RFC 2350

Derechos de autor

Confidencialidad

Este documento contiene información confidencial de la empresa de naturaleza propietaria y sensible. Por lo tanto, debe ser manejado con la seguridad y precauciones con que se gestionan documentos confidenciales de esta naturaleza. Este documento debe tener una distribución controlada a las entidades relevantes exclusivamente, y no debería ser copiado sin el permiso escrito de ASHA Solution.

Contenido

1. Información del Documento

1.1. Introducción

El presente documento contiene la información que el CSIRT ASHA considera de interés para su comunidad objetivo, la cual se describe en la sección posterior. La organización del texto cumple con las directrices establecidas en la RFC-2350 del IETF, disponible en https://tools.ietf.org/html/rfc2350

1.2. Destinatarios del Documento

Los principales destinatarios de este documento son los clientes del CSIRT ASHA. No obstante, también está dirigido a cualquier otro CSIRT constituido, organización con un interés legítimo en los servicios provistos y al público en general. En consecuencia, el documento puede distribuirse libremente, sujeto exclusivamente a controles de copyright.

1.3. Fecha de la última actualización

Versión 1.0, publicada 05/12/2025.

1.4. Lista de distribución para notificaciones

No existe una lista de distribución para notificar cambios en este documento. Las nuevas versiones, cuando se generen, sustituirán a la anterior en https://ashasolution.com/contacto/.

1.5. Ubicaciones donde se puede encontrar este documento

Esta versión del documento está disponible en el sitio web de CSIRT ASHA la URL es: https://ashasolution.com/contacto/. Asegúrese de estar utilizando la última versión.

2. Información de contacto

2.1. Nombre del Equipo

CSIRT ASHA.

2.2. Dirección

Av. Ejército Nacional Mexicano 1112-Oficina 1001, Polanco, primera sección, Miguel Hidalgo, 11510 Ciudad de México, CDMX

2.3. Zona Horaria

Mexico City, CDMX (GMT-6)

2.4. Número de teléfono

+52 55 7258 2896

2.5. Dirección de correo electrónico

inteligencia@ashasolution.com

2.6. Otros medios de comunicación

Teléfono de emergencia: 8006573719

2.7. Llaves públicas y cifrado

-----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
99PVKG7vMWJheaW8nFbKKMsx9kubClWjZeYZM0aCb1vh84t4bUPP6eMMIf02uCVg
ACeP0VrbEZ9lFXQkCdeNDG4RselG1WjkdAFkuzr1uEc4m66ZB2nz7LM2UvcH5khX
XfHbturmCFZuM1n9TkSG2sAJ5qDpP9rd+OHMwRbGpFXvMRjCU0Xc7B8N+MUUXLqd
EYoAPUqXhuyvkYgnIH3aMVk5/Sg4FwEum0ntCMpUMK7GqIezTxW4S16oNU5nbsPC
IRaeVYnU3MBQBHQqk+ShkWsatEmCddkXFneB9UY25/wfTzvduyK1pWErqo3+Uqsx
NUvEYT9FZ2gkbnvqBlcNVnHVkgRbLQrjsshqLckpvFTuy8ZnTI4vM5EwuPfnVXIT

92gVdCoJqPWvckszuiNzy1sGPtwTJ8wCHZ8=
=eM0e
-----END PGP PUBLIC KEY BLOCK-----

2.8. Componentes del equipo

La información de contacto y los nombres de los miembros que integran el CSIRT ASHA son de carácter confidencial y no se difunden públicamente. En caso de que se requiera realizar un reporte, el personal del equipo se identificará plenamente con su nombre completo a través de una comunicación formal. Con la siguiente estructura:

- Líder del CSIRT
- Especialistas de Ciberinteligencia
- Analistas de Ciberinteligencia
- Ingenieros de Operaciones

2.9. Horario de Funcionamiento

Horario: 10:00 a.m. a 5:00 p.m (GMT-6), esquema 5x7 y la disponibilidad de la mesa de servicio: 24/7/365

2.10. Información Adicional

Para encontrar información adicional relacionada con el CSIRT ASHA , visite el sitio web de Asha Solution y consulte específicamente la sección dedicada al equipo: https://ashasolution.com/contacto/

2.11. Puntos de Contacto

El canal de contacto preferente es a través de la dirección de correo electrónico: inteligencia@ashasolution.com. Esta cuenta es supervisada por los miembros de nuestro equipo. En caso de requerir atención urgente, se solicita incluir la palabra “urgente” en el campo de “Asunto” (Subject) del correo para priorizar su gestión.

