COMUNICADO

Gobierno de Gibraltar

El Gobierno confirma que el incidente de ciberseguridad ha sido contenido, tras la aplicación de medidas de seguridad exhaustivas

Gibraltar, 9 November 2026

El Gobierno Gibraltar informa de que ha estado gestionando un incidente de ciberseguridad que ha afectado a algunos componentes de su entorno informático basado en la nube.

El incidente, originado hace varias semanas, consistió en un acceso no autorizado al entorno en la nube del Gobierno, que incluye servicios como Microsoft Outlook, Teams, SharePoint y OneDrive. Tras recibir una alerta de Microsoft sobre una posible filtración de datos, el Departamento de Tecnología de la Información y Logística (Information Technology and Logistics Department, ITLD) del Gobierno comenzó de inmediato a trabajar para contener la amenaza, proteger los sistemas afectados y reforzar las medidas de seguridad existentes.

El Gobierno ha estado colaborando estrechamente con Microsoft y con el Centro Nacional de Ciberseguridad del Reino Unido (National Cyber Security Centre, NCSC), que ha coordinado el apoyo especializado en ciberseguridad. Un equipo de expertos de organizaciones asociadas al NCSC viajó a Gibraltar el lunes 2 de noviembre para trabajar directamente junto al ITLD en la investigación y la respuesta.

El viernes 6 de noviembre, el Gobierno suspendió algunos servicios para permitir que se llevara a cabo una investigación forense y se aplicaran medidas de seguridad adicionales. El Gobierno pide disculpas por las molestias causadas.

El ITLD y los equipos especializados han llevado a cabo medidas exhaustivas para contener el incidente y han implantado garantías de seguridad adicionales. El ITLD sigue vigilando la situación y no ha detectado indicios de que se haya logrado acceder a las cuentas en la nube. Los intentos de acceso continúan, pero están siendo bloqueados. Este trabajo se lleva a cabo en paralelo a la investigación forense.

Es importante destacar que el incidente ha sido identificado dentro del entorno en la nube del Gobierno. Las principales bases de datos del Gobierno que contienen los registros personales de los residentes se mantienen por separado, en su propio centro de datos y en su infraestructura local.

Sin embargo, dado que el entorno en la nube también aloja el correo electrónico y el almacenamiento de documentos del Gobierno, sigue en curso una investigación forense detallada para determinar la naturaleza y el alcance completos del incidente, incluyendo si se ha accedido o extraído información sin autorización. Si la investigación determina que los datos personales de alguna persona se han visto afectados, el Gobierno se pondrá en contacto con ella directamente. El Gobierno facilitará más información conforme avance la investigación.

El Gobierno desea reconocer el compromiso excepcional del personal del ITLD, que ha trabajado sin descanso durante toda la semana pasada y el fin de semana, junto con socios

internacionales especializados, para proteger los sistemas del Gobierno y minimizar las interrupciones en los servicios públicos.

El Gobierno también aprovecha esta oportunidad para recordar a los ciudadanos la importancia de observar buenas prácticas de ciberseguridad:

- Desconfíen de los correos electrónicos, mensajes de texto o llamadas inesperadas, aunque parezcan proceder del Gobierno o de alguien que conozca, y no haga 'clic' en enlaces ni abra archivos adjuntos que no esperaba recibir.
- Utilice una contraseña segura y diferente para cada cuenta importante, especialmente para el correo electrónico.
- Active la autenticación multifactorial (también llamada verificación en dos pasos) siempre que se ofrezca.
- Mantenga sus dispositivos y su software actualizados.
- El Gobierno nunca le pedirá su contraseña por correo electrónico, mensaje de texto o teléfono.

Puede encontrar más consejos en la página web del Centro Nacional de Ciberseguridad: www.ncsc.gov.uk.

Las amenazas a la ciberseguridad son un reto cada vez más habitual para los gobiernos y las organizaciones de todo el mundo. El Gobierno seguirá invirtiendo en la resiliencia de su infraestructura digital y colaborando con socios especializados para reforzar aún más su seguridad.

Nota a redactores:

Esta es una traducción realizada por el Servicio de Información de Gibraltar. Algunas palabras no se encuentran en el documento original y se han añadido para mejorar el sentido de la traducción. El texto válido es el original en inglés.

Para cualquier ampliación de esta información, rogamos contacte con
Servicio de Información de Gibraltar

Miguel Vermehren, miguel@infogibraltar.com, Tel 609 004 166
Sandra Balvín, sandra@infogibraltar.com, Tel 637 617 757
Eva Reyes Borrego, eva@infogibraltar.com, Tel 619 778 498
Álvaro López, alvaro@infogibraltar.com, Tel 662 386 833
Nacho Arranz, nacho@infogibraltar.com, Tel 674 283 002

Web: www.infogibraltar.com, web en inglés: www.gibraltar.gov.gi/press
Twitter: @InfoGibraltar

HM Government of Gibraltar

PRESS RELEASE

No: 865/2026

Date: 09 November 2026

Government confirms cyber security incident contained following extensive security measures

HM Government of Gibraltar confirms that it has been responding to a cyber security incident affecting elements of its cloud-based IT environment.

The incident, which originated several weeks ago, involved unauthorised access to the Government's cloud environment, which includes services such as Microsoft Outlook, Teams, SharePoint and OneDrive. After Microsoft alerted the Government to a potential data breach, the Government's Information Technology and Logistics Department (ITLD) immediately began working to contain the threat, secure affected systems and strengthen existing security measures.

The Government has been working closely with Microsoft and the UK's National Cyber Security Centre (NCSC), which has coordinated specialist cyber security support. A team of experts from NCSC partner organisations travelled to Gibraltar on Monday 2 November to work directly alongside ITLD on the investigation and response.

On Friday 6 November, the Government suspended some services to allow a forensic investigation to take place and additional security measures to be implemented. The Government apologises for the disruption this caused.

ITLD and the specialist teams have taken extensive action to contain the incident and have put additional security measures in place. ITLD continue to monitor and have not seen signs of successful access to the cloud accounts. Access attempts continue but are being blocked. This work continues alongside the forensic investigation.

Importantly, the incident has been identified within the Government's cloud environment. The Government's principal databases containing residents' personal records are maintained separately, within its own data centre and local infrastructure.

However, because the cloud environment also supports Government email and document storage, a detailed forensic investigation remains ongoing to establish the full nature and extent of the incident, including whether any information was accessed or extracted without authorisation. If the investigation finds that anyone's personal data has been affected, the Government will contact them directly. The Government will provide further information as the investigation progresses.

The Government wishes to recognise the exceptional commitment of ITLD staff, who have worked continuously throughout the past week and over the weekend, alongside specialist international partners, to protect Government systems and minimise disruption to public services.

The Government also takes this opportunity to remind members of the public of the importance of good cyber security practices:

- Be wary of unexpected emails, texts or calls, even if they appear to come from the Government or someone you know, and do not click on links or open attachments you were not expecting.
- Use a strong, different password for each important account, especially your email.
- Turn on multi-factor authentication (also called two-step verification) wherever it is offered.
- Keep your devices and software up to date.
- The Government will never ask for your password by email, text or phone.

Further advice is available from the National Cyber Security Centre at ncsc.gov.uk.

Cyber security threats are an increasingly common challenge for governments and organisations worldwide. The Government will continue to invest in the resilience of its digital infrastructure and work with specialist partners to strengthen its security further.

ENDS