



**SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**

**INDICE**

I. DESCRIPCIÓN .....	2
OBJETIVO .....	2
ALCANCE.....	2
DEFINICIONES .....	2
II. POLÍTICAS DE OPERACIÓN.....	3
III. RESPONSABILIDADES .....	4
IV. PROCEDIMIENTO .....	5
DESARROLLO .....	5
DIAGRAMA .....	7
V. REFERENCIAS.....	8
VI. FORMATOS.....	8
VII. ATENCIÓN A USUARIOS .....	8
VIII. PREGUNTAS FRECUENTES .....	9
IX. HISTÓRICO DE REVISIONES.....	10
X. CONTROL DE VERSIONES.....	11
XI. CREDITOS. ....	11



### I. DESCRIPCIÓN

#### OBJETIVO

Atender las solicitudes de instalación cliente antimalware en los equipos de cómputo, propiedad de la Universidad Veracruzana, como una medida de protección contra la infección, contaminación y propagación de malware, con el fin de mantener su disponibilidad y buen funcionamiento.

#### ALCANCE

Aplica al personal que labora en la Universidad Veracruzana que solicite la instalación del cliente de antimalware institucional para los equipos de cómputo propiedad de la Institución.

#### DEFINICIONES

<b>Administrador del Centro de Servicios.</b>	Persona con perfil especializado, encargado de coordinar y canalizar la atención de reportes de asistencia técnica solicitados por los usuarios a través de la Herramienta para la Gestión de Servicios, todos relacionados a la atención de problemas o incidentes en los servicios de TI (Tecnologías de Información).
<b>Check List. (Lista de Cotejo)</b>	Conjunto de actividades preestablecidas que se deben ejecutar en la revisión de un equipo de cómputo infectado por un posible malware.
<b>Equipo de cómputo.</b>	Es el equipo de escritorio o portátil, propiedad de la Universidad Veracruzana, al cual se le instalará el cliente de antimalware.
<b>Folio de Servicio.</b>	Clave alfanumérica asignada por la herramienta para la gestión de servicios para identificar una solicitud de servicio.
<b>Formato de Servicio.</b>	Documento establecido para documentar el servicio solicitado (Formato SGSI-GISI-F-022).
<b>Herramienta para la Gestión de Servicios.</b>	Punto de contacto único para el registro, seguimiento, control y solución de servicios tecnológicos que ofrece la Dirección General de Tecnología de Información a la comunidad universitaria.
<b>Instalación nativa o Stand Alone.</b>	Instalación del cliente configurada para operar de manera independiente, sin conectarla a una de las consolas de administración de antimalware de la Dirección General de Tecnología de Información (DGTI).
<b>Malware.</b>	Término general aplicado a todo el software que perjudica el comportamiento de una computadora, en español es conocido con el nombre de código malicioso. En esta categoría entran: Virus, Troyanos,



	Backdoors, Worms, Bots, Spyware, Sdware, etc.
<b>Nomenclatura de equipo institucional.</b>	Nombre institucional asignado a los equipos de cómputo, propiedad de la Universidad Veracruzana.
<b>Personal de apoyo técnico/Personal de la DGTI.</b>	<p>Persona con perfil técnico especializado de una entidad académica o dependencia responsable de brindar el soporte técnico a los usuarios.</p> <p>Para efectos del procedimiento quien realiza dichas funciones en la Dirección General de Tecnología (DGTI), es la oficina de Atención de Servicios Tecnológicos en Xalapa y el personal de las Coordinaciones Regionales respectivamente; el personal que brinda estos servicios en las entidades académicas y dependencias se le conoce como personal de apoyo técnico.</p>
<b>Usuario.</b>	Personal que labora en la Universidad Veracruzana, responsable de un equipo de cómputo propiedad de la misma y que solicita el servicio de instalación de la herramienta de cliente de antimalware.

