+RR2JMA
r4wG8/vItj0X5wlfVB0l0U6XdkHHqhu9vjdB9MP2mJrfyG7EPUl7CVq+EZt9gmWA
EGvKbmyZFU2ytSQfoBVwx4eGDfqDseTFkOP4L09kO4748ZpErrwz95PmbbnteF0X

QJcKYhv/oUVWPH16wEcEslCf4qCyJCAz5q3D1Cvg1+lL3XJdX9Ms0hslLSFMWTw9
mAxAK0xaRU1c6Ty5QeSv8nDYUMNTYfvls5FJcbExzrSiXUuyU7yABqQYfchakQQp
BT7Jie2cwOM7KkPUBGyvY/7BUqAWYnLT0DiBqRP/e0EB2byrYArvA5Etd66YM+fp
e87HzISFBijA0qo/5xDTavFx+zpWHURtC8catlRspKWcwU7fc+nqtHXmbb0bM3pO
VfaisegQOdu5xVLJISnA5V12BQ//GAAzfD0xMqY8Mxa7oCyuzk287WeJtbuHWdpx
me86RkqpS6lDxvP8REw21JRS+ONhpYkX1q7+IggxPP0JwV5CoLCXt+W7fAR3zk8Q
toNdU/2WtPJD0KgzvMN4OgpHizjhNtPdVtQALNcAEQEAAYkCPAQYAQgAJhYhBLLy
HR4TZBX+8KS94JGtIP98K/BUBQJpamYWAhsMBQkB4UoKAAoJEJGtIP98K/BUsncP
/AuFkORNpu0WXNyafe75LpTY0sk5rYVtRGST1ep8wLguaNQ5O/zF2fslEljXXRFf
7YRsABpBKI0v7HIRwmbHm880N0wwi2kMoVJ5fTEUML6b0D29J8akMW5vwzRB1DJC
g4jTKvjkLVWMwdCGrlrxwEoWHY13KI+1PV8sgA11U6PeUyFhILPvwveJr04IBKbP
Mfm6f4BXYO2svrcQdUWdVX11DAoa0/cCUPVXX78pjKenWVIrM32o/uZn+v7Ci6q+
QnaUtBgZkWFlhxqUB2p3JmmjJQt6aNJjHI1xNBCdW5ZUB+Nka5TzpYL1v1z8lWL0
OCRf1iY9ufG0Kt0xD2SdMGeNWwFYBJ8yWVRVc4EKE8P2ogB6ItGdxoV3oC94bhtE
lEtIwckq4goatfKGKu1cBfRiV2IMQna1Yuj9w2I2h7Qj2txlRS4Xtazwstt96CXT
YiiVNZYcwBJGWjOuzBbm/xUX251Eh8+z0uNJ3J8ov4ZpxMVDn+noM04yGimrW0na
1jehfqS2Ha3Fb2488NOpKozi/itPVTr5cbs59HWM4P8QCnVJuQihVE/6s0Pf1XuU
rLm7tU2/uPmQ4H5yI8IlfyOMhwYDPN5iU+QlshTm5KtRHQOVtHiytjt7BKqo3eNH
q4AHCew8xwAYVudHjw4fHfQTWhyEvgyYGrliBu+XEVQo
=RxdR
-----END PGP PUBLIC KEY BLOCK-----

5 SERVICES

5.1 Monitoring and detection

Purpose: To implement automated and continuous processing of diverse sources of information security incidents and contextual data in order to identify potential information security incidents, such as attacks, intrusions, data leakage, or security policy violations.

5.2 Acceptance of information security incident report

Purpose: To receive and process reports of potential information security incidents submitted by constituents, security event management services, or third parties.

5.3 Vulnerability response

Purpose: To actively acquire information about known vulnerabilities and act upon that information to prevent, detect, and remedy/mitigate those vulnerabilities.

6 INCIDENT REPORTING

It is important to specify useful information when reporting an incident, including the following elements:

6.1 Key incident details

- Contact Name and Organization
- Date and time of the incident
- Identification of the affected equipment or service (host name, IP address, function, operating system, specific service or application)
- Physical or network location where it occurred (e.g., department, network segment)
- Description of the incident
- Perceived or current impact
- Evidence collected (screenshots, error messages or malware, relevant logs during the incident, suspicious IP address, URL, or file name related to the event)

6.2 Actions taken

- Containment measures
- Notification to third parties

7 LEGAL DISCLAIMER

KIO Cyber Security Incident Response Team is not responsible for the misuse of the information provided in this document.