Ciberseguridad
UV-CSIRT

TLP: CLEAR

Protocolo de reporte de incidentes de ciberseguridad en la Universidad Veracruzana

Definición:

Un incidente de Ciberseguridad es un evento o serie de eventos inesperados o no deseados, que compromete las operaciones de la universidad; provocando la pérdida o uso indebido de información, así como la interrupción parcial o total de los servicios tecnológicos.

Incidentes más comunes:

Malware: también conocido como "software malicioso" es todo aquel programa, aplicación o código que invade y daña un sistema interfiriendo con su funcionamiento normal, intentado tomar el control total o parcial de él para ejecutar acciones sin el conocimiento del usuario.

Hay algunos comportamientos en tu equipo que pueden ayudarte a conocer si tu equipo está infectado por algún tipo de malware, estos son algunos:

1. Utilización de recursos del sistema (CPU y RAM) es elevada de forma anormal;
2. Bloqueos constantes del sistema incluso mostrando la conocida "pantalla azul";
3. La aparición de ventanas emergentes masivas con anuncios publicitarios;
4. Reducción sospechosa de espacio en disco o memoria interna del dispositivo;
5. El equipo trabaja de una manera más lenta de lo habitual sin motivo alguno;
6. El programa antivirus deja de funcionar o no puede actualizarse;
7. Aparición inesperada en el navegador de nuevas barras de tareas, extensiones o complementos;
8. Desaparición inesperada de información almacenada en el dispositivo;
9. En el caso del malware tipo ransomware, los cibercriminales informan que tienen tu información o que la han hecho inaccesible y solicitan dinero como rescate para liberarla.

Phishing o Spam: Los correos no solicitados, deseados o de remitentes que intentan engañar a los usuarios para obtener información personal, se consideran no deseados, phishing o spam.

La mayoría de los correos fraudulentos, tienen algunas características que nos permiten estar alerta y reconocer que se trata de una estafa o de publicidad masiva.

Algunos de estas se describen a continuación:

1. Remitente desconocido.
2. Correo inesperado que sugiere pertenecer a una institución reconocida.
3. El asunto del correo capta la atención para hacerlo parecer importante.
4. Comunicación con un sentido de urgencia, miedo, extorsión o gratificación.
5. Contenido solicita realizar alguna acción como descargar un archivo, ingresar información a alguna liga o responder el correo.
6. Contenido con mala redacción, faltas de ortografía, o incluso parecen una mala traducción de otro idioma.
7. Correo con publicidad o información no solicitada.

Robo de cuenta y la suplantación de identidad: son prácticas maliciosas relacionadas con la seguridad en línea:

- El robo de cuenta ocurre cuando alguien obtiene acceso no autorizado de inicio de sesión, como usuario y contraseña, para acceder a tus cuentas.
- La suplantación de identidad es cuando un individuo se hace pasar por otra persona para realizar actividades ilícitas o mal intencionadas.

Algunos indicios de que tu cuenta ha sido comprometida o alguien está suplantando tu identidad incluyen:

1. Actividad inusual como inicios de sesión desde ubicaciones desconocidas o dispositivos no reconocidos.
2. Cambios en la configuración como modificaciones en la contraseña, dirección de recuperación o configuración de seguridad.
3. Correos electrónicos o mensajes no enviados por ti.
4. Contactos eliminados o modificados.
5. Modificaciones en la configuración de las bandejas de correo electrónico.
6. Recibes notificaciones sobre modificaciones que no hiciste.
7. Reporte de tus contactos que han recibido mensajes desde tu cuenta sin que tú los hayas enviado.
8. Inaccesibilidad a los servicios permitidos con mi cuenta.

Objetivo:

Informar a la comunidad universitaria de la Universidad Veracruzana el proceso a seguir para reportar un incidente de ciberseguridad.

Alcance:

Aplica para toda la Comunidad Universitaria.

Medidas preventivas de seguridad Generales:

- ¡Ser precavido!, leer atentamente el remitente, si no se espera recibir un correo de dicho remitente, usar el sentido común.
- No confiar únicamente en el nombre del remitente, verificar que el propio dominio del correo recibido es de confianza.
- Si se sospecha que el correo es fraudulento no abrir los enlaces.
- Analizar el enlace, situar el cursor encima del enlace para ver la URL real a la que dirige. Si no coincide con el dominio de la institución que supuestamente envía el correo, o es una web sin certificado de seguridad, no dar clic.
- No descargar ni abrir los archivos adjuntos de correos que parezcan sospechosos.
- Crear filtros para aquellos correos que se desconozcan, así la próxima vez que se vuelvan a recibir, no estarán en la bandeja de entrada.
- Revisar la redacción y buscar errores de ortografía y gramaticales, o si parece una mala traducción, sospeche.

- Mantener actualizado su equipo de cómputo, así como el antivirus. Las versiones más recientes de Windows 10 traen incorporado un antivirus “Windows Defeder” o “Microsoft Defender” que se actualiza diariamente.
- Si recibe un correo sospecho de un remitente con dominio de una institución conocida, repórtelo directamente al área de seguridad de su institución.
- Utilizar contraseñas seguras y únicas en cada una de sus cuentas
- Configurar adecuadamente la privacidad de nuestros dispositivos y cuentas en línea.

Proceso de reporte de incidentes de ciberseguridad:

Si has sido víctima de algún incidente de Ciberseguridad o sospechas que lo eres, sigue los pasos siguientes:

1. Documenta el incidente, describe brevemente la situación con fecha y hora de la detección y cualquier evidencia que apoye al diagnóstico.
2. Para servicios de terceros externos al control de la Universidad Veracruzana

Por ejemplo:	Reporta:
Redes sociales (Facebook, Instagram, X, etc.)	• A la plataforma afectada en la sección de ayuda o Políticas y reportes. • A la Unidad de la Policía Científica Preventiva del Estado de Veracruz al teléfono 086
Servicios de correo electrónico (Hotmail, Gmail, etc.)	
Servicios de almacenamiento en línea (Dropbox, Megaupload, etc.)	
Equipos de cómputo no institucionales.	
Entre otros servicios de terceros.	

3. Para servicios de la Universidad Veracruzana

Por ejemplo:	Casos:	Reporta:
Correo electrónico institucional (cuenta@uv.mx)	Recepción de correo spam o phishing.	• Reenviando el correo electrónico reportaspam@uv.mx • Realiza tu registro mediante la página https://www.uv.mx/csirt/reporta-un-incidente-de-ciberseguridad/
	Robo de cuenta o suplantación de identidad	• Por correo electrónico a contactocsirt@uv.mx • Realiza tu registro mediante la página https://www.uv.mx/csirt/reporta-un-incidente-de-ciberseguridad/ • Llamando al (228) 8 421700, Ext. 11532
Equipos de cómputo institucionales.	Virus, Malware, comportamiento anómalo.	
Servicios institucionales (RIUV, HERMES, entre otros).	Ciberataques a los servicios como denegaciones, accesos no permitidos, entre otros.	

Una vez que se reciba el reporte, se procederá al análisis correspondiente, estableciendo contacto con el usuario para dar seguimiento al reporte.

Si requiere apoyo o asesoría en la materia, comunicarse al teléfono 2288421700 ext. 11532 en un horario de 09:00 a 15:00 hrs. y de 16:00 a 20:00 hrs.

Por último, lo invitamos a **seguir las recomendaciones que emite el UV-CSIRT de la Universidad Veracruzana a través del portal Infosegura.**