Constitución

CSIRT-AVP

AVP Sistemas S.A.

VERSIÓN 01	
FECHA DE PUBLICACIÒN: 21 de diciembre de 2023	
Próxima revisión:	21 de diciembre de 2024
Elaborado por:	Estefanía Valencia
Aprobado por:	Aldo Verni

Índice de contenidos

1. INFORMACIÓN DEL DOCUMENTO

Este documento contiene una descripción de CSIRT-AVP. El presente documento contiene información básica sobre el CISRT-AVP en sus responsabilidades y servicios prestados.

1.1. Fecha de última actualización.

La última actualización de la documentación se realizó el 21 de diciembre de 2023 como su versión 1.0.

1.2. Lista de distribución.

Se cuenta con una lista de distribución pública para comunicaciones y notificaciones relacionados a eventos y/o incidentes de seguridad de la información a través de csirt@avp-ec.com.

1.3. Ubicación del documento.

La versión actual de este documento está disponible en www.avp-ec.com.

1.4. Identificación del documento.

Título: Constitución

Versión: 1.0.

Fecha del documento: 21 de diciembre de 2023

Caducidad: este documento es válido hasta que sea reemplazado por una versión posterior.

2. INFORMACIÓN DE CONTACTO

2.1 Nombre del equipo.

CSIRT-AVP.

2.2 Dirección postal.

CSIRT-AVP

Leonidas Plaza N24-318 y Baquerizo Moreno. Edificio Plaza 246. Planta baja, oficina 101.

CP: 170143

Quito, Ecuador.

2.3 Zona horaria.

América/Guayaquil (GMT-0500).

2.4 Teléfono.

+593 22529003

2.5 Fax.

No disponible.

2.6 Otros medios de comunicación.

Facebook: @AVPsistemas.sa

Instagram: @avp_ec

Linkedin: @avpsistemas

Twitter: @avp_ec

WhatsApp: +593 96 916 4676

2.7 Dirección de correo electrónico.

csirt@avp-ec.com.

2.8 Claves públicas.

CSIRT-AVP proporcionará la clave una vez realizado el contacto con el cliente.

2.9 Miembros del Equipo.

Equipo CSIRT-AVP (Operadores, Analistas, Especialistas en Respuesta a Incidentes).

2.10 Otra Información.

Toda la información sobre el CSIRT-AVP se encuentra disponible en el siguiente link: https://www.avp-ec.com/csirt-avp

2.11 Formas de contacto.

El método de contacto recomendado se establece a través del correo electrónico a csirt@avp-ec.com.

Los mensajes serán recibidos por el Equipo Especializado de AVP de forma inmediata. En caso de no contar con acceso a correo electrónico, se recomienda como segunda

opción el uso de nuestro canal de comunicación por teléfono en horarios de operación. Los horarios de operación del CSIRT-AVP son de lunes a viernes de 8AM a 6PM.

3. CONSTITUCIÓN

3.1 Propósito y misión

Propósito. El CSIRT-AVP se constituye como un CSIRT comercial de carácter mixto, cuyos propósitos se basan en los siguientes puntos:

- Apoyar a sus miembros en la implementación de medidas preventivas y proactivas en temas de seguridad de la información, para evitar riesgos asociados a sus activos críticos de información.
- Apoyar a sus miembros en la investigación forense y respuesta a incidentes bajo solicitud.
- Apoyar a otros equipos de seguridad de la información como punto de contacto con fuentes de inteligencia nacionales e internacionales de información ante escenarios de respuesta a incidentes.

Misión. Brindar soluciones tecnológicas a empresas locales medianas y grandes, multinacionales y gubernamentales contando con el personal altamente calificado y especializado en todas las soluciones que ofrecemos, comprometiéndonos con el usuario al darle la mejor de las experiencias. Nuestro equipo carece de barreras mentales y geográficas lo cual nos permite de la mano de la tecnología trascender fronteras y generaciones.