## II. POLÍTICAS DE OPERACIÓN

1. La instalación del cliente antimalware institucional se realiza en equipos de cómputo propiedad de la Universidad Veracruzana con plataforma Microsoft Windows, que cumplan con los siguientes requisitos:
  - 1.1 Equipos de uso administrativo, con red cableada institucional, con nombre estándar y agregados al dominio.
  - 1.2 Equipos de uso académico, con red cableada institucional, con nombre estándar, agregados al dominio y que accedan al Sistema Integral de Información Universitaria (SIIU).
2. En los equipos de Centros de cómputo, Talleres, Laboratorios y Personal académico que no acceda al Sistema Integral de Información Universitaria (SIIU) se debe instalar la versión de Microsoft Windows Defender, además, los equipos deben tener nombre estándar y estar agregados al dominio.
3. En las entidades académicas y dependencias que cuenten con personal de apoyo técnico, serán los responsables de realizar la Instalación de Cliente de Antimalware a los equipos correspondientes.
4. El personal de apoyo técnico debe documentar el servicio en el Formato de Servicio con clave SGSI-GISI-F-022.
5. La revisión del presente documento se llevará a cabo cuando ocurran cambios significativos en la manera de llevarse a cabo el procedimiento.



### III. RESPONSABILIDADES

- **Usuario:**

- Solicitar la instalación del antimalware institucional ante el personal de apoyo técnico responsable de la entidad académica o dependencia o en caso de no contar con uno, se deberá solicitar ante la Oficina de Atención de Servicios Tecnológicos a las coordinaciones regionales de la Dirección General de Tecnología de Información, por medio de oficio, o también consultando mediante los sitios de Hermes (<https://hermes.uv.mx>), la Herramienta para la Gestión de Servicios (<https://servicios.uv.mx>) o correo electrónico institucional.
- Proporcionar como mínimo los siguientes datos:
  - Nombre de la dependencia solicitante.
  - Nombre y cargo de la persona que realiza la solicitud.
  - Cantidad de equipos afectados o que requieran la instalación de cliente de antimalware.
  - Horario disponible en la dependencia para su atención.
  - Número de inventario del equipo de cómputo.
- El traslado del equipo de cómputo es responsabilidad del usuario.

- **Administrador del Centro de servicios.**

- Canalizar el reporte a las áreas de competencia para su atención.
- Dar seguimiento a las solicitudes.

- **Personal de apoyo técnico/Personal de la DGTI.**

- Atender y dar seguimiento a las solicitudes generadas por el usuario.
- El personal adscrito a la Dirección General de Tecnología de Información. Debe documentar el seguimiento en la Herramienta para la Gestión de Servicios, la atención del servicio realizado hasta su conclusión y en el Formato SGSI-GISI-F-022 por cada equipo recibido de acuerdo a los requerimientos solicitados por el usuario.

