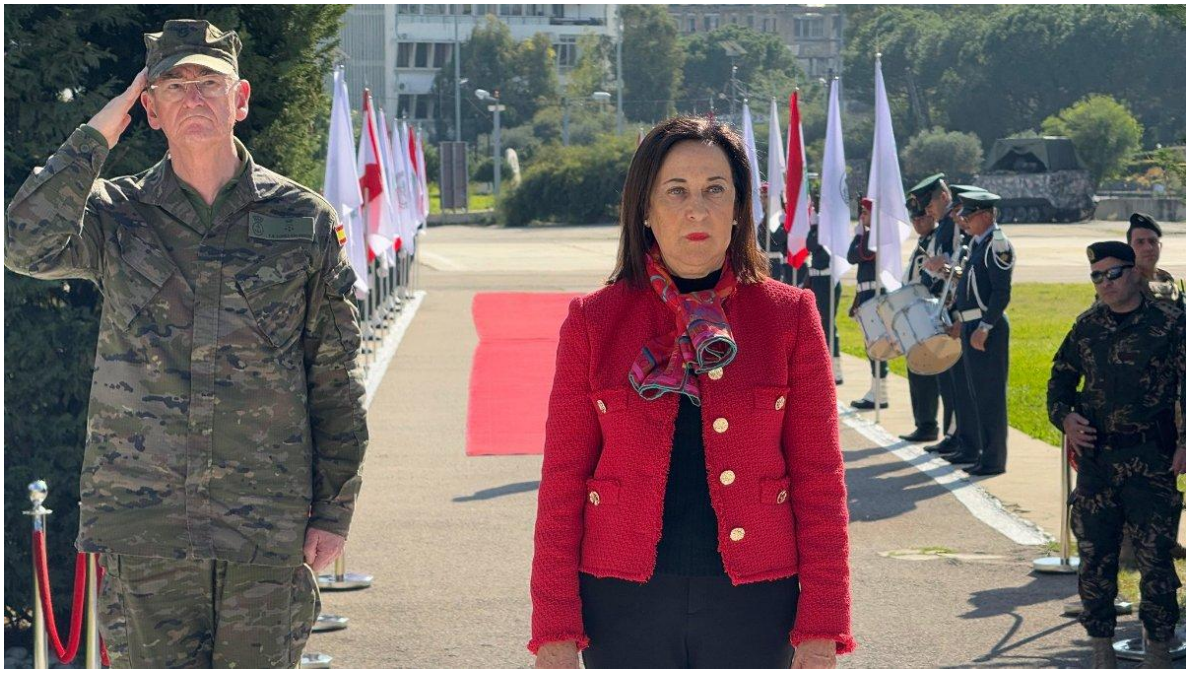
https://theobjective.com/espana/politica/2025-01-29/defensa-correo-robo-datos-militares-guardia-civiles/

Defensa admite en un correo interno el robo de datos a miles de guardias civiles y militares

El ministerio anuncia medidas de «mitigación» tras filtrarse nombres y correos oficiales en un foro de ciberdelincuentes



La ministra de Defensa, Margarita Robles, junto al jefe del Estado Mayor de la Defensa (Jemad), almirante Teodoro López Calderón, en su última visita a Líbano. | Foto: Flickr M.Defensa

- **Antonio Rodríguez**
@antonioRG9ar@theobjective.com

Publicado: 29/01/2025 • 04:30Actualizado: 29/01/2025 • 10:11

El Ministerio de Defensa ha admitido en un correo interno al que ha tenido acceso THE OBJECTIVE el robo cibernético de información sobre datos personales que afectaría **a alrededor de 160.000 guardias civiles y militares**. El departamento de **Margarita Robles** asegura que se han tomado «las medidas de **mitigación y prevención adecuadas** que establece la legislación».

