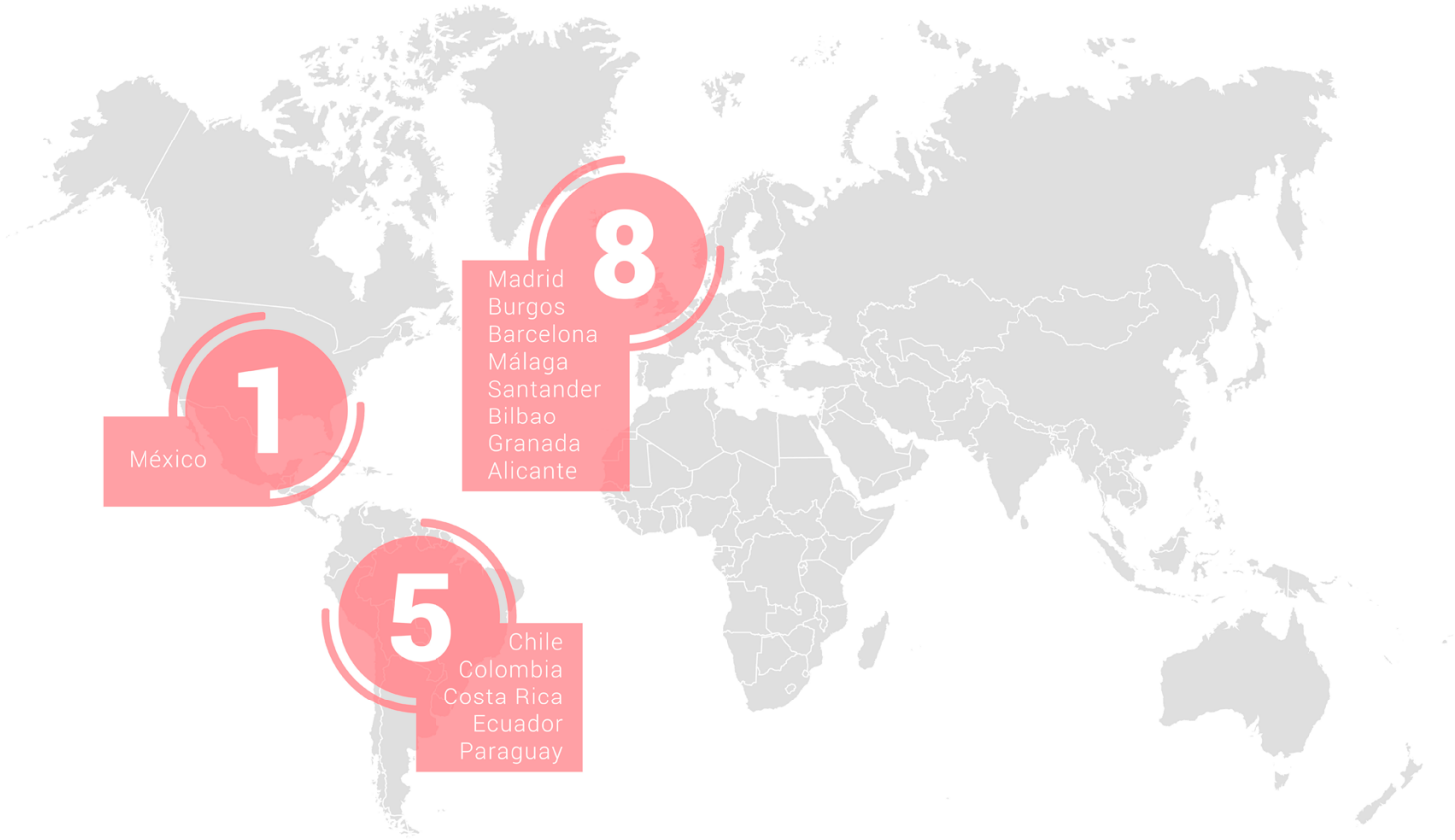
GrupoACMS
CONSULTORES

GRUPO ACMS Consultores

Recomendaciones sobre ciberseguridad electoral



AENOR
ER
Empresa Registrada
ISO 9001

(ER-0772/2013)

Alcance ISO 9001

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

Alcance ISO 27001

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.