Si no fuera posible el uso del correo electrónico, o por motivos de seguridad no se pudiera hacer uso de este, puede contactarnos llamando al número especificado en la Sección 2.4 de este documento. La atención telefónica está sujeta a nuestro horario de oficina, de 10:00 a 17:00 horas, de lunes a viernes

3. Objetivos / Carta

3.1. Misión

Proporcionar inteligencia cibernética proactiva, contextualizada y confiable mediante la adquisición, análisis y comunicación oportuna de información relevante sobre amenazas, actores maliciosos y vectores de ataque para fortalecer de forma continua la postura de seguridad de nuestros clientes, socios y partes interesadas, contribuyendo activamente a un ecosistema digital más resiliente y seguro.

3.2. Alcance / Circunscripción

Los servicios proporcionados por el CSIRT ASHA están dirigidos para toda la base de clientes de ASHA Solution, abarcando tanto a nuestros departamentos/áreas internas como a cualquier entidad u organismo externo, sin importar si su naturaleza es pública o privada.

3.3. Patrocinio y/o afiliación

ASHA CSIRT pertenece a Asha Solution S.A. de C.V. y reporta directamente a la Coordinación de SecOps.

3.4. Autoridad

ASHA CSIRT reporta directamente a la Coordinación de SecOps, manteniendo una comunicación continua para efectos de alineación estratégica y supervisión, pero con capacidad de toma de decisiones propia, mando operativo pleno y atribuciones técnicas para dirigir el CSIRT de forma autocrática dentro del marco establecido.

4. Políticas

- Toda la información y documentación gestionada por el CSIRT ASHA, así como aquella proveniente de clientes, socios de negocio, proveedores y terceros, deberá ser tratada con responsabilidad y bajo los principios de Confidencialidad, Integridad y Disponibilidad (CIA).
- Por defecto, toda la información es tratada como confidencial, sin importar su origen o naturaleza, hasta que sea formalmente clasificada.
- El manejo de la información se realizará conforme a las políticas de seguridad vigentes, asegurando que su uso, almacenamiento y transferencia se realicen únicamente a través de medios corporativos autorizados y bajo los controles técnicos definidos.

4.1. Clasificación y Protección de la Información

- Toda la información será clasificada y manejada de acuerdo con el estándar Traffic Light Protocol (TLP), garantizando que su distribución se limite a lo permitido por el nivel asignado:
  - TLP:RED: Uso exclusivo del personal directamente involucrado en la gestión del incidente.
  - TLP:AMBER: Difusión controlada a organizaciones específicas que requieran los datos para mitigar amenazas.
  - TLP:GREEN: Intercambio dentro de la comunidad de ciberseguridad, sin restricciones geográficas, pero no pública.
  - TLP:CLEAR: Información que puede hacerse pública, libre de datos sensibles.

- La clasificación asignada deberá mantenerse visible en documentos y/o reportes de investigación, evitando divulgación no autorizada.
- Se aplicará un proceso formal de clasificación de la información entrante, evaluando su relevancia, sensibilidad y fuente de origen, preservando la clasificación TLP durante su ciclo de vida.
- La información almacenada en servidores y/o estaciones de trabajo deberá estar protegida mediante cifrado AES-256.

4.2. Controles de Acceso y Responsabilidades

- El acceso a la información estará restringido bajo el principio de privilegio mínimo (need-to-know) y gestionado mediante controles basados en roles (RBAC), autorizados por la Gerencia de Ingeniería.
- El Líder de Área será responsable de mantener actualizadas las medidas tecnológicas de protección, garantizando la alineación con la Política de Seguridad de la Información.
- Los Propietarios de la Información deberán realizar revisiones periódicas de manera anual o si se efectua algún cambio significativo para verificar el cumplimiento de políticas, normas y procedimientos, incluyendo periodos de retención y requisitos legales aplicables.
- Todo el personal del CSIRT ASHA deberá haber firmado clausulas de confidencialidad, y los códigos internos de ética y conducta.