*[Handwritten signature]*



IV. PROCEDIMIENTO

DESARROLLO

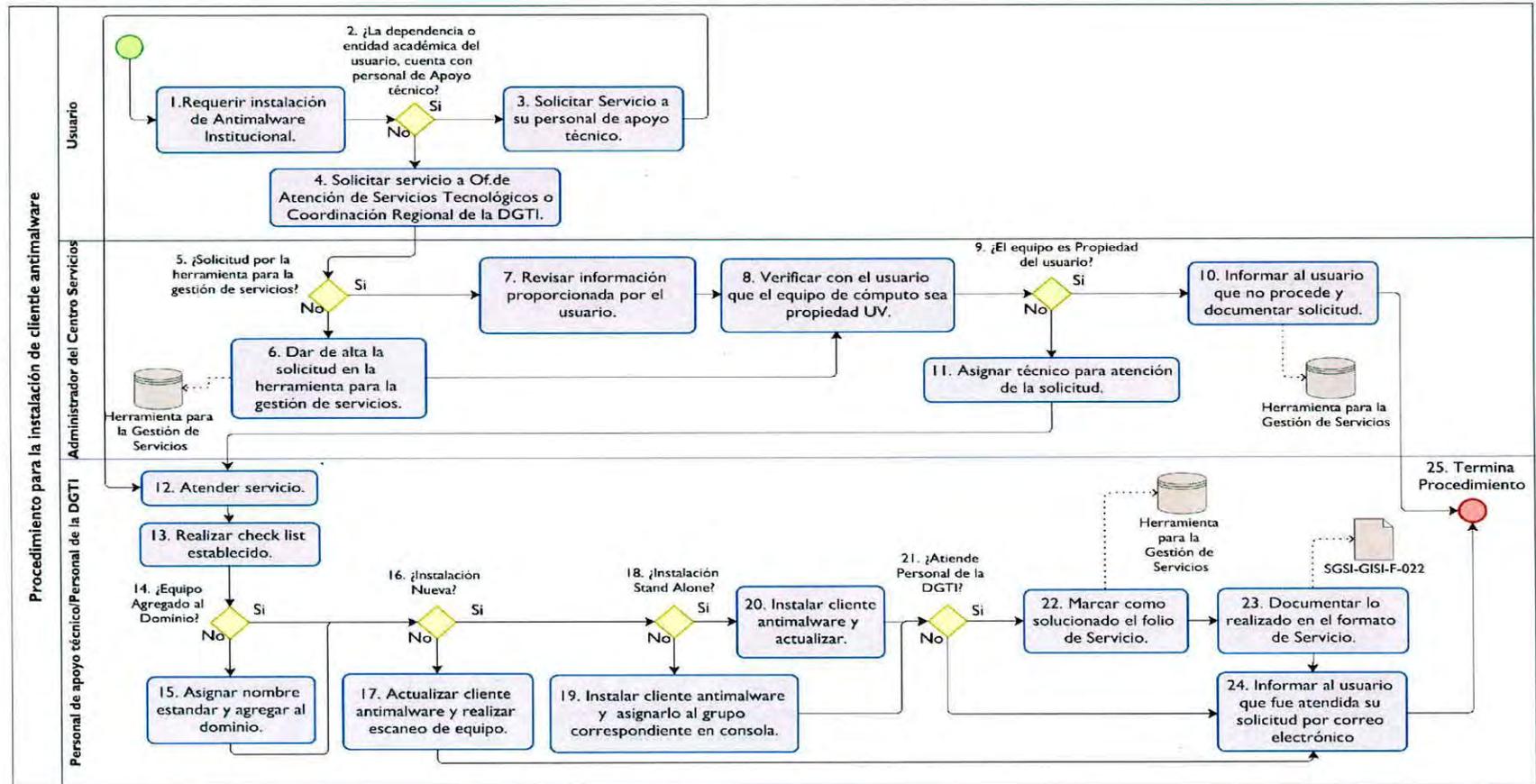
Actividad	Responsable	Descripción de la Actividad
1	Usuario	Requerir instalación de Antimalware Institucional.
2		<p>¿La dependencia o entidad académica del usuario, cuenta con personal de Apoyo técnico?</p> <ul style="list-style-type: none"> <li>• <b>SI</b>, pasar a la <b>actividad siguiente</b>.</li> <li>• <b>No</b>, pasar a la <b>actividad 4</b>.</li> </ul>
3		<p>Solicitar Servicio a su personal de apoyo técnico.</p> <ul style="list-style-type: none"> <li>• Continuar en la <b>actividad 12</b>.</li> </ul>
4		<p>Solicitar el servicio de instalación de cliente de antimalware a la Oficina de Atención de Servicios Tecnológicos o Coordinación Regional de la Dirección General de Tecnología de Información, a través de los medios de solicitud: Oficio, Herramienta para la Gestión de Servicios, Hermes (<a href="https://hermes.uv.mx">https://hermes.uv.mx</a>) o Correo electrónico institucional.</p>
5		<p>¿Solicitud realizada por la Herramienta para la Gestión de Servicios?</p> <ul style="list-style-type: none"> <li>• <b>SI</b>, pasar a la <b>actividad 7</b>.</li> <li>• <b>No</b>, pasar a la <b>actividad siguiente</b>.</li> </ul>
6		Dar de alta la solicitud en la herramienta para la gestión de servicios.
7		Revisar información proporcionada por el usuario.
8	Administrador del Centro de Servicios	Verificar con el usuario que el equipo de cómputo sea propiedad UV.
9		<p>¿El equipo es Propiedad del usuario?</p> <ul style="list-style-type: none"> <li>• <b>SI</b>, pasar a la <b>actividad siguiente</b>.</li> <li>• <b>No</b>, pasar a la <b>actividad 11</b>.</li> </ul>
10		Informar al usuario que no procede y documentar solicitud en el Formato de Servicio. Pasar a la <b>actividad 25</b> .
11		Asignar al Personal de la DGTI la solicitud.
12		Atender servicio.
13		Realizar check list (lista de cotejo) establecido.
14		¿Equipo Agregado al Dominio?



