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-----

```
mQGNBGYizhMBDACqMEmHcVVZL5g+NODv4laTax9gpujioOEK4Qa/LjRdgPILdYzv
Hl127lIq9D+qUa9GTzFqaMoGGBsNZRBQ0OFP6V1J559g/kPLDUzI6fQzWklC7EyU
tnRtsbk+xebcdiU0VsaNSCx06xJfWdssyCYfJsEs5BYNoDHMKtGkIeXAN+iq+KIy
857CUa+fAEBeiN/vkBJUOBK03ESGz4YDXmJv8rGisLT2blDTWRNdXUbKWet132Z/
yCMKBk2+NY6Q8exGv8vEvkPfg4WtRc+Tq1L3hExhqfmIeAio4gVg8aIZeLOkqetm
cvT7KfGmQ0DCYLPtea1lYoiBHCW4/F8qZzH7fbNrzQ/yYeuvwBivvtO/d6g0tzuo
8cIvtlaBUgpfznH1Xuf6ft7fSqJrqg6t6fsHXbyWdc9wFHSfDMiReuqZpr+e9a74
1et3/0qEhnd+0Fg34mtgktCIF+S84jkR0XC+KMjYpumNMKtPW4UH7/Djha9l7vku
p19G6zIm5Bsga4cAEQEAAbReQXV0b2dlbmVyYXRlZCBLZXkgKFdBUk5JTkc6IE1J
U1AgQXV0b0dlbmVyYXRlZCBLZXkgY29uc2lkZXIgdGhpcyBLZXkgVk9JRCEpIDxh
ZG1pbkBhZG1pbi50ZXN0PokBzgQTAQoAOBYhBDXqH26tdriQIxY3djotbnIVz8PB
BQJmIs4TAhsDBQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEDotbnIVz8PBrvML
/3DnQ9TUen0GN43vLoVPwOjAXf3XddDBIJth1+nOOIDtKjqZGHts6X237ZmOTaXy
wq81yIVqbuUYAVAdGxxUXmXKP0WxdyCCjEwo1nl1FECgN4Hl7WGx04ChutRUgnx8
ShseVO4xHF49L3afLAKKL+rXaBkYgwBbsNslGm0hn6Jiund5KKDdnxyEwOgulaM4
2eS62ahDJ7nPVdjsI2gzhKqy/AIw7qWy2BzEeqCZrmcreKxF97PdQM6lFZyI5WFo
YJsrYLbNiLpO1/DzD1fkE2LE8F2SrAOZqv/DjBkWY7pXS8x2KzNzeUt0ir3f+ek4
HMVlM9+4wGBYfIQm09rEG4qkJwhJmaSQDVjxND9oCtkhIod0tgiWriBOVQO1FAP3
IXSws81Vs9Vmk3G3JpKPaoziZSG+aruuGK6xqdOpBdw0yveD11q3FYCZCk0h3lf4
KPp1y+RQjl/lEMoWiyHkOvln0iQxR/n8opyypOqLWaHAhSuGh0ICGYsH+jPL1+CC
krkBjQRmIs4TAQwA1RDCe1BvrUv88hYlQe0Y+gsby0glWAhiOYJmxp6w5EA+wZ7i
WG6JJ3UfGocy/jQ9qdE9cvNBavI4VItn8gbebnmyeOGzeVxTjqUwlPtzcRaknFVp
qAAFCopQ+dcEBJoGtje8xoQhtaqT7qdp5+PUDvs4MgPkLEm5rH1otSy84vC1Ud8r
xaBsfPd+ofKGDir4L0ajT1JN3TIGv0Bq+NCx49YH2A2eIgI4PElPRxtFdOY31jo/
/gwcoklgQePLMzp+BolmcmbgnwYf6+p25qwhOGjjQxy6be9Ci7yh/OYNtDN34A32
Z2YugCUnloGA+tEoiSZwPz1HM9bynPTySjStwHnF+kzDvl8YFpfXY06YkWQN0Ys5
mG2y6tfyIeJnaES5SScOkvdx4oaVVKMcAiOLG/CBgM7jMaD/ziAGr6OZ3Qt0uejQ
cV4cg2qpGb+NkIorzFcMRx7I9yDJG2/ltNmiN/1ZYnIDHz8ZNzb0fhcrVKbpximJ
IIHmRj6SKxVaMj67ABEBAAGJAbYEGAEKACAWIQQ16h9urXa4kCMWN3Y6LW5yFc/D
wQUCZiLOEwIbDAAKCRA6LW5yFc/DwbntDACcQtsE+tv/zxgrBL2M4rAWTnfNU5U+
qyDVui/Z6A/rsy9ZGU93++wCFCfi+5p97t0OhHA+4QLyyIud6qkHguhL7eD5E/kD
99PVKG7vMWJheaW8nFbKKMsx9kubCIWjZeYZM0aCb1vh84t4bUPP6eMMIf02uCVg
```

```
ACeP0VrbEZ9lFXQkCdeNDG4RselG1WjkdAFkuzr1uEc4m66ZB2nz7LM2UvcH5khX
XfHbturmCFZuM1n9TkSG2sAJ5qDpP9rd+OHMwRbGpFXvMRjCU0Xc7B8N+MUUXLqd
EYoAPUqXhuyvkYgnIH3aMVk5/Sg4FwEum0ntCMpUMK7GqIezTxW4S16oNU5nbsPC
IRaeVYnU3MBQBHQqk+ShkWsatEmCddkXFneB9UY25/wfTzvduyK1pWErqo3+Uqsx
NUvEYT9FZ2gkbnvqBlcNVnHVkgRbLQrjsshqLckpvFTuy8ZnTI4vM5EwuPfnVXIT
92gVdCoJqPWvckszuiNzy1sGPtwTJ8wCHZ8=
=eM0e

-----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.