AENOR
ER
Seguridad Información
ISO/IEC 27001

(SI-0021/2020)

Publicada el 22/03/2019

En el contexto de las próximas elecciones para el Parlamento Europeo, la Agencia de la UE para la ciberseguridad de la UE ENISA publica un documento de opinión sobre la ciberseguridad de las elecciones y proporciona recomendaciones concretas y futuras para mejorar la ciberseguridad de los procesos electorales en la UE.

La seguridad cibernética

ENISA explora las amenazas cibernéticas, que pueden socavar el proceso democrático de la UE. De particular importancia es la posibilidad de interferencia en las elecciones por medios cibernéticos, debido al uso generalizado de la tecnología digital para apoyar los procesos electorales en actividades tales como comunicaciones confidenciales de políticos y partidos políticos, campañas políticas, el registro electoral, el conteo de votos, y la difusión de los resultados.

ENISA alienta a los Estados miembros de la UE y a las partes interesadas clave, como los partidos políticos, a participar en más ejercicios cibernéticos destinados a probar la ciberseguridad electoral para mejorar la preparación, la comprensión y la respuesta a posibles amenazas cibernéticas relacionadas con las elecciones y escenarios de ataques. Estas partes interesadas deben tener planes de respuesta a incidentes en el lugar, en el caso de que sean víctimas de fugas de datos.

Una amenaza en evolución es la motivación detrás de los actores que interfieren con el debido proceso de las elecciones por medios cibernéticos. La motivación para los actores puede ser múltiple, por ejemplo, para obtener ganancias financieras, fama y reputación, o para provocar el caos y la anarquía, socavar la confianza en la democracia y subvertir la oposición política.

A través de este documento, ENISA presenta una serie de recomendaciones destinadas a mejorar la ciberseguridad de las elecciones en toda la UE y apoyar a los Estados miembros en sus esfuerzos.

Las recomendaciones más importantes que hace ENISA son:

- Los Estados miembros deberían considerar la introducción de una legislación nacional para abordar los desafíos asociados con la desinformación en línea y, al mismo tiempo, proteger en la mayor medida posible los derechos fundamentales de los ciudadanos de la UE;

- Los Estados miembros deben continuar trabajando activamente junto con el objetivo de identificar y eliminar redes de bots;

- Debería considerarse la regulación de los proveedores de servicios digitales, redes sociales, plataformas en línea y proveedores de servicios de mensajería a nivel de la UE para garantizar un enfoque armonizado en toda la UE para abordar la desinformación en línea con el objetivo de socavar el proceso democrático;

- También se recomienda a los jugadores mencionados que implementen tecnología que identifique patrones de tráfico inusuales que podrían estar asociados con la propagación de la desinformación o los ataques cibernéticos en los procesos electorales;

- Debería considerarse la obligación legal de clasificar los sistemas, procesos e infraestructuras electorales como infraestructura crítica para que se implementen las medidas de ciberseguridad necesarias;

- Debe establecerse una obligación legal que obligue a las organizaciones políticas a desplegar un alto nivel de ciberseguridad en sus sistemas, procesos e infraestructuras;

- Se deben identificar los canales / tecnologías oficiales para la difusión de los resultados, así como los canales / tecnologías de respaldo que validan los resultados con los centros de conteo. Donde se utilizan los sitios web, se deben aplicar técnicas de mitigación de DDoS.

Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

Madrid

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

Burgos

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

Barcelona

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

Málaga

C/ Alejandro Dumas 17 29004 Málaga

Tfno.: (+34) 95 113 69 04

México

José González Varela 15 14700 Tlalpan

Tfno.: (+52) 5513 39 96 22

www.grupoacms.com
informacion@grupoacms.com