¿Qué hacer en caso de detectar un ciberincidente?

¿Qué es un ciberincidente (o incidente de seguridad)?

Es una acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traduce en un efecto real o potencialmente adverso sobre un sistema de información, la información que trata o los servicios que presta.

(spam, mal uso de contraseñas, phishing, suplantación de identidad, contenido difamatorio o discriminatorio, software malicioso, ingeniería social, uso de software sin licencia, pérdida o robo de dispositivo, pérdida de datos, incumplimiento de política o de normativa de seguridad de la información del Ministerio,…)

¿Qué debo hacer ante un evento con rasgos de ciberincidente?

Notificar el evento a la Unidad de Seguridad de la Subdirección General TIC mediante correo electrónico a la dirección **seguridad.tic@educacion.gob.es**

¿Qué hace el Responsable de Seguridad después de la notificación de un ciberincidente?

1. Notificación del usuario a **seguridad.tic@educacion.gob.es**
2. Registro del incidente en la herramienta LUCIA de gestión de incidentes de seguridad en las Administraciones Públicas
3. Valoración de la información remitida por el usuario: Contacto con usuarios o responsables afectados; análisis técnico de dispositivos afectados;…
4. Investigación del incidente; recopilación de evidencias
5. Aplicación de medidas de contención del incidente
6. Resolución del incidente y comunicación a responsables y usuarios afectados
7. Lecciones aprendidas del incidente

NIPO: 847211246