SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

INDICE

I. DESCRIPCIÓN

OBJETIVO

Identificar y atender vulnerabilidades cibernéticas en los activos de Tecnologías de Información (TI) que apoyan a los servicios digitales de la Universidad Veracruzana.

ALCANCE

Este procedimiento está dirigido al personal del CSIRT y/o los responsables de administrar los activos de TI que se encuentran alojados en los sites de telecomunicaciones bajo el control de la Dirección General de Tecnología de Información de la Universidad Veracruzana.

DEFINICIONES.

Activo de TI	Cualquier recurso tecnológico que la Universidad Veracruzana utiliza para gestionar y prestar sus servicios informáticos mediante la red de telecomunicaciones.
Administrador de área de TI	Personal responsable de un área que administra algún servicio alojado en la infraestructura tecnológica de la Universidad Veracruzana.
CVSS	Estándar de la industria que clasifica la criticidad de las vulnerabilidades informáticas (Common Vulnerability Scoring System (CVSS, por sus siglas en inglés).
DGTI	Dirección General de Tecnología de Información de la Universidad Veracruzana
Herramienta para la Gestión de Servicios	Punto de contacto para el registro, seguimiento, control y solución de servicios tecnológicos que ofrece la Dirección General de Tecnología de Información a la comunidad universitaria.

Incidente de ciberseguridad	La violación o potencial amenaza de violación a la seguridad de la información, como acceso no autorizado, robo de contraseñas, robo de información y alteración de información, entre otros.
UV-CSIRT	Equipo de Respuesta a Incidentes de Ciberseguridad coordinado por el Departamento de Seguridad y Monitoreo de la Universidad Veracruzana.
Mitigación de vulnerabilidades	Implementación de medidas de seguridad que reducen la probabilidad de explotar una vulnerabilidad.
Remediación de vulnerabilidades	Implementación de medidas de seguridad que eliminan una vulnerabilidad.
Ticket	Folio único de seguimiento de vulnerabilidades que se crea en la Herramienta para la Gestión de Servicios.
Vulnerabilidad	Es una debilidad en los Activos de TI que potencialmente permite que una amenaza se materialice.

II. POLÍTICAS DE OPERACIÓN

1. Con base en el Reglamento de la Seguridad de la Información vigente, los mecanismos y estrategias para la prevención, identificación y mitigación de incidentes de ciberseguridad serán implementados por la Dirección General de Tecnología de Información a través del UV-CSIRT;

2. El calendario para la ejecución del análisis, remediación y validación de vulnerabilidades:
   - Será establecido por el UV-CSIRT bajo un plan de trabajo para la identificación y atención de vulnerabilidades el cual contemplará al menos 2 periodos por año;
   - UV-CSIRT se encargará de compartir vía correo electrónico institucional, el plan de trabajo, al Administrador de área de TI;

3. UV-CSIRT notificará al Administrador de área de TI, vía correo electrónico institucional, recordatorio una semana previa a la ejecución del análisis de vulnerabilidades ;

4. El UV-CSIRT creará y asignará al Administrador de área de TI un ticket en la Herramienta para la Gestión de Servicios por cada activo de TI que tenga vulnerabilidades críticas y/o altas;

5. El Administrador de área de TI podrá solicitar análisis de vulnerabilidades para validar avances en la remediación de las vulnerabilidades atendidas siempre y cuando esté en los tiempos establecidos para cada periodo en el plan de trabajo y con un mínimo de 8 días hábiles previos al vencimiento;

6. El Administrador de área de TI debe cerrar el ticket cuando haya atendido todas las vulnerabilidades críticas y/o altas informadas, y debe documentar las acciones de remediación o mitigación realizadas por cada vulnerabilidad reportada.

7. Para las vulnerabilidades que no puedan ser remediadas, se deberán documentar en el ticket las acciones de mitigación realizadas junto con la leyenda "El responsable del activo de TI acepta el riesgo", siendo estas excluidas de la generación de tickets futuros;

8. UV-CSIRT cerrará los tickets que no fueron atendidos durante el tiempo establecido en el calendario del plan de trabajo, con la leyenda "Cerrado por Caducidad, el responsable del activo de TI acepta el riesgo";

9. El Administrador de área de TI podrá solicitar vía correo electrónico institucional un análisis de vulnerabilidades extemporáneo al plan de trabajo definido para los activos de TI bajo su control, coordinando con el UV-CSIRT los tiempos de atención;

10. La información resultante de los análisis de información se considera confidencial;

11. Las vulnerabilidades se clasifican en críticas, altas, medias, bajas e informativas de acuerdo con el CVSS.

12. Este documento solo se actualizará en caso de que exista algún cambio significativo en el proceso de gestión de las vulnerabilidades de los activos de TI institucionales.