		<ul style="list-style-type: none"> <li>• <b>SI</b>, pasar a la <b>actividad 16</b>.</li> <li>• <b>No</b>, pasar a la <b>actividad siguiente</b>.</li> </ul>
15		Asignar nombre estándar y agregar al dominio.
16		<p>¿Instalación nueva?</p> <ul style="list-style-type: none"> <li>• <b>SI</b>, pasar a la <b>actividad 18</b>.</li> <li>• <b>No</b>, pasar a la <b>actividad siguiente</b>.</li> </ul>
17	Personal de apoyo técnico/Personal de la DGTI	<p>Actualizar cliente antimalware y realizar escaneo de equipo.</p> <ul style="list-style-type: none"> <li>• Pasar a la <b>actividad 24</b>.</li> </ul>
18		<p>¿Instalación Stand Alone?</p> <ul style="list-style-type: none"> <li>• <b>SI</b>, pasar a la <b>actividad 20</b>.</li> <li>• <b>No</b>, pasar a la <b>actividad siguiente</b>.</li> </ul>
19		<p>Instalar cliente antimalware y asignarlo al grupo correspondiente en consola.</p> <ul style="list-style-type: none"> <li>• Pasar a la <b>actividad 21</b>.</li> </ul>
20		Instalar cliente antimalware y actualizar.
21		<p>¿Atiende personal de la DGTI?</p> <ul style="list-style-type: none"> <li>• <b>SI</b>, pasar a la <b>actividad siguiente</b>.</li> <li>• <b>No</b>, pasar a la <b>actividad 24</b>.</li> </ul>
22		Marcar como solucionado el folio de servicio en la herramienta para la gestión de servicios.
23		Documentar lo realizado en el formato de Servicio (SGSI-GISI-F-022)
24		Informar al usuario que fue atendida su solicitud por correo electrónico.
25		<b>Termina Procedimiento.</b>



### DIAGRAMA



## V. REFERENCIAS

- Estatuto General, Título VII, Capítulo III, Sección segunda, Artículo 252, Fracción: X, XII.
- Reglamento para la Seguridad de la Información. Título III, De la Seguridad Física y Lógica de los Activos de Información, Sección tercera, Artículo 51. Detección y Contención de Código Malicioso.
- Código de ética de la Universidad Veracruzana.
- Anexo "A" de la norma ISO/IEC27001:2013 objetivo de control y controles de la Tabla A-I correspondiente, Punto A. 12. "Seguridad en la operativa", Punto A. 12. 2 "Protección contra código malicioso". (No aplica para el SGCUV)
- Cédula de Servicio de instalación de antimalware.
- Herramienta para la gestión de servicios. <https://servicios.uv.mx>.
- Check List de Procedimiento de Cliente Antimalware (lista de cotejo).

## VI. FORMATOS

- SGSI-GISI-F-022 Formato Servicio.

## VII. ATENCIÓN A USUARIOS

De lunes a viernes de 8:00 a 15:00 y 16:00 a 18:00 horas durante todo el año. A excepción de los días marcados en el calendario oficial de la UV de personal de confianza, como no laborables.

- Oficina de Atención de Servicios Tecnológicos(OAST), Lomas del Estadio S/N Edificio E planta baja, Ext: 11502, 11506, 11529 y 11510.
- Coordinación Regional Veracruz, Av. Ruiz Cortines y Juan Pablo II. Edificio USBI Piso 2, Col. Fracc. Costa Verde C.P. 94294, Boca Del Río Ext. 22115.
- Coordinación Regional Orizaba-Córdoba, Poniente 7 # 1383 Col. Centro, C.P. 94300, Orizaba, Ext 33203 y 333205.
- Coordinación Regional Poza Rica-Tuxpan, Blvd. Ruiz Cortines Entre Justo Sierra Y Cedro 306 Col. Obras Sociales, C.P. 93240, Poza Rica, Ext. 41120.
- Coordinación Regional Coatzacoalcos-Minatitlán, Av. Universidad Veracruzana Km 7.5 Edificio USBI, Col. Santa Isabel IA. Etapa C.P. 96538, Ext. 51215