4.3. Divulgación y Coordinación de la Información

- La divulgación de información sobre incidentes se realizará únicamente bajo protocolos estrictos, priorizando la protección de las partes involucradas y la cooperación nacional.
- La autorización de divulgación recae en el Líder del CSIRT ASHA, en coordinación con la Coordinación de SecOps, y toda divulgación deberá ser registrada, incluyendo destinatarios, fecha y nivel TLP aplicado.
- Antes de divulgar información, el equipo de ciberinteligencia y los analistas técnicos verificarán su veracidad, relevancia y sensibilidad, evitando fugas o exposición indebida.
- El CSIRT ASHA podrá compartir IoCs, TTPs y reportes validados con redes de confianza como FIRST, ISACs y MISP, bajo canales seguros y trazables.

4.4. Preservación de Evidencias y Consideraciones Legales

- En los casos que involucren potenciales implicaciones legales, el CSIRT ASHA asegurará la preservación de la cadena de custodia, garantizando la trazabilidad y conservación de evidencias digitales.
- En las interacciones con terceros, se exigirá la utilización de canales seguros.

4.5. Uso de Herramientas y Reporte de Incidentes

- El uso de herramientas para detección y análisis de incidentes estará limitado exclusivamente a las aprobadas por el área de seguridad; se prohíbe el uso de software no autorizado o sin licencia.
- Cualquier incidente, vulnerabilidad detectada o uso indebido de la información deberá ser reportado de forma inmediata al Líder de Área y a las Coordinaciones de SecOps y CyberOps, ya sea de manera directa o anónima.
- El personal del CSIRT ASHA deberá proteger toda la información bajo su responsabilidad utilizando únicamente los canales y repositorios corporativos aprobados.

5. Servicios

El CSIRT ASHA realiza actividades de investigación cibernética orientadas a la detección, análisis y gestión de amenazas, con base en sus atribuciones operativas y en los acuerdos contractuales establecidos con sus clientes. Las investigaciones se realizan bajo un marco metodológico formal, respetando principios de confidencialidad, integridad, legalidad y trazabilidad.
Los servicios de investigación incluyen, pero no se limitan a:

5.1. Recepción y Análisis Inicial de Incidentes

El CSIRT ASHA está autorizado para:

- Recibir, analizar y gestionar incidentes de seguridad tanto internos como externos.
- Validar, clasificar y priorizar los eventos en función de la matriz de severidad definida.
- Iniciar investigaciones técnicas basadas en indicadores de compromiso (IoC).
- Coordinar escalaciones hacia equipos especializados según la naturaleza del incidente.

5.2. Investigación de Inteligencia de Amenazas (Threat Intelligence)

Como parte de sus funciones, el CSIRT ASHA:

- Incorpora inteligencia de amenazas proveniente de **fuentes internas y externas** (OSINT, SOCMINT, MISP, feeds comerciales y comunidades ISAC).
- Analiza tácticas, técnicas y procedimientos (TTPs) asociados a actores de amenaza conocidos, emergentes o dirigidos a la región.
- Genera reportes de inteligencia, alertas y directivas de seguridad para clientes, entidades aliadas y público en general.
- Participa activamente en foros nacionales e internacionales (FIRST, OEA, CSIRTAmericas), actuando en representación de ASHA Solution.

5.3. Investigación de Indicadores de Compromiso (IoC)

El CSIRT ASHA realiza investigaciones sobre indicadores tales como:

- Direcciones IP
- Dominios / subdominios
- Hashes de archivos (MD5, SHA-256)
- URLs sospechosas
- Artefactos de malware
- Evidencias de infraestructura de comando y control (C2)

Las investigaciones incluyen la correlación de IoCs con bases de datos de amenazas, repositorios comunitarios, plataformas MISP y otras fuentes de inteligencia colaborativa.

5.4. Preservación de Evidencia y Cadena de Custodia

Cuando el incidente lo requiere:

- El CSIRT ASHA protege evidencia digital para fines regulatorios o legales.
- Asegura la **cadena de custodia** siguiendo buenas prácticas forenses.
- Documenta cada acción ejecutada, manteniendo la trazabilidad completa.