III. RESPONSABILIDADES

UV-CSIRT

- Realizar plan de trabajo para establecer los tiempos de ejecución, remediación y validación de los análisis de vulnerabilidades.
- Socializar el plan de trabajo a la persona titular de la DGTI y sus direcciones, así como al Administrador de área de TI.
- Realizar la ejecución de los análisis de vulnerabilidades a los activos de TI pertenecientes a la Universidad Veracruzana.
- Compartir por correo electrónico al Administrador de área de TI correspondiente los siguientes documentos:
    1. Informe general de vulnerabilidades, que contiene el detalle de las vulnerabilidades críticas, altas, medias, bajas e informativas encontradas en todos

los activos de TI bajo su tramo de control con recomendaciones para su remediación.

2. Informe concentrado de vulnerabilidades, que contiene el detalle de las vulnerabilidades críticas y/o altas encontradas en todos los activos de TI bajo su tramo de control con recomendaciones para su remediación.

- Crear y asignar al Administrador de área de TI un ticket en la Herramienta para la Gestión de Servicios para cada activo de TI con vulnerabilidades críticas y/o altas, incluyendo nombre de la vulnerabilidad, Sinopsis, descripción y solución.
- Brindar apoyo a los Administradores de área de TI durante las etapas de la gestión de vulnerabilidades.
- A solicitud del Administrador de área de TI realizar análisis de validación y compartirle mediante correo electrónico el informe concentrado de vulnerabilidades, indicando si las vulnerabilidades críticas o altas fueron corregidas con las acciones de remediación implementadas.
- Dar seguimiento al cierre oportuno de los tickets en la Herramienta para la Gestión de Servicios.
- Informar a la DGTI el estatus y avances que se tiene en la atención de tickets y la gestión de vulnerabilidades, así la como la creación de un reporte al final de cada periodo establecido en el plan de trabajo.
- Mantener la confidencialidad de la información que se gestiona.

Administrador del área de TI

- Atender todas las vulnerabilidades registradas y asignadas en los tickets en la Herramienta para la Gestión de Servicios.
- Con la finalidad de minimizar los riesgos de ciberseguridad en los activos de TI que gestiona, deberá analizar y realizar las acciones que considere para las vulnerabilidades compartidas en el informe general de vulnerabilidades.
- Apoyar al UV-CSIRT durante las etapas de planeación y ejecución de análisis de vulnerabilidades;
- Documentar las acciones de remediación y acciones de mitigación en la bitácora pública del ticket asignado.
- Solicitar por correo electrónico a UV-CSIRT que se realice el análisis de validación para verificar que las acciones de remediación o mitigación implementadas hayan sido aplicadas correctamente.
- Cerrar ticket en Herramienta para la Gestión de Servicios en cuanto se hayan remediado o mitigado todas las vulnerabilidades críticas y/o altas del activo de TI

reportado y confirmado por el UV-CSIRT.

- El Administrador de área de TI podrá compartir los tickets asignados a personal técnico bajo su cargo para la atención y seguimiento, sin embargo, mantendrá la responsabilidad del cierre de estos en la herramienta para gestión de servicios.
- Preservar la confidencialidad de la información que le sea compartida por UV-CSIRT.