La circular interna se envió el pasado domingo desde el **Centro de Sistemas y Tecnologías de la Información y las Comunicaciones** (CESTIC), el organismo dirigido por el teniente general **José María Millán Martínez** que se encarga de proteger la llamada **Infraestructura Integral de Información para la Defensa** (I3D en la jerga interna). Para ello, este departamento tiene asignadas las competencias en ciberseguridad para el blindaje del **Centro de Atención al Usuario** (CAU) del que disponen las Fuerzas Armadas. El director del CESTIC tiene el cargo de **oficial jefe de la Información** dentro del ministerio.

«Aclaración de información aparecida en redes», se indicó en el asunto del mensaje distribuido el 26 de enero. «En relación con **cierta información aparecida en algunos medios de comunicación** se informa que el Ministerio de Defensa ha tomado las medidas de mitigación y prevención adecuadas que establece la legislación», se señala en dicho correo después de que *eldiario*.es desvelase una filtración masiva que expuso la identidad de al menos 160.000 guardias civiles y militares. La información provenía, supuestamente, de **bases de datos robadas a uno de sus proveedores**.

«También está circulando cierta información, **carente de todo rigor**, que alerta de posibles modificaciones **malintencionadas** de datos personales **muy sensibles** de los usuarios del Ministerio de Defensa. Se ha constatado que estas informaciones **carecen de veracidad y son infundadas**», indicó el CESTIC antes de subrayar que el Ministerio de Defensa «establece **unos plazos máximos** de validez de contraseñas, que **garantizan la seguridad** de los accesos a sus servicios y aplicaciones».

Con ello se pretendía **tranquilizar** a los destinatarios de la circular. Sin embargo, el lunes apareció un documento castrense en Ciudadanos de Uniforme -un canal anónimo que suma 24.200 seguidores y donde se difunden mensajes de miembros de las Fuerzas Armadas que critican decisiones de sus superiores y denuncian supuestas irregularidades en sus unidades y cuarteles- en el que **se instaba a cambiar de contraseña**.

En concreto, se trataba de un correo de la secretaría general del Ala 49 del Ejército del Aire en el que se confirmaba «**una filtración de datos sensibles**» en el campus virtual antiguo y se recomendaban dos actuaciones a todo el personal de la unidad ubicada en la base balear de Son San Juan. Primero, renovar la contraseña. Y segundo, comprobar en el expediente de la nómina que el IBAN bancario de cada uno «**no haya sido alterado**».

«Esto es **extremadamente grave** y debería ser denunciado. No podemos permitir que jueguen con nuestros datos personales», se indicó desde este canal anónimo de Telegram antes de lanzar la pregunta al aire de si los datos robados «**se filtraron o se han vendido**» a ciberdelincuentes.

Nombres y correos oficiales

La supuesta filtración tuvo su origen **en un foro de ciberdelincuentes**, donde actores no identificados pusieron a la venta **tres bases de datos** con información relativa a la identidad de 160.000 guardias civiles y militares, según *eldiario.es*. Dos de ellas contenían los nombres y correos electrónicos de miembros de la Guardia Civil y la otra, de personal de las Fuerzas Armadas y el Ministerio de Defensa.

A pesar de que no contenía datos sensibles como contraseñas o credenciales, este tipo de filtraciones expone a los afectados y sus familias **a riesgos de seguridad**. Los ciberdelincuentes pueden utilizar dichos datos para realizar ataques de *phishing* personalizados, suplantar identidades, identificar a personal en misiones sensibles, elaborar perfiles para chantaje o extorsión, y también pueden comprometer sistemas de comunicación e información oficial.

Fuentes militares consultadas por THE OBJECTIVE han admitido la filtración de datos. En lo que se refiere a soldados y oficiales, contenía **el nombre completo y el correo oficiales** de cada uno de ellos en Defensa. A todos los potenciales afectados les une el haber pasado unos cursos de formación por la plataforma que ha sido 'hackeada'.

- **Antonio Rodríguez**
@antonioRG9ar@theobjective.com
Antonio Rodríguez (Madrid, 1976) es jefe de Redacción y miembro del Comité Editorial. Estudió Periodismo en la Universidad Complutense de Madrid.