RFC 2350

Copyright

Confidentiality

This document contains confidential company information of a proprietary and sensitive nature. Therefore, it must be handled with the same security and precautions applied to confidential documents of this nature. Distribution must be controlled and limited to relevant entities only, and it must not be copied without written permission from ASHA Solution.

Table of contents

1. Document Information

1.1 Introduction

This document contains the information that CSIRT ASHA considers relevant to its target community, described in the following sections.The organization of this document follows the guidelines established in IETF RFC 2350, available at https://tools.ietf.org/html/rfc2350

1.2 Document Audience

The primary audience of this document is CSIRT ASHA clients. However, it is also intended for other established CSIRTs, organizations with a legitimate interest in the services provided, and the general public.
The document may be freely distributed, subject to copyright controls.

1.3 Last Updated

Version 1.0, published 05/12/2025.

1.4 Distribution List for Notifications

There is no distribution list for document change notifications. New versions, when published, will replace previous versions at:

https://ashasolution.com/contacto/

1.5 Location of This Document

This version is available on CSIRT ASHA's website at: https://ashasolution.com/contacto/ Make sure you're using the latest version of this document.

2. Contact Information

2.1 Team Name

CSIRT ASHA

2.2 Address

Av. Ejército Nacional Mexicano 1112 – Office 1001, Polanco, First Section Miguel Hidalgo, 11510, Mexico City, CDMX

2.3 Time Zone

Mexico City (GMT-6)