IV. PROCEDIMIENTO

DESARROLLO

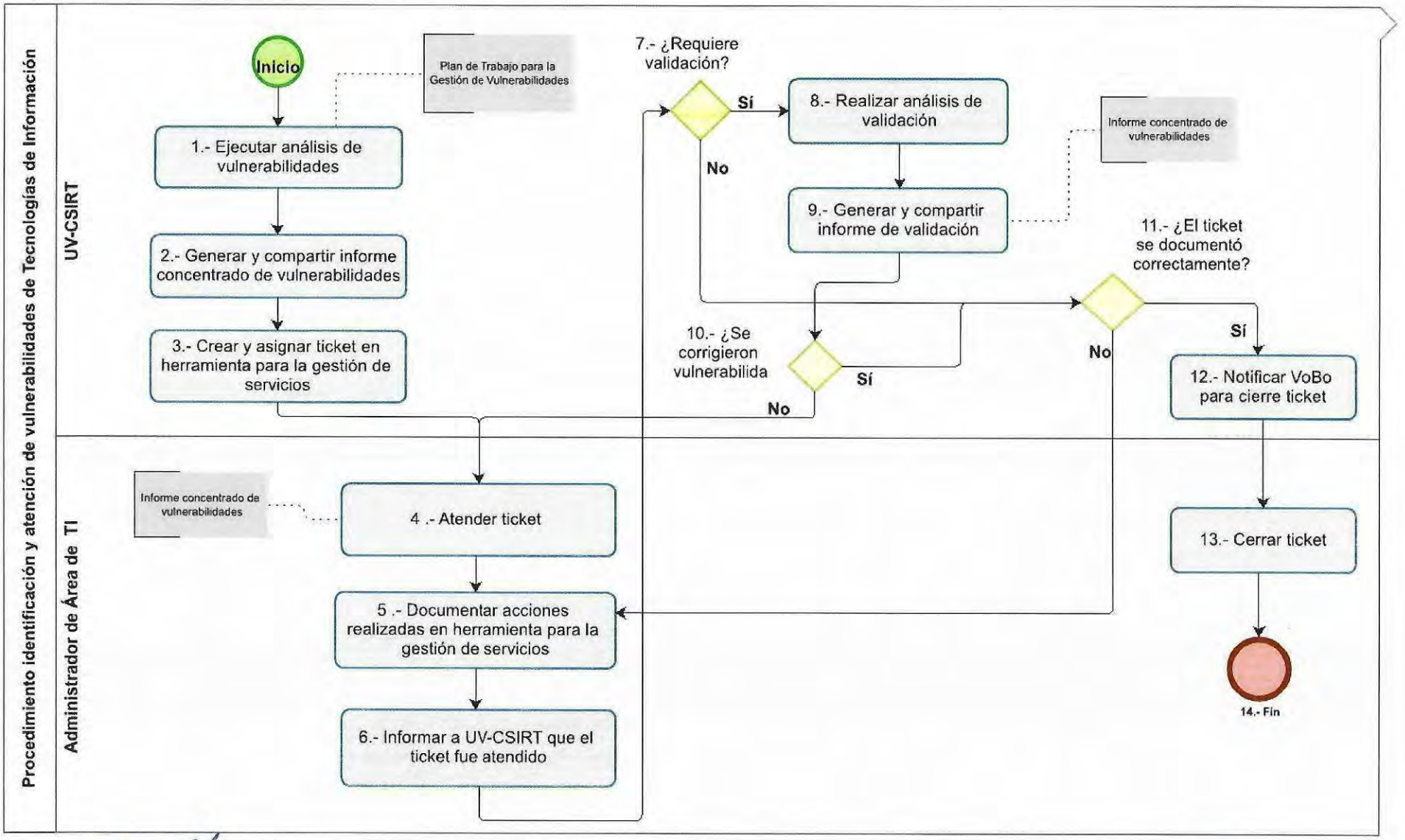
Actividad	Responsable	Descripción de la Actividad
1	UV-CSIRT	• Ejecutar análisis de vulnerabilidades de acuerdo con el Documento Plan de trabajo o solicitud de análisis de vulnerabilidades.
2		• Generar y compartir informe de análisis de vulnerabilidades y reporte con sugerencias de remediación al Administrador de área de TI.
3	Administrador de área de TI	• Crear y asignar ticket en Herramienta para la Gestión de Servicios.
4		• Atender ticket
5		• Documentar las acciones realizadas en Herramienta para la Gestión de Servicios.
6		• Informar a UV-CSIRT ticket atendido.
7	UV-CSIRT	• ¿Requiere validar las acciones de remediación? o Sí, pasar actividad 8. o No, pasar a la actividad 11
8		• Realizar análisis de vulnerabilidades para validar las acciones realizadas por el administrador de área de TI.
9		• Genera y comparte informes de validación.
10		• ¿Se corrigieron las vulnerabilidades? o Sí, pasar actividad 11. o No, pasar actividad 4.
11		• ¿El ticket se documentó correctamente? o Sí, pasar actividad 12.

