1 INFORMACIÓN DEL DOCUMENTO

1.1 Fecha de la última actualización

09/03/2026

1.2 Distribución de notificaciones

csirt@kio.tech

1.3 Ubicación del documento

https://kio.tech/csirt

2 INFORMACIÓN DE CONTACTO

2.1 Nombre de equipo

KIO Cyber Security Incident Response Team

2.2 Dirección

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

2.3 Teléfono

+52 5579061458

2.4 Método de contacto preferente

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

2.5 Website

https://kio.tech/csirt

2.6 Zona horaria

UTC / GMT - 6 horas

2.7 Horario de atención

24x7

2.8 Claves públicas y cifrado

El CSIRT utiliza PGP para comunicaciones seguras, la clave está disponible en https://kio.tech/csirt

3 MANDATO

3.1 Misión

Gestionar el ciclo de vida completo de la respuesta a incidentes para minimizar el impacto de las ciberamenazas en nuestra circunscripción, asegurando la resiliencia operativa. Nuestra misión incluye actuar como un nodo de confianza en la comunidad internacional, contribuyendo activamente con inteligencia y mejores prácticas para fortalecer la defensa colectiva del ecosistema digital.

3.2 Circunscripción objetivo

La circunscripción objetivo del KIO Cyber Security Incident Response Team es interna y externa, ya que KIO ITS es uno de los MSP/MSSP más importantes en México, por lo que necesita proteger contra incidentes de ciberseguridad el ecosistema digital propio, de sus clientes y de la región.

Circunscripción Interna: Comprende toda la infraestructura tecnológica, sistemas de información, redes y activos digitales que son propiedad de, o están operados por KIO ITS para sus operaciones corporativas y de prestación de servicios.

Circunscripción Externa: Comprende toda la infraestructura tecnológica, sistemas de información, redes y activos digitales de las organizaciones de los sectores público y privado o de la comunidad FIRST que soliciten los servicios de respuesta a incidentes del KIO Cyber Security Incident Response Team.

3.3 Patrocinio

KIO Cyber Security Incident Response Team pertenece a KIO IT Services.

3.4 Autoridad

La autoridad y autonomía técnica del KIO Cyber Security Incident Response Team se la otorga el equipo Directivo de KIO ITS para la circunscripción interna, por otro lado la autoridad y autonomía en la circunscripción externa se establece en términos de la comunidad FIRST.

Dentro de este marco, el equipo está autorizado para:

- Dirigir y coordinar todas las actividades de respuesta a incidentes de seguridad.
- Realizar análisis técnicos en los sistemas afectados, incluyendo análisis forense y de malware, según lo permita el acuerdo con la circunscripción.
- Recomendar y, cuando sea aplicable, ejecutar acciones de contención inmediatas, como el aislamiento de sistemas o el bloqueo de indicadores de compromiso en la infraestructura de seguridad.
- Interactuar directamente con el personal técnico y administrativo de la circunscripción para la gestión eficaz de un incidente.

4 POLÍTICAS

4.1 Intercambio de información y confidencialidad

El KIO CSIRT gestiona toda la información bajo estrictos criterios de confidencialidad, utilizándola exclusivamente para la prevención, detección, análisis y mitigación de incidentes. Para garantizar la integridad, autenticidad y resguardo de los datos en todo momento, cumplimos con la política de Clasificación de la Información de KIO, empleamos los protocolos TLP (Traffic Light Protocol) y el cifrado PGP.

Llave PGP:

