el Periódico Mediterráneo

CONSECUENCIAS DEL CONFLICTO EN EL ÁMBITO DIGITAL

Las administraciones de Castellón se blindan ante el repunte de ciberataques

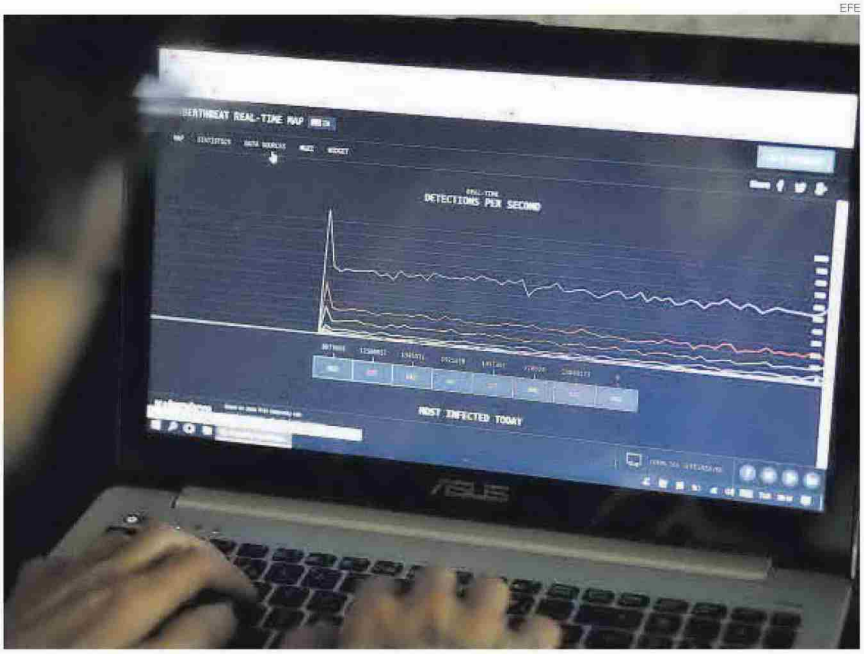
Consell, Diputación, Ayuntamientos o la UJI refuerzan sus sistemas informáticos

La Generalitat baraja formar a la ciudadanía en caso de aumentar el riesgo cibernético

IVÁN CHECA
ichecagonzalez@mediterraneo.elperiodico.com
CASTELLÓN

La invasión rusa a Ucrania ha tenido también su impacto en el mundo digital con un repunte de los ciberataques, los cuales se han traducido en alertas instando a reforzar la seguridad. Es por ello que las administraciones de la provincia de Castellón han optado por blindar sus equipos y sistemas para evitar sus consecuencias, que pueden llegar a paralizar por completo su día a día.

La Generalitat, ante el aumento del nivel de alerta por parte del Centro Criptológico Nacional, ha adoptado medidas preventivas como cambios de contraseñas o desconexión de la red de ordenadores sin uso. De hecho, la Dirección General de Tecnologías de la Información y Comunicación, según fuentes de la Conselleria de Hacienda de la que depende, «como precaución y ante posibles aumentos de las tensiones internacionales» ha elevado también el nivel de alerta de todos los equipos que trabajan en el área de ciberseguridad y también de los sistemas de protección, tal y como establecen sus protocolos, dando instrucciones básicas a los trabajadores de la administración autonómica en la Comunitat.



EFE

Los ciberataques han aumentado de forma considerable desde que se inició la invasión rusa a Ucrania.

Por el momento, las mismas fuentes aseguran que el Consell no ha detectado ninguna situación de vulnerabilidad, pero de crecer más el riesgo cibernético el Centro de Seguridad TIC de la Comunitat Valenciana prepararía material para formar a la gente. Desde donde recuerdan a su vez que están a disposición de empresas y ciudadanos, a la vez que recomiendan ante este escenario «asumir los mínimos riesgos posibles».

GUