RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/34172 **09/02/2026** **98767**

AUTOR/A: GONZÁLEZ-ROBATTO PEROTE, Jacobo (GVOX); HERNÁNDEZ QUERO, Carlos (GVOX); RAMÍREZ DEL RÍO, José (GVOX)

RESPUESTA:

En relación con el asunto interesado y según ha informado el Centro de Operaciones de Ciberseguridad de la Agencia Estatal de Administración Digital, se indica que se produjo un incidente relacionado con la plataforma ACCEDA1 los días 1 y 2 de febrero. El mismo 2 de febrero se procedió a cerrar de forma inmediata el acceso a la sede electrónica del Ministerio de Ciencia, Innovación y Universidades y comenzaron las investigaciones sobre lo sucedido.

El incidente quedó caracterizado como una exfiltración limitada de documentos mediante abuso de 3 credenciales previamente robadas, sin evidencia de explotación masiva de IDOR ni de volcado de BBDD (base de datos), con el impacto concentrado en la confidencialidad de información de expedientes específicos.

El acceso externo a la aplicación se ha vuelto a abrir el 25 de febrero, tras haber implantado un refuerzo en los mecanismos de autenticación mediante un nuevo sistema de acceso mediante usuario y contraseña con doble factor de autenticación (2FA), con el objetivo de reforzar la seguridad y proteger la información gestionada en la subsede.

Por otro lado, el Ministerio de Ciencia, Innovación y Universidades se ha puesto en contacto con la Guardia Civil para denunciar los hechos.

Además, el Ministerio del Interior señala que el Ministerio de Ciencia, Innovación y Universidades no ostenta la condición de operador de servicios esenciales, por lo que no es competente en la gestión directa de incidentes de ciberseguridad en los términos previstos en la normativa aplicable.

Por otra parte, se informa de que no constan el incidente mencionado ni la existencia de una brecha de seguridad verificada. La información disponible proviene de fuentes abiertas y carece, hasta la fecha, de elementos que permitan acreditar su autenticidad. La determinación precisa del momento de detección inicial correspondería en su caso, al órgano titular del sistema afectado y al CSIRT (Computer Security Incident Response Team) competente que gestione técnicamente el incidente.

Madrid, 18 de marzo de 2026