<https://servicios.uv.mx>



### VIII. PREGUNTAS FRECUENTES

**¿Dónde realizo la solicitud del servicio?**

-La solicitud debe realizarse a través de: correo electrónico institucional, oficio (<https://hermes.uv.mx>) o la herramienta para la gestión de servicios (<https://servicios.uv.mx>)

**¿En qué tiempo se atiende mi solicitud?**

-En un periodo de 48 (Cuarenta y ocho) hrs. (Cabe mencionar que las solicitudes fuera de unidad central serán únicamente cuando el área usuaria justifique el servicio en sitio; los gastos de traslado del personal de la DGTI, serán a cargo de la dependencia solicitante. Cualquier asesoría podrá ser atendida vía telefónica o correo electrónico institucional).

**-¿A dónde se entrega el equipo?**

- Oficina de Atención de Servicios Tecnológicos
- Coordinaciones Regionales de TI

**¿Tengo que llevar algo más aparte del equipo para el servicio?**

-No, solo el equipo.

**¿Cuál es el horario de atención?**

-lunes a viernes de 8:00 a 15:00 y 16:00 a 18:00 horas durante todo el año.

A excepción de los días marcados en el calendario oficial de la UV de personal de confianza, como no laborables.

<b>IX. HISTÓRICO DE REVISIONES</b>			
<b>No. DE REVISION</b>	<b>FECHA REVISIÓN O MODIFICACIÓN</b>	<b>SECCIÓN O PAGINA MODIFICADA</b>	<b>DESCRIPCIÓN DE LA REVISIÓN O MODIFICACIÓN</b>
I.	12-Julio-2016	Página 7, Control de Versiones.  Sección I Descripción.  Sección II Políticas de Operación.  Sección IV Procedimiento.  Apartado V. Referencias.	Se actualizó fecha de revisión y versión del documento.  Se actualizó el Nombre de la Oficina de Atención de Servicios Tecnológicos.  Se actualizaron las políticas de operación.  Se actualizó el diagrama de flujo y apartado de desarrollo conforme a las adecuaciones del diagrama de flujo.  Se modifican las referencias.
II.	19-Agosto-2016.	Página 8: Control de versiones.	Se actualiza la versión y fecha del procedimiento.
III.	11-October-2016.	Apartado V. Referencias.	Se añadió en anexo A-12.
IV.	09-Febrero-2017.	Sección II. Políticas de Operación.  Sección IV Procedimiento.	Se modificó las políticas de operación.  Se actualizó el diagrama de flujo y apartado de desarrollo conforme a las adecuaciones del diagrama de flujo.
V	12-Septiembre-2019.	Revisión completa.	Actualización completa en todos los apartados.
VI	15-Marzo-2024	Revisión completa.	Actualización completa en todos los apartados.
VII	20-Enero-2025	Revisión completa	Actualización completa en todos los apartados por cambio de nombre y titular

*[Handwritten signature and mark]*

Control de versiones

<b>X. CONTROL DE VERSIONES</b>				
CÓDIGO	FECHA		VERSIÓN	NIVEL DE CONFIDENCIALIDAD
	VERSIÓN O AUTORIZACIÓN	ENTRADA EN VIGOR		
SGSI-GISI-P-008	07-febrero-2025	12-febrero-2025	V 8.0	Público
CREADO POR:			AUTORIZADO POR:	
 Lic. Alberto Mesa Huerta Jefe de Oficina de Atención de Servicios Tecnológicos			 Mtro. Rafael Gómez Quezada Director de Servicios Informáticos Administrativos	

Las firmas avalan y dan validez de la autenticidad del documento, así mismo aprueban su publicación para su implementación.

**XI. CRÉDITOS.**

La elaboración del presente Procedimiento estuvo a cargo de la Oficina de Atención de Servicios Tecnológicos y la Dirección de Servicios Informáticos Administrativos de la Dirección General de Tecnología de la Información. Fue concluido y autorizado en febrero de 2025, para su publicación en el manual de Procedimientos Administrativos.

Mtro. Rafael Gómez Quezada.  
Director de Servicios Informáticos Administrativos.

Lic. Alberto Mesa Huerta.  
Jefe de Oficina de Atención de Servicios Tecnológicos.