3.2 Miembros

- **Miembros externos:** Los miembros del CSIRT-AVP son todos sus clientes.
- **Miembros internos:** Se cuenta con el apoyo interno de nuestro equipo especializado CSIRT-AVP

3.3 Auspicios y afiliados.

El CSIRT-AVP opera bajo la dirección del Coordinador del CSIRT/Gerente Operativo de SOC

3.4 Autoridad.

El CSIRT-AVP trabaja en colaboración con los administradores de sistemas y usuarios de AVP Sistemas S.A. Si las circunstancias lo justifican, el CSIRT-AVP apelará para ejercer su autoridad, directa o indirecta, según lo definan las políticas internas de la organización.

4. POLÍTICAS

4.1 Tipos de incidentes y nivel de soporte.

Los miembros del CSIRT-AVP reportarán toda actividad asociada a incidentes de seguridad de la información a través del correo electrónico: csirt@avp-ec.com o a través del registro del formulario disponible aquí. El Coordinador del CSIRT-AVP debe gestionar todo requerimiento que ingrese con el canal de comunicación mencionado considerando:

- Validar la membresía del solicitante para la gestión del incidente reportado.
- Para los miembros se procederá con la asignación de un técnico líder de respuesta a incidentes para la gestión del incidente reportado. Para los reportes que procedan de no miembros, el Coordinador del CSRIT validará la posibilidad de apoyo para el envío de información acerca de indicadores de compromiso asociados al incidente reportado.

Adicionalmente a la asignación del líder de respuesta a incidentes, el Coordinador del CSIRT establecerá la clasificación del incidente considerando:

Incidentes de relevancia crítica:

- Ataques de Ransomware.
- Infección de malware.
- Accesos no autorizados como usuarios administradores.
- Daños a la reputación.

Incidentes de relevancia alta:

- Accesos no autorizados como usuarios sin privilegios.
- Ataques de denegación de servicio dirigidos.
- Comportamiento malicioso desde la red interna.
- Secuestro de servicio web de la organización.
- Ataques de SCAM.

Incidentes de relevancia media:

- Ataques a través de correo electrónico (SPAM, ingeniería social, chantaje por email, Spoofing, Phishing).
- Ataques de malware a dispositivos móviles.
- Fuga de información.
- Nuevos escenarios de riesgo no identificados.

Incidentes de relevancia baja:

- Abuso interno de activos de información (Generación de tráfico elevado de red, intentos de acceso por fuerza bruta).
- Ataques contra la marca de la organización.

Los nuevos escenarios de seguridad de la información no identificados tendrán una categorización inicial de relevancia Medio. Sin embargo, en caso de ser necesario y

según lo disponga el Coordinador del CSIRT, se puede recategorizar su nivel de riesgo y afectación.

4.2. Cooperación, interacción y publicación de información.

El CSIRT-AVP podrá colaborar con otros CSIRT y CERT nacionales o internacionales, así como con otros terceros afectados en la medida en que los acuerdos de trabajo lo definan o bajo la autorización del Coordinador del CSIRT. La información generada por los servicios del CSIRT-AVP se puede compartir con sus suscriptores, así como con los proveedores y partners de servicios de ciberseguridad, según sea necesario.

El intercambio de información se realizará con el cumplimiento de obligaciones contractuales, legales y éticas definidas con sus suscriptores, principalmente con el ofuscamiento de información para la protección de entidad de nuestros suscriptores. Información como Indicadores de compromiso, perfilamiento de atacantes y posibilidades de explotación de vulnerabilidades se podrán compartir según lo defina el Coordinador del CSIRT.