2.4 Telephone

+52 55 7258 2896

2.5 Email Address

inteligencia@ashasolution.com

2.6 Other Communication Means

Emergency phone: 8006573719

2.7 Public Keys and Encryption

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

mQINBGmvJSQBEADu7gpwesBFoxHbUG4WoIPmrUqde0lHMxphMMDJuFl1Zl4AJTu7
jFsnC4xmnNvFycKrNxHA1gWzo0ZcNs+w0G1qyN7Dln7gfcczoztXefzf3V3nd/fp
cVqBabJleerEUnlRPuq3LsAHRvMpe0jhI0UsUpxs+UGA9Q82bIaTRgetUnJGI2+H
F/iDcLYr0iI3gWVB96tIBwrEBG6JpPa4C0wLcnbFbrecDSNBfP0MG19SD2ZD0Cdn
a6KmqjIQb5ApKTJoDlSTK7tXyXWWewyb6dt4SwYBt8VZNQP0yETiKZtly2pWeoLf
dW/rpTROWY1ZuMJSccOJzkzzEU4xzoErQNIDpFHyh90gJTU8bdhpksfURnKP7lIm
ViNP7msRU9QzQ5HGIUF/j5Fj1RHQJkqiKgMUP+JML/XYURx8jRPoYam/nnzUAvS+
m85hNp7hBHSZZSg0HiP83vBZJ/NZAXXV2Aj0JqXEkt1LQSdB7GQE6InH96ue0Idj
3moSY9WDmvCU8zxYFESyL4QJLz1CMb7VMd88MHZpkXKgnsUjcPJUQNBZtGF90aCH
jFxkkTxgKIyo4hWCOstMLJg83bT6+2cLnkoRcyFDgHZ4Hn+e+h+YYThc5GALfUY9
AvNhiX/vY5j+ZSsBrzshCt1wnbSQ0Gwnn7aOFbFsNBUkSRksjEa5S0471QARAQAB
tCpDU0lSVCBBU0hBIDxpbnRlbGlnZW5jaWFAYXNoYXNvbHV0aW9uLmNvbT6JAnME
EwEIAF0bFIAAAAAABAAObWFudTIsMi41KzEuMTEsMiwxAhuBBQsJCAcCAiICBhUK
CQgLAgQWAgMBAh4HAheAFiEEDqZMjXGGezFlTyQbmBkr8DMPP2UFAmmvJxEFCQWl
ef8ACgkQmBkr8DMPP2Vxpg//ZiJT92Xfgi5Phs/KPEDNZxAeHao/vwLBVc/sl4u/
jIKSftPOTzHA3hBsxqw9wd8gzQsPN5uWetYayq8XH3mMPhXpQyUHCJbT2tvsBOZV
s/+tfCGRiCcXxdx6nGPDvR14Me1HWOTpZ/VlhmuPulxm6U1mGfmCBW0H5Gzf/IbY
5ZKa6bljXeWiraO63QKpnIvZGVlTepEZy7O7PUP6ipaRP2lg6uAxFV6VTwAQ62Il
SeB2RGDBQcPLFPolxOqM/HtbBFjgWu5tMugWHHaUodPzuQmLynH+/8OdjVTNV/Xi
EqFnr9PdaEsE6agzZxQd4M2pe7zh17rMhSFoqOGsmnL+d7niFotwcUkSP5EgOZcW
qRWeCXSKZEIBqjywr2ZfV/lJAP8J3WAxjJS/Z0kpCQybSgj/IQCeQMe7+wcwRpCh
EjqHYzStx/ixW4jHXJEIAiC0czIktUao3hkpEZ7FJYJJtrbpgCEMKD+Y13f9ID4l
ID9Op8/pGdg4UwKh99FQDxvNgM0byJJ96NklAjwA6d3Fl0l/Rehd+8zjgVzBvCwK
xgH3X342WrlnSZDFrB+GjzSlOrEwIomElQ6B1/YSb16X6y9bvsnOgDvRDW/mzdWQ
OHHax2z5rx4oPlYSTsYLM13jqDz1tvGFs9Ro52QA8EHylsoScW8jAnRz4MSI1ozN
wqK5Ag0Eaa8lJAEQAKJLXkf+IMEfJDabRYcc04dDrQio+9FZe+uOksrhJcZ9yO92
HAgD296++TCjP0g3KYXGb4rC53lCpGvZRa2QZIXbYKlT3AP9IWfzS5z6fBOPNrQ5
zJnQmeoHS9f7hI5/Mqj5VFrhce/tKmesHXtXSJRLK+s6xvsF3kIp4MAyy1HHWdD3
lY4qxWVW/lmG/CpcfrOR014RFa+R3/51h78MU3zDsOygIYL9W5pFvMTHzABe3XBo
Ls3ZIXvO1NyqXmGF+bcjq3LLNLQjeRLG96g1a9F7kdqdm2nV9ezzQ8+eAfhcc8yd
CVjA3t7DqkfCs/j5OH5vO9eC8FZzN6l5/BTrweoRcuCIFYOzznfV6vhI5SZlaejT
ZQYRCaHekFfWKy6Qp9ESjPBeQvbZGKTfK+ZFaXhqd6sKnEfgxrhX0Ppb+bgFyrSw

