



REPRESENTACIÓN EN ESPAÑA COMUNICADO DE PRENSA

Ejercicio de ciberseguridad de la UE para fomentar la cooperación y promover unas elecciones de la UE libres y limpias

Bruselas, 22 de noviembre de 2023

Para evaluar y reforzar los métodos de trabajo actuales antes de las elecciones de 2024, las instituciones de la UE organizaron ayer un ejercicio de ciberseguridad. Los socios nacionales y de la UE pusieron a prueba sus planes de crisis y las posibles respuestas a posibles incidentes de ciberseguridad que afecten a las elecciones europeas.

El ejercicio formaba parte de las medidas que está aplicando la Unión Europea para garantizar unas elecciones libres y limpias en junio de 2024. Se celebró en el Parlamento Europeo y lo organizaron los servicios del Parlamento Europeo, la Comisión Europea y la Agencia de la Unión Europea para la Ciberseguridad (ENISA). El ejercicio permitió a los participantes intercambiar experiencias y mejores prácticas, y los ayudará a mejorar su capacidad de respuesta a los incidentes de ciberseguridad, así como a contribuir a la actualización de las directrices y mejores prácticas existentes en materia de ciberseguridad de la tecnología utilizada en el proceso electoral.

En la segunda edición del ejercicio participaron representantes de las autoridades nacionales electorales y de ciberseguridad, junto con observadores del Parlamento Europeo, la Comisión Europea, el CERT-UE y la Agencia de la UE para la Ciberseguridad (ENISA). Si bien la principal responsabilidad de proteger la integridad de las elecciones recae en los Estados miembros de la UE, este ejercicio contribuyó a que perfeccionaran su preparación común a la hora de hacer frente a posibles amenazas cibernéticas y otras amenazas híbridas, así como su capacidad para fomentar y mantener rápidamente el conocimiento de la situación a escala nacional y de la UE en caso de producirse un incidente grave de ciberseguridad.

Todo está en marcha para velar por que los ciudadanos europeos puedan confiar en el proceso electoral de la UE. Los riesgos para las elecciones pueden adoptar diversas formas, desde la manipulación de la información y la desinformación hasta los ciberataques que ponen en peligro las infraestructuras.

Sobre la base de diversas hipótesis con posibles amenazas e incidentes cibernéticos, el ejercicio permitió a los participantes:

- Profundizar en sus conocimientos sobre el nivel de los aspectos críticos de las elecciones europeas, incluida una evaluación del grado de concienciación de otras partes interesadas (por ejemplo, partidos políticos, organizaciones de campañas electorales y proveedores de los equipos informáticos pertinentes).
- Mejorar la cooperación entre las autoridades pertinentes a nivel nacional, por ejemplo, las autoridades electorales y otros organismos y agencias pertinentes como las autoridades de ciberseguridad, los equipos de respuesta a incidentes de seguridad informática (CSIRT), las autoridades de protección de datos (APD), y las autoridades que se ocupan de cuestiones relacionadas con la desinformación, y también a escala de la UE, como los servicios de la Comisión encargados de la aplicación de la Ley de Servicios Digitales.
- Comprobar la capacidad existente de los Estados miembros de la UE para evaluar adecuadamente los riesgos relacionados con la ciberseguridad de las elecciones europeas, fomentar prontamente el conocimiento de la situación y coordinar la comunicación al público.
- Poner a prueba los planes de gestión de crisis existentes, así como los procedimientos pertinentes para prevenir, detectar, gestionar y contrarrestar los ataques de ciberseguridad y las amenazas híbridas, incluidas las campañas de desinformación.
- Determinar todas las demás posibles lagunas y las medidas adecuadas de reducción del riesgo, que deberían aplicarse antes de las elecciones al Parlamento Europeo.

Más información

[Elecciones europeas](#)

Cita(s)

Las elecciones y las campañas se celebran cada vez más en el entorno digital. Aunque esto ofrece muchas oportunidades, también plantea riesgos, y debemos estar preparados para proteger nuestra infraestructura frente a los ciberataques desde dentro y fuera de la UE. Las próximas elecciones europeas serán una

prueba importante y no la debemos fallar. Nuestra mejor defensa es difundir conocimientos y colaborar en toda la UE.

Věra Jourová, vicepresidenta responsable de Valores y Transparencia - 21/11/2023

Los ciberataques y la desinformación constituyen una amenaza para las democracias. Cabe esperar que agentes malintencionados también ataquen las elecciones para intentar dañar la credibilidad de nuestras instituciones democráticas. Es fundamental que las instituciones de la UE y los Estados miembros salvaguarden la confianza en la integridad y la legitimidad de las elecciones europeas, lo que supone colaborar para reforzar nuestra ciberresiliencia en el período previo a las elecciones europeas de 2024.

Thierry Breton, comisario responsable de Mercado Interior - 21/11/2023

La digitalización reporta enormes beneficios y representa la promesa de un futuro mejor. Sin embargo, también plantea ciertas amenazas. Entre ellas se cuentan los ciberataques, que pueden perjudicar unas elecciones libres y limpias. Las elecciones deben basarse en información y hechos correctos. No debemos ser ingenuos y bajar nuestra guardia, especialmente con vistas a las elecciones europeas del año que viene.

Didier Reynders, comisario responsable de Justicia - 21/11/2023