-----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+IahnH9Nv8IsuIzUW5pUPN/1sob6w+RQcJUnn9DwPumHvS+drP8
WTQOpUqwOwkvJDkHLidajVn3O3wnqO/vJWeysx5JLDg61mSaaEukSJLDa82GvIL4
xLbgQlU2EjC9u5wyRbK6W7zn9y5VBCugxuKMID1V+TSNZgSI703kkdN8QVwZ96u3
HFbaFzRiUw8WKs1X4b3GoCyWo5Bz8H4xgnYhGAq/4p8AilZmHQlJ8KQKgQARAQAB
tDZDeWJlciBTZWN1cmI0eSBJbmNpZGVudCBSZXNwb25zZSBUZWFtIDxjc2lydEBr
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
RIg9UtE3OvO1ratemfI02klyIWdTA8Vl9LLWmSLU5SsCFvuGZN7onb+fxx7yGa+a
hYvI0yZwTs/jJFjDpt8P8hFFr4ubPQaGNQkQadWYdRYBPbkx81WjsqSbt3ll+ynb
L2Y5SuabauHNxuLzVQvFmBFx0mRM/0C5OX06jb11y/7xuT+73uiyLdc0Xjp1loWQ
HmGDjrzfvqMy49x6blJIqxnEuTy/jQIqrPsre3JYlZd8fbkCDQRpamYWARAA4Qnn
CfKYjcH0Xmx/yrsRC0HF8Ab4FR2W2uYnGPOzZDXD47ybhnFZSeIMkhxDUI+wNZZN
LNmh2zj33Ve0Eye2qDKKBOyUbrNWpKqNfxhfFfkZBGBEBy3kaonasbXeW+RR2JMA
r4wG8/vItj0X5wlfVB0l0U6XdkHHqhu9vjdB9MP2mJrfyG7EPUI7CVq+EZt9gmWA
EGvKbmyZFU2ytSQfoBVwx4eGDfqDseTFkOP4L09kO4748ZpErrwz95PmbbnteF0X
QJcKYhv/oUVWPH16wEcEslCf4qCyJCAz5q3D1Cvg1+IL3XJdX9Ms0hslLSFMWTw9
mAxAK0xaRU1c6Ty5QeSv8nDYUMNTYfvls5FJcbExzrSiXUuyU7yABqQYfchakQQp
BT7Jie2cwOM7KkPUBGyvY/7BUqAWYnLT0DiBqRP/e0EB2byrYArvA5Etd66YM+fp
e87HzlSFBijA0qo/5xDTavFx+zpWHURtC8catlRspKWcwU7fc+nqtHXmbb0bM3pO
VfaisegQOdu5xVLJISnA5V12BQ//GAAzfD0xMqY8Mxa7oCyuzk287WeJtbuHWdpx
me86RkqpS6lDxvP8REw21JRS+ONhpYkX1q7+IggxPP0JwV5CoLCXt+W7fAR3zk8Q
toNdU/2WtPJD0KgzvMN4OgpHizjhNtPdVtQALNcAEQEAAYkCPAQYAQgAJhYhBLLy
HR4TZBX+8KS94JGtIP98K/BUBQJpamYWAhsMBQkB4UoKAAoJEJGtIP98K/BUsncP
/AuFkORNpu0WXNyafe75LpTY0sk5rYVtRGST1ep8wLguaNQ5O/zF2fslEljXXRFf
7YRsABpBKI0v7HlRwmbHm880N0wwi2kMoVJ5fTEUML6b0D29J8akMW5vwzRB1DJC
g4jTKvjkLVWMwdCGrlrxwEoWHY13KI+1PV8sgA11U6PeUyFhILPvwveJr04IBKbP
Mfm6f4BXYO2svrcQdUWdVX11DAoa0/cCUPVXX78pjKenWVIrM32o/uZn+v7Ci6q+
QnaUtBgZkWFlhxqUB2p3JmmjJQt6aNJjHI1xNBCdW5ZUB+Nka5TzpYL1v1z8lWL0
OCRf1iY9ufG0Kt0xD2SdMGeNWwFYBJ8yWVRVc4EKE8P2ogB6ItGdxoV3oC94bhtE
lEtlwckq4goatfKGKu1cBfRiV2IMQna1Yuj9w2I2h7Qj2txlRS4Xtazwstt96CXT
YiiVNZYcwBJGWjOuzBbm/xUX251Eh8+z0uNJ3J8ov4ZpxMVDn+noM04yGimrW0na
1jehfqS2Ha3Fb2488NOpKozi/itPVTr5cbs59HWM4P8QCnVJuQihVE/6s0Pf1XuU
rLm7tU2/uPmQ4H5yI8IlfyOMhwYDPN5iU+QlshTm5KtRHQOVtHiytjt7BKqo3eNH
q4AHCew8xwAYVudHjw4fHfQTWhyEvgyYGrliBu+XEVQo
=RxdR
-----END PGP PUBLIC KEY BLOCK-----

5 SERVICIOS

5.1 Supervisión y detección

Finalidad: Poner en marcha un procesamiento automatizado y continuo de muy diversas fuentes de incidentes de seguridad de la información y datos contextuales a fin de identificar posibles incidentes de seguridad de la información, como ataques, intrusiones, filtración de datos o infracciones de la política de seguridad.

5.2 Aceptación del informe de incidentes de seguridad de la información

Finalidad: Recibir y procesar informes de posibles incidentes de seguridad de la información remitidos por los mandantes, los servicios de gestión de eventos de seguridad de la información o por terceros.

5.3 Respuesta de vulnerabilidades

Finalidad: Adquirir activamente información sobre las vulnerabilidades conocidas y actuar teniendo en cuenta esa información para prevenir, detectar y remediar/mitigar esas vulnerabilidades.

6 REPORTES DE INCIDENTES

Es importante especificar la información útil en el momento de reportar un incidente, incluyendo los siguientes elementos:

6.1 Detalles clave del incidente

- Nombre y Organización del contacto
- Fecha y hora del incidente
- Identificación del equipo o servicio afectado (nombre del *host*, dirección IP, función, sistema operativo, servicio o aplicación específica)
- Ubicación física o de la red donde ocurrió (ej. departamento, segmento de red)
- Descripción del incidente
- Impacto percibido o actual
- Evidencia recopilada (capturas de pantalla, mensajes de error o malware, logs relevantes durante el incidente, dirección IP sospechosa, URL o nombre del archivo relacionado en el evento)

6.2 Acciones tomadas

- Medidas de contención
- Notificación a terceros

7 DESCARGO DE RESPONSABILIDAD LEGAL

KIO Cyber Security Incident Response Team no se hace responsable por el uso indebido de la información proporcionada en este documento.