-----END PGP PUBLIC KEY BLOCK-----

WSqnrMGqzdcfHkMYyabBPNfro9oxexr7hFeQqfQzu9Yx0B+9QrUAR+tdXVMg/FCp
KGrab4VdIu95r6UgIO73yyzlWlN9zfrDiN6jUx86wj3XLHdf/HrMVVj8DKgXfSKZ
nZ9q99gs19DCyFr/CeLLYRwr28ra2Q3kuwxePcJUeULq1Cmflbqi7elMaiCKLXbZ
hTwznkZK+nOCgfzbKErXiD/76N/Lo0f412boXfMRxb6D6dUieTYFBFUsOXzhABEB
AAGJAlgEGAEIAEIWIQQOpkyNcYZ7MWVPJBuYGSvwMw8/ZQUCaa8lJBsUgAAAAAAE
AA5tYW51MiwyLjUrMS4xMSwyLDECGwwFCQWk0XwACgkQmBkr8DMPP2VdCRAA1BoF
9rWnYzbawhaCZF5hP52lZS8waiPC0yxdFMshg3Yp2rVSaPh2EEWzibv/3JunjTxk
grToH/TPfPmA3hAnt0qHXjGELcOS9TZ9Dw3WZvCAdRO3jQEbDj3bYZwzelCiIulR
89hobTm33UTvkuq2zWcrO0qPBAejRnK0L5iy7xOxs4QY0sAUXqn4Rw9cr4Cs8T2a
qP3H4W501YalrOHGb6viqIvjRHr/UifK9chnQBJjxDf/5HY+nlbfaP/PnZTJPyu6
N4m7nepudKWzfKN4JZdakgeZoUN7hcHVKeDcmjXMdWcWWd0JfHuJOIS+4nRNNnDz
fxutKuraIUtkaX84RTIG26b4mm38IwEVXwNaX9dEbYch7zk0z9CTnZLENN3pUxst
6r3+8dWsx0EibM1Doow6BKR4hFR/gnGKggnFY914W8nSwGBFRqpnUE03cG8Mfxiu
23FWqVu4SwmX1IEpkfzhE7KCUTjertr2R615/wUj/xcuneyYe9vVR9fJVt37v3sb
zMso/5+J79bRXFk5yZnYgSjlQJ2SOkWOUBvuiGvO9wNYEdHqMchKf0xfRmy0Hmnb
Indnw4z26IulXljyH89Sk+oRcfMWQsYvRszc0uv8AB9N8yN9tVd18lSyUNQiuaQo
NYpEXvhm2/Ytvs8GrJCg3knXxDytRUNSUrVRsdm5Ag0Eaa8lOQEQALNXXoIjZw5c
b2bhw0VL7lWKVRpEb5ssEUdWYNVta2we9/XEoyqeSfWNZBnbD2ku8OISINvtQkj0
f2Q/Rh6SGV0UwpE0UCtFwxevutAwyTkTNSXWd7n74UHTlRewsAcgj0wpuPTci6Wh
ijDH0WUP9AOxsFmm/WkUZDTk27q2XFwiPnTxpHqRqoAmnKw0fxhm9pcNgzBs3ops
WhwX+n/5c/Cp2mPyb9uMK4I4MVGZCr6d1j1NtAw8rNDHW3yPh3Zapk4gLdCUDQRE
6kkCqoqyi2v5JwXKDO3ZTe4qnBrgx3zejiU/ddgVxPbMDdV/+u88248SQ5opXhj6
bNtC3hn0+u3o9AFJSdf1A3JYiz6ZZeekMfTDHU5HeEXLFtZ1AaHhYK01eGAcuEvs
+McrZgYt57ENDysHTtg3divJnSt8YKFR5S1uiqm4d6dghsbXzIeCP8oAF+gga36U
Zz1NZ99+XG6PzgcI8yg6PZxCUIITc9x+df2hyGZzAJDkFu3IxgT6C66WNUI/e4q0
Q0K1pQxnrlYzqt8FATaLXCE9RrwBmWw8JO/4qbk6snWD3WsgFjeAdvyTP7ctIbP/
yXYpgZ5ggNsU3uiU8DDSH2FZE1GAqZzo+3jqO7TZttV+OxL7exJAGQCYu8b32CIn
T+VnXXTlo5DZXufl3WDuLGbmEkKtYnzRABEBAAGJBIgEGAEIADwWIQQOpkyNcYZ7
MWVPJBuYGSvwMw8/ZQUCaa8lORsUgAAAAAAEAA5tYW51MiwyLjUrMS4xMSwyLDEC
GwICQAkQmBkr8DMPP2XBdCAEGQEIAB0WIQScB4d7SYPqE6BX4OCZ8dn0yFEySgUC
aa8lOQAKCRCZ8dn0yFEySjDiEACWpmUUnwGxMdhdXt092gb8dKbvRD45xcea6KpK
TB4H88aMs3/Z7Bj1kN2s4m1jsni3rt8w/SYI+XrmHfvXrJZu/2xDxGt3L6PZslS7
+q2VZ4MIVICcQVlNMJRvyi1SuuiNnWqUIclg2E7zv7/A2TTj1nBjHkjIFBs/wIg1
AknsHO9ClQU0Q9R+ASlg43x9XSNMh87zNV3P3akhmKLJC3UZqTWDfXDqoL9VAKc2
R36dZLkBzq1UvGvRa90jp0SwrfWhz1hmH6mQmwyzbnHEfh9XUJLW9hAfDIMxvW2Q
bpQy4BOoSfmuMf+vRAMt4i1/4L0zQUK9WE6svE5oT3K32yt4fGc6DEU99SQzsrTx
pd7frqAYQTSMh1HE0/QB44t1rTEmMpRXR2uMjGy5eLlTU+r12x5Zl9tXu6vfqNeL
ZlCtg1BNO4Ri78b9ic/09lXRhCG7bvO8qZnnleXKT0eyAmf93NXmW2p4kSFcoyWW
mZmn+ta+TnWMohN87Nn7lpoBNag/vPtZtcsjR5cN8nqQiuczP5cUvGjK1Xo64llS
d28fZK478oVuj9/rBBnqrTDV/S7pNYFQ0cwklpGgjNvja2YDPJRuDNMOva5Miyy9
QpGhuH0TAJeNGe03QIorIqX+BreJzK9peheMtxtAYadxtO9lFm7bFjoRJy0g+baH
Cje91mXlD/4tBwAy9FiLgYJtKjBeQHs37h3z3CoYsdemoJesB0UFxV3pn9sJwDGF
mj32iHq+kvqcEz7Rd4hJaMMBq/eRMYFECqkUeILU2JXv1yMgmlnD3ALOoBp3k+yd
GQ5rpo6yIzvNuTQlozoQC6oY8RFZStF6nfw3j83qkGEG/XxYBI/pyldm6Gek1n4q
UWVKwOh1Yg68hHdORS5fS8afyXltlxHQ/lgN0d8PhD1jCENxwPEC9w6A4Qy4V7CM
tmyJY04syZfkLB3Six13ATqkdtLv8zZFQId4CH9QWHScCSZsAX/6ysI4Yl0lm+/8
ts6nXj/Wx10T6Slrx3idoYknZEIo4vgr5Xu40xYBabiEernFEBUDrQ/QmJ2hxLlr

