

COMUNICADO

Gobierno de Gibraltar

El Gobierno pone a prueba la resiliencia de Gibraltar en un ejercicio de ciberseguridad

Gibraltar, 20 de octubre de 2026

El pasado el miércoles 14 de octubre, unos cincuenta participantes de distintos departamentos del Gobierno, servicios de emergencia, organismos y autoridades públicas, compañías de suministros básicos y organizaciones colaboradoras participaron en una simulación teórica de ciberseguridad (Cyber Security Tabletop Exercise) celebrada en el hotel Sunborn Gibraltar.

El ejercicio fue planificado y dirigido conjuntamente por la Oficina de Contingencias Civiles y la División de Ciberseguridad (Cyber Division) del Departamento de Tecnología de la Información y Logística (Information Technology & Logistics Department, ITLD) del Gobierno.

El escenario simulaba un sofisticado ataque de *ransomware* contra los sistemas informáticos del Gobierno de Gibraltar que interrumpía la prestación de importantes servicios públicos. Su objetivo era evaluar la respuesta de los equipos informáticos del Gobierno, los servicios de emergencia, los departamentos y organismos gubernamentales y otros socios clave ante un ciberincidente grave.

Además de poner a prueba la respuesta técnica y estratégica al ataque simulado, el ejercicio examinó los mecanismos de continuidad de negocio de los participantes. Se analizó, por ejemplo, cómo mantendrían las organizaciones sus funciones críticas, coordinarían sus decisiones, se comunicarían con las partes interesadas y contribuirían al restablecimiento de los servicios esenciales mientras los sistemas habituales siguieran sin estar disponibles.

El ejercicio reunió a representantes de:

- Oficina de Contingencias Civiles;
- Departamento de Tecnología de la Información y Logística;
- Autoridad Sanitaria de Gibraltar (Gibraltar Health Authority, GHA);
- Departamento del Tesoro;
- Policía Real de Gibraltar (Royal Gibraltar Police, RGP);
- Servicio de Salvamento y Bomberos de Gibraltar (Gibraltar Fire & Rescue Service, GFRS);
- Servicio de Bomberos y Rescate del Aeropuerto (Airport Fire & Rescue Service, AFRS);
- Servicio de Aduanas de Gibraltar (HM Customs);
- Agencia de Fronteras y Guardacostas (Borders & Coastguard Agency, BCA);
- Autoridad Portuaria de Gibraltar (Gibraltar Port Authority, GPA);
- Aeropuerto Internacional Joshua Hassan de Gibraltar;
- Agencia de Medio Ambiente (Environmental Agency);
- Departamento de Personal y Desarrollo;
- Ministerio de Inmigración y Asuntos Internos;
- Oficina de Prensa del Número 6 de Convent Place (No.6 Press Office);

COMUNICADO

- Departamento de Educación;
- Departamento de Servicios Técnicos (Technical Services Department, TSD);
- Gibtelecom;
- Compañía Eléctrica de Gibraltar (Gibraltar Electricity Authority, GEA);
- AquaGib;
- Ministerio de Defensa;
- Ministerio de Asuntos Exteriores, de la Commonwealth y de Desarrollo del Reino Unido (Foreign, Commonwealth & Development Office, FCDO); y
- Autoridad Reguladora de Gibraltar (Gibraltar Regulatory Authority, GRA).

El ejercicio brindó a los participantes la oportunidad de afrontar, en un entorno controlado, las complejas consecuencias de un ciberincidente a gran escala. Se pusieron a prueba los procedimientos establecidos, las estructuras de toma de decisiones, los mecanismos de intercambio de información y la coordinación necesaria entre especialistas técnicos, equipos operativos de respuesta y altos responsables.

Los ciberincidentes pueden afectar a mucho más que a ordenadores y datos. Pueden interrumpir la atención sanitaria, las comunicaciones, el transporte, los suministros básicos, los sistemas financieros y otros servicios de los que depende la comunidad. En su Informe Anual de 2025, el Centro Nacional de Ciberseguridad (National Cyber Security Centre, NCSC) del Reino Unido advirtió de que los ciberataques tienen cada vez más consecuencias reales para empresas, productos, servicios y personas. De ahí la importancia de prepararse antes de que se produzca un incidente.