		○ No, pasar actividad 5.
12	Administrador de área de TI	• Notifica de visto bueno para cerrar ticket
13		• Cierra ticket
14		• Fin de proceso.

Universidad Veracruzana
Dirección General de Tecnología de Información

UNIVERSIDAD VERACRUZANA

Procedimiento Identificación y atención de vulnerabilidades de Tecnologías de Información SGSI-SO-P-041



V. REFERENCIAS

- Reglamento para la Seguridad de la Información Capítulo VII "De la ciberseguridad" https://www.uv.mx/legislacion/files/2019/12/Seguridad-de-la-Informacion-2019-Gaceta.pdf;
- ISO/IEC 27001:2022 Anexo A Tabla A.1, Control 8.7 "Gestión de vulnerabilidades técnicas"
- NIST SP 800-53 RA-5 Vulnerability Monitoring and scanning
- FIRST CSIRT Services Framework Versión 2.1, punto 7 Service Area: Vulnerability Management

VI. ANEXO

N/A

VII. ATENCIÓN A USUARIOS

Departamento de Seguridad y Monitoreo, Lomas del Estadio s/n. Zona Universitaria Edificio "E" 1er. Piso.

Teléfono: (228) 8421700 Ext. 11535 y 11536.

Correo electrónico: contactocsirt@uv.mx

Lunes a viernes de 9:00 a 15:00 y 16:00 a 18:00 horas a excepción de los días marcados en el calendario oficial de la UV como no laborales.

VIII. PREGUNTAS FRECUENTES

¿Puedo solicitar un análisis de vulnerabilidades?

R: Actualmente los análisis de vulnerabilidades solo realizan bajo un plan de trabajo establecido por el Departamento de Seguridad y Monitoreo (UV-CSIRT) hacia los activos de TI que se encuentren alojados en los sites institucionales.

¿Cómo se priorizan las vulnerabilidades encontradas?

R: Se utiliza el sistema de puntuación mundialmente conocido CVSS para evaluar la severidad de las vulnerabilidades.

¿Puedo solicitar información de los análisis de vulnerabilidades de activos de TI que no soy responsable?

R: No, esta información es confidencial y su divulgación podría poner en riesgo la seguridad de los activos de TI de la Universidad Veracruzana.

IX. ENTRADAS Y SALIDAS

Entradas		Salidas	
Proveedor	Requisitos	Receptor	Requisitos
1.UV-CSIRT	1.1 Plan de trabajo 1.2 Informe concentrado de vulnerabilidades	1.Administrador de área de TI	1.1 Ticket en Herramienta para la Gestión de Servicios con vulnerabilidades críticas y/o altas. 1.3 Ticket en Herramienta para la Gestión de Servicios cerrado con documentación correcta.

Histórico de Revisiones

No. DE REVISION	FECHA REVISIÓN O MODIFICACIÓN	SECCIÓN O PAGINA MODIFICADA	DESCRIPCIÓN DE LA REVISIÓN O MODIFICACIÓN
0			

Control de versiones

CÓDIGO	FECHA		VERSIÓN	NIVEL DE CONFIDENCIALIDAD
	VERSIÓN O AUTORIZACIÓN	ENTRADA EN VIGOR		
SGSI-SO-P-041	10/feb/2025	15/feb/2025	1.0	Público

CREADO POR:	AUTORIZADO POR:
LIC. Rigo Daniel Salazar Falfán Jefe de Departamento de Seguridad y Monitoreo	MRT. Héctor Bonola Virués Director de la Dirección de Servicios de Red e Infraestructura Tecnológica.

X. CRÉDITOS

La elaboración del presente Procedimiento estuvo a cargo del Departamento de Seguridad y Monitoreo y la Dirección de Servicios de Red e Infraestructura Tecnológica dependiente de la Dirección General de Tecnologías de la Información, fue concluido y autorizado el 10 de febrero del 2025, para su publicación en el Manual de Procedimientos Administrativos.

Mtra. María Dacia González Cruz
Directora General de Tecnología de Información
Mtro. Héctor Bonola Virues
Director de Servicios de Red e Infraestructura Tecnológica
Lic. Rigo Daniel Salazar Falfán
Jefe de Departamento de Seguridad y Monitoreo
Mtro. Juan León Toral
Técnico en Seguridad