4PRFCJ+yNpbwDkh2Cwue9BgmKNNBduydXl0qqob5qjlJjKj9GTx0ICAG8ph+kqSk
pqLSsoHR8ie2awtv+moUIrcR2mxhuYFzcOfXS+evdYzV5Y7Bih6Tq6Q9jTvJKjs6
0nLgS0Bfjng4lCmMcefuDJJ6l4l64XbESHIIgpnHMsiwqk+S5TLNJMKHGDw5qvjI
kdeW4ZKA/S9qzQTuGhf189MZT2PzCrPRtx8xFvELCwle1UVkCduOwF5qoHcFYeo1
RjliXmUkjTB1JgQLycMaTcN/vzsGSW8ioR0IqEfBCJX7jRyd/aAf2g==
=OMtg
-----END PGP PUBLIC KEY BLOCK-----

2.8 Team Members

The contact information and names of CSIRT ASHA members are confidential and not publicly disclosed. When necessary, team members will fully identify themselves in formal communications.

Structure:

- CSIRT Leader
- Cyber Threat Intelligence Specialists
- Cyber Threat Intelligence Analysts
- Operations Engineers

2.9 Operating Hours

Business hours: 10:00 a.m. – 5:00 p.m. (GMT-6), 5x7 schedule, Service Desk availability: 24/7/365

2.10 Additional Information

Additional information is available at:

https://ashasolution.com/contacto/

2.11 Contact Points

The preferred contact channel is via the following email address: inteligencia@ashasolution.com. This account is monitored by members of our team. If urgent attention is required, please include the word “urgent” in the “Subject” field of the email to ensure it is prioritized.

If it is not possible to use email, or if email cannot be used for security reasons, you may contact us by calling the number specified in Section 2.4 of this document. Telephone support is available during our business hours, from 10:00 a.m. to 5:00 p.m., Monday through Friday.

3. Charter

3.1 Mission

To provide proactive, contextualized, and reliable cyber intelligence through the acquisition, analysis, and timely communication of relevant information about threats, malicious actors, and attack vectors, continuously strengthening the security posture of our clients, partners, and stakeholders, and contributing to a more resilient and secure digital ecosystem.

3.2 Scope

CSIRT ASHA services are directed to the entire ASHA Solution client base, including internal departments and any external entity, whether public or private.