Durante su intervención en CYBERUK 2026, el Director Ejecutivo del Centro Nacional de Ciberseguridad, Richard Horne, afirmó que el *ransomware* sigue siendo la ciberamenaza más extendida para la mayoría de las organizaciones. Insistió además en que la ciberseguridad debe convertirse en una misión compartida por toda la organización, desde la alta dirección hasta los equipos operativos y técnicos, en lugar de seguir siendo responsabilidad exclusiva de los especialistas informáticos.

Este enfoque, que implica a toda la comunidad, se reflejó también en la actualización anual sobre amenazas que presentó el 13 de octubre el Director General del MI5 [servicio de inteligencia interior británico], Sir Ken McCallum. McCallum destacó la importancia de las resiliencias sistémica, social y tecnológica y advirtió de que los ciberataques pueden afectar directamente a infraestructuras críticas, servicios públicos, empresas y comunidades. En su mensaje recalcó que la resiliencia exige un “esfuerzo de toda la sociedad” y que hay que prepararse antes de que se produzcan las interrupciones.

El Ministro de Relaciones Industriales, Contingencias Civiles y Deporte, Leslie Bruzón, indicó:

“Las ciberamenazas evolucionan constantemente y pueden alterar los servicios de los que depende nuestra comunidad. Ejercicios de este tipo nos permiten poner a prueba nuestra preparación en un entorno realista pero controlado, detectar aspectos mejorables y reforzar la cooperación entre el Gobierno, los servicios de emergencia y nuestros socios clave.

COMUNICADO

La resiliencia frente a los ciberataques no es una responsabilidad exclusivamente técnica. Depende de un liderazgo eficaz, de unos mecanismos sólidos de continuidad operativa y de que las personas de cada organización entiendan el papel que les corresponde. Agradezco a todos los que han contribuido a la planificación y ejecución de este importante ejercicio”.

El Director del ITLD, Tyrone Manasco, hizo balance del ejercicio:

“Un ciberincidente grave requeriría una respuesta coordinada de todo el Gobierno y no puede gestionarse únicamente desde los equipos técnicos. Este ejercicio nos ha permitido comprobar cómo se comparte la información técnica, cómo se fijan las prioridades operativas y cómo se toman las decisiones cuando los sistemas y los servicios están sometidos a una fuerte presión.

También ha puesto de relieve la importancia de mantener prácticas de seguridad sólidas, tener los sistemas actualizados, notificar sin demora cualquier actividad sospechosa y garantizar que los mecanismos de recuperación se revisen y se ensayen periódicamente”.

El Coordinador de Contingencias Civiles, el Teniente Coronel retirado Ivor López, señaló:

“El propósito de un ejercicio no es simplemente demostrar lo que ya funciona. Se trata de cuestionar nuestras suposiciones, detectar carencias y extraer lecciones prácticas que mejoren nuestra preparación colectiva.

La amplia variedad de organizaciones representadas en el ejercicio refleja lo interconectados que están los servicios públicos modernos. Un ciberataque que afecte a una organización puede tener rápidamente consecuencias para muchas otras, así que una comunicación, una coordinación y una planificación de la continuidad operativa eficaces resultan esenciales”.

La ciberseguridad es una responsabilidad compartida. Tanto los ciudadanos como las organizaciones pueden contribuir utilizando contraseñas seguras y distintas para cada servicio, activando la autenticación multifactor, manteniendo actualizados sus dispositivos y programas, tratando con cautela los correos electrónicos y los enlaces y notificando sin demora cualquier sospecha de ciberincidente.

COMUNICADO

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

PRESS RELEASE

No: 804/2026

Date: 20 October 2026

Government Tests Gibraltar's Resilience During Cyber Security Exercise

Around 50 participants from across Government, the emergency services, public agencies and authorities, utility providers and partner organisations took part in a Cyber Security Tabletop Exercise at Sunborn Gibraltar on Wednesday 14 October 2026.

The exercise was jointly planned and delivered by the Office of Civil Contingencies and the Cyber Division of the Government's Information Technology & Logistics Department (ITLD).