4.3. Comunicación y autenticación.

Los niveles de intercambio de información dependerán de su destinatario, el CSIRT-AVP identifica los siguientes niveles de comunicación:

- Intercambio de información propia del suscriptor: Cuando el CSIRT-AVP establezca un intercambio de información de indicadores de compromisos (informes y/o reportes) y alertas del propio suscriptor se aceptará como envió seguro el uso de correos electrónicos sin encriptar.
- Intercambio de información consolidados y nuevas amenazas: Cuando el CSIRT-AVP realice un intercambio de información de indicadores de compromiso regionales o nuevas amenazas detectadas a través de reportes consolidados se considera como envió seguro el uso de correo electrónico sin encriptar.
- Intercambio de información con CSIRT/CERT regionales: Cuando el CSIRT-AVP establezca un intercambio de información sobre incidentes y/o indicadores de compromiso sobre escenarios de riesgo actuales, lo debe realizar a través de correos electrónicos encriptados.

El cumplimiento de esta política se realizará desde el correo oficial del CSIRT-AVP csirt@avp-ec.com así como con el uso de correos institucionales del personal que forma parte del proceso (Operadores, Analistas, Coordinadores, Gerentes, Consultores de Seguridad de la Información).

Se prohíbe el intercambio de información del CSIRT por medios no oficiales como: redes sociales, correos electrónicos personales o dispositivos de almacenamiento externo no autorizados.

5. SERVICIOS

Los servicios prestados por el CSIRT-AVP se dividen en dos grandes grupos: Respuesta a incidentes y actividades proactivas para resolución de incidentes.

5.1 Respuesta a Incidentes.

La respuesta a incidentes busca proporcionar disponibilidad para coordinar la contención, erradicación y recuperación de los incidentes relacionados con la seguridad de la información y consiste en experiencia, herramientas y otras capacidades para actuar, analizar y comunicarse con las partes interesadas y los medios de comunicación.

5.1.1 Monitoreo de infraestructura tecnológica

- Monitoreo 24/7 de activos críticos de información a través de los logs que estos generen.
- Detección de amenazas, indicadores de compromiso y vulnerabilidades asociados a los activos de información que formen parte del alcance de monitoreo.

5.1.2 Resolución de incidentes

- Brindar asesoramiento a los suscriptores a eliminar las vulnerabilidades o brechas de seguridad que permitieron la ejecución del incidente y proteger los sistemas de los efectos de los incidentes.
- Evaluar qué acciones son más adecuadas para proporcionar los resultados deseados con respecto a la resolución del incidente.
- Acompañamiento en la contención y erradicación de artefactos, malware y/o comunicaciones asociadas al incidente de seguridad de la información.

5.1.3 Análisis forense

- Proporcionar asistencia en la recopilación de pruebas y la interpretación de datos para identificar el escenario de riesgo usado en el incidente.
- Realizar la investigación en base a las evidencias sobre las brechas de seguridad y/o actores asociados al incidente de seguridad de la información materializada en la organización.

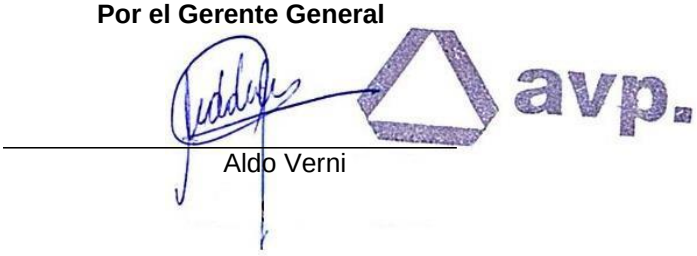
6. FORMULARIOS DE REPORTE DE INCIDENTES

Para informar sobre algún incidente asociado al CSIRT-AVP, se debe reportar a csirt@avp-ec.com o registrarlo en el formulario de incidentes que está disponible en el servicio web del CSIRT-AVP.

7. AVISO LEGAL

Considerando los controles y precauciones en la preparación de información, notificaciones y alertas, el CSIRT-AVP no asume responsabilidad por errores, omisiones o daños resultantes de la información aquí contenida.

Por el Gerente General



Aldo Verni