3.3 Sponsorship / Affiliation

ASHA CSIRT belongs to ASHA Solution S.A. de C.V. and reports directly to the SecOps Coordination.

3.4 Authority

ASHA CSIRT reports directly to SecOps Coordination for strategic alignment and oversight, while maintaining operational autonomy, full command authority, and technical decision-making capabilities within the established framework.

4. Policies

- All information managed by CSIRT ASHA must be handled under Confidentiality, Integrity, and Availability (CIA) principles.
- By default, all information is treated as confidential until formally classified.
- Information must be handled according to current security policies and through authorized corporate channels only.

4.1 Information Classification and Protection

All information is classified according to the Traffic Light Protocol (TLP):

- **TLP:RED** – Restricted to individuals directly involved.
- **TLP:AMBER** – Limited distribution to specific organizations.
- **TLP:GREEN** – Shareable within the cybersecurity community, not public.
- **TLP:CLEAR** – Public information, no sensitive data.

The assigned classification must remain visible in documents and/or investigation reports, preventing unauthorized disclosure. A formal classification process will be applied to incoming information, evaluating its relevance, sensitivity, and source, preserving the TLP classification throughout its lifecycle.

Information stored on servers and workstations must be protected with AES-256 encryption.

4.2 Access Controls and Responsibilities

- Access to information will be restricted under the principle of least privilege (need-to-know) and managed through role-based access controls (RBAC), authorized by the Engineering Management.
- The Area Leader will be responsible for keeping technological protection measures up to date, ensuring alignment with the Information Security Policy.
- Information Owners must perform periodic reviews annually or whenever a significant change occurs to verify compliance with policies, standards, and procedures, including retention periods and applicable legal requirements.
- All CSIRT ASHA personnel must have signed confidentiality agreements and internal codes of ethics and conduct.

4.3 Information Disclosure and Coordination

- Disclosure of incident-related information will be carried out only under strict protocols, prioritizing the protection of the involved parties and national cooperation.
- Authorization for disclosure rests with the CSIRT ASHA Leader, in coordination with SecOps Coordination, and all disclosures must be recorded, including recipients, date, and the applied TLP level.
- Before disclosing information, the cyber intelligence team and technical analysts will verify its accuracy, relevance, and sensitivity, preventing leaks or improper exposure.
- CSIRT ASHA may share IoCs, TTPs, and validated reports with trusted networks such as FIRST, ISACs, and MISP, through secure and traceable channels.

4.4 Evidence Preservation and Legal Considerations

- In cases involving potential legal implications, CSIRT ASHA will ensure the preservation of the chain of custody, guaranteeing the traceability and preservation of digital evidence.
- In interactions with third parties, the use of secure communication channels will be required.

4.5 Tools and Incident Reporting

- The use of tools for incident detection and analysis will be limited exclusively to those approved by the security area; the use of unauthorized or unlicensed software is prohibited.
- Any incident, detected vulnerability, or misuse of information must be reported immediately to the Area Leader and to the SecOps and CyberOps Coordinations, either directly or anonymously.
- CSIRT ASHA personnel must protect all information under their responsibility using only approved corporate channels and repositories.

5. Services

CSIRT ASHA conducts cyber investigation activities focused on the detection, analysis, and management of threats, based on its operational responsibilities and the contractual agreements established with its clients. Investigations are carried out under a formal methodological framework, respecting the principles of confidentiality, integrity, legality, and traceability.

Investigation services include, but are not limited to:

5.1 Incident Intake and Initial Analysis

CSIRT ASHA is authorized to:

- Receive, analyze, and manage both internal and external security incidents.
- Validate, classify, and prioritize events based on the defined severity matrix.
- Initiate technical investigations based on indicators of compromise (IoCs).
- Coordinate escalations to specialized teams according to the nature of the incident.

5.2 Threat Intelligence

As part of its functions, CSIRT ASHA:

- Integrates threat intelligence from internal and external sources (OSINT, SOCMINT, MISP, commercial feeds, and ISAC communities).
- Analyzes tactics, techniques, and procedures (TTPs) associated with known, emerging, or regionally targeted threat actors.
- Produces intelligence reports, alerts, and security advisories for clients, partner entities, and the general public.
- Actively participates in national and international forums (FIRST, OAS, CSIRTAmericas), representing ASHA Solution.