5.5. Reportes Técnicos y Ejecutivos

Las investigaciones incluyen la elaboración de:

- Reportes técnicos detallados
- Resúmenes ejecutivos para Alta Dirección
- Alertas de seguridad
- Boletines de amenazas emergentes
- Análisis de causa raíz (RCA), cuando corresponda
- Actualización del inventario de amenazas y del mapa de riesgos cibernéticos

5.6. Cobertura del Servicio

Los servicios de investigación del CSIRT ASHA aplican a:

- Infraestructura interna de ASHA Solution.
- Servicios administrados (MSSP, CSIRT as a Service, MISP, CISO as a Service).
- Plataformas en la nube gestionadas: AWS, Azure, GCP.
- Ambientes híbridos bajo contratos activos y acuerdos de confidencialidad.
- Coordinación regional en Latinoamérica y apoyo a operaciones globales mediante socios estratégicos.

6. Formularios de investigación

El CSIRT ASHA dispone de un **Formulario Oficial de Solicitud de Investigación** para canalizar y procesar eventos de seguridad, indicadores sospechosos, incidentes de abuso de marca, actividad maliciosa, datos expuestos o cualquier solicitud de análisis especializado.

El formulario se encuentra en:

- **https://ashasolution.com/contacto/**

Este formulario constituye el **mecanismo primario de contacto** para iniciar una investigación formal. A continuación se describe su contenido:

6.1. Datos de Contacto del Solicitante

Se recopila la información necesaria para dar trazabilidad y permitir una comunicación efectiva con quien solicita la investigación:

- **Nombre completo (obligatorio)**
- **Correo electrónico (obligatorio)**
- Teléfono
- País de residencia
- **Organización (obligatorio)**
- **Relación con ASHA** (cliente / no cliente / aliado)

Esta información será utilizada exclusivamente para la gestión del incidente, según las políticas de confidencialidad del CSIRT ASHA.

6.2. Descripción del Incidente o Contexto

La sección permite al solicitante explicar brevemente:

- Qué está ocurriendo
- Qué necesita investigar
- Riesgos percibidos o impacto potencial
- Fuente de la alerta (equipo interno, usuario final, sistema de monitoreo, terceros)

Además, se define:

- **Nivel de urgencia** (Alta, Media, Baja)

Esto ayuda al CSIRT ASHA a priorizar la solicitud y asignar un analista de manera adecuada.

6.3. Indicadores para Investigar

El formulario permite reportar indicadores técnicos mediante campos estructurados:

- Direcciones IP (una por línea): Permite ingresar IPv4 e IPv6 sospechosas o asociadas al incidente.
- Dominios (uno por línea): Para reportar dominios, subdominios o URLs relevantes.
- Hashes MD5 (uno por línea): Archivos sospechosos o relacionados con malware.
- Hashes SHA-256 (uno por línea): Archivos sospechosos o relacionados con malware.

Evidencias técnicas de mayor precisión para análisis avanzado.

Estos campos permiten al CSIRT iniciar una investigación técnica inmediata y correlacionar datos con fuentes externas.

6.4. Adjuntar Evidencia (Opcional)

El formulario permite cargar archivos relevantes como:

- Capturas de pantalla
- Registros o logs
- Documentos maliciosos sospechosos
- Evidencias adicionales necesarias para profundizar la investigación

6.5. Proceso Tras el Envío del Formulario

Una vez enviada la solicitud:

- **Se genera una confirmación de recepción** hacia el correo del solicitante.
- **El caso se registra en el sistema de eventos** del CSIRT.
- **Se asigna un analista** que evaluará la severidad y el alcance.
- **Se inicia la investigación**, incluyendo:
    - Revisión de los indicadores
    - Análisis OSINT/SOCMINT
    - Correlación con inteligencia MISP/FIRST
    - Evaluación de riesgo e impacto
- Se mantendrá comunicación directa con el solicitante durante todo el proceso.

7. Descarga de responsabilidad

La información contenida en este documento se proporciona “tal cual” con el propósito de apoyar a la comunidad atendida por el CSIRT ASHA en la comprensión de sus servicios, procesos de contacto y capacidades operativas. Aunque el CSIRT ASHA realiza esfuerzos razonables para asegurar la precisión, vigencia y confiabilidad del contenido aquí presentado, no se garantiza que la información sea completa, esté libre de errores o sea aplicable a todos los escenarios posibles. El uso que terceros hagan de este documento es de su exclusiva responsabilidad.