The scenario simulated a sophisticated ransomware attack affecting HM Government of Gibraltar's information technology systems and disrupting the delivery of important public services. It was designed to evaluate the response of Government IT teams, emergency services, Government departments and agencies and other key partners during a major cyber incident.

In addition to testing the technical and strategic response to the simulated attack, the exercise examined participants' business continuity arrangements. This included how organisations would maintain critical functions, coordinate decisions, communicate with stakeholders and support the restoration of essential services while normal systems remained unavailable.

The exercise brought together representatives from:

- Office of Civil Contingencies;
- Information Technology & Logistics Department;
- Gibraltar Health Authority;
- Treasury;
- Royal Gibraltar Police;
- Gibraltar Fire & Rescue Service;
- Airport Fire & Rescue Service;
- HM Customs;
- Borders & Coastguard Agency;
- Gibraltar Port Authority;
- Joshua Hassan Gibraltar International Airport;
- Environmental Agency;
- Department of Personnel & Development;



- Department of Immigration & Home Affairs;
- No.6 Press Office;
- Department of Education;
- Technical Services Department;
- Gibtelecom;
- Gibraltar Electricity Authority;
- AquaGib;
- Ministry of Defence;
- Foreign, Commonwealth & Development Office; and
- Gibraltar Regulatory Authority.

The exercise provided participants with an opportunity to work through the complex consequences of a large-scale cyber incident in a controlled environment. It tested established procedures, decision-making structures, information-sharing arrangements and the coordination required between technical specialists, operational responders and senior leaders.

Cyber incidents have the potential to affect far more than computers and data. They can interrupt healthcare, communications, transport, utilities, financial systems and other services on which the community depends. The UK's National Cyber Security Centre warned in its 2025 Annual Review that cyberattacks increasingly have real-world consequences for businesses, products, services and people, underlining the importance of preparing before an incident occurs.

Speaking at CYBERUK 2026, Richard Horne, Chief Executive of the National Cyber Security Centre, said that ransomware remained the most prevalent cyber threat to most organisations. He also stressed that cyber security must become a shared organisational mission, extending from senior leadership to operational and technical teams, rather than remaining the responsibility of IT specialists alone.

This whole-community approach was also reflected in the annual threat update delivered by Sir Ken McCallum, Director General of MI5, on 13 October 2026. He highlighted the importance of systemic, societal and technological resilience and warned that cyberattacks can directly affect critical infrastructure, public services, businesses and communities. His message emphasised that resilience requires a "whole-of-society effort" and that preparation must take place before disruption occurs.

The Minister for Industrial Relations, Civil Contingencies and Sport, the Hon Leslie Bruzon MP, said: "Cyber threats are constantly evolving and have the potential to disrupt the services on which our community relies. Exercises of this kind allow us to test our preparedness in a realistic but controlled environment, identify areas for improvement and strengthen cooperation across Government, the emergency services and our key partners.

"Cyber resilience is not solely a technical responsibility. It depends on effective leadership, sound business continuity arrangements and people across every organisation understanding the part they have to play. I am grateful to everyone who contributed to the planning and delivery of this important exercise."



Reflecting on the exercise, the Director of ITLD, Tyrone Manasco, said: “A major cyber incident would require a coordinated response across the whole of Government and cannot be managed by technical teams in isolation. This exercise enabled us to test how technical information is shared, how operational priorities are established and how decisions are taken when systems and services are under significant pressure.

“It also reinforced the importance of maintaining robust security practices, keeping systems updated, reporting suspicious activity promptly and ensuring that recovery arrangements are regularly reviewed and exercised.”

The Civil Contingencies Coordinator, Lieutenant Colonel (Retired) Ivor Lopez MBE, said: “The purpose of an exercise is not simply to demonstrate what already works. It is to challenge our assumptions, identify gaps and generate practical lessons which can improve our collective preparedness.

“The wide range of organisations represented at the exercise reflects the interconnected nature of modern public services. A cyberattack affecting one organisation can quickly have consequences for many others, so effective communication, coordination and business continuity planning are essential.”

Cyber security is a shared responsibility. Individuals and organisations can contribute by using strong and unique passwords, enabling multi-factor authentication, keeping devices and software updated, handling emails and links with care, and promptly reporting suspected cyber incidents.

ENDS