5.3 IoC Investigation

CSIRT ASHA conducts investigations on indicators such as:

- IP addresses
- Domains / subdomains
- File hashes (MD5, SHA-256)
- Suspicious URLs
- Malware artifacts
- Evidence of command and control (C2) infrastructure

Investigations include correlating IoCs with threat databases, community repositories, MISP platforms, and other collaborative intelligence sources.

5.4 Evidence Preservation

When the incident requires it:

- CSIRT ASHA protects digital evidence for regulatory or legal purposes.
- Ensures the chain of custody following forensic best practices.
- Documents every action taken, maintaining full traceability.

5.5 Reports

Investigations include the preparation of:

- Detailed technical reports
- Executive summaries for senior management
- Security alerts
- Emerging threat bulletins
- Root Cause Analysis (RCA), when applicable
- Updates to the threat inventory and the cyber risk map

5.6 Service Coverage

CSIRT ASHA investigation services apply to:

- ASHA Solution internal infrastructure.
- Managed services (MSSP, CSIRT as a Service, MISP, CISO as a Service).
- Managed cloud platforms: AWS, Azure, GCP.
- Hybrid environments under active contracts and confidentiality agreements.
- Regional coordination in Latin America and support for global operations through strategic partners.

6. Investigation Forms

CSIRT ASHA has an Official Investigation Request Form to channel and process security events, suspicious indicators, brand abuse incidents, malicious activity, exposed data, or any request for specialized analysis.

The form is available at:

- https://ashasolution.com/contacto/

This form constitutes the primary contact mechanism to initiate a formal investigation. Its content is described below:

6.1 Applicant Contact Data

The necessary information is collected to ensure traceability and enable effective communication with the person requesting the investigation:

- Full name (required)
- Email address (required)
- Phone number
- Country of residence
- Organization (required)
- Relationship with ASHA (client / non-client / partner)

This information will be used exclusively for incident management, in accordance with CSIRT ASHA confidentiality policies.

6.2 Incident Description

The section allows the requester to briefly explain:

- What is happening
- What needs to be investigated
- Perceived risks or potential impact
- Source of the alert (internal team, end user, monitoring system, third parties)

In addition, it defines:

- Urgency level (High, Medium, Low)

This helps CSIRT ASHA prioritize the request and assign an analyst appropriately.

6.3 Indicators

The form allows reporting technical indicators through structured fields:

- IP addresses (one per line): Allows entry of suspicious IPv4 and IPv6 addresses or those associated with the incident.
- Domains (one per line): To report relevant domains, subdomains, or URLs.
- MD5 hashes (one per line): Suspicious files or files related to malware.
- SHA-256 hashes (one per line): Suspicious files or files related to malware.

These provide precise technical evidence for advanced analysis.

These fields allow CSIRT to initiate an immediate technical investigation and correlate data with external sources.

6.4 Attach Evidence (Optional)

The form allows uploading relevant files such as:

- Screenshots
- Records or logs
- Suspicious malicious documents
- Additional evidence necessary to deepen the investigation

6.5 Post-Submission Process

Once the request is submitted:

- A confirmation of receipt is sent to the requester's email.
- The case is registered in the CSIRT event management system.
- An analyst is assigned to evaluate the severity and scope.
- The investigation begins, including:
  - Review of the indicators
  - OSINT/SOCMINT analysis
  - Correlation with MISP/FIRST intelligence
  - Risk and impact assessment
- Direct communication will be maintained with the requester throughout the entire process.

7. Disclaimer

The information contained in this document is provided "as is" for the purpose of supporting the community served by CSIRT ASHA in understanding its services, contact processes, and operational capabilities.

Although CSIRT ASHA makes reasonable efforts to ensure the accuracy, timeliness, and reliability of the content presented here, it does not guarantee that the information is complete, free of errors, or applicable to all possible scenarios.

Any use of this document by third parties is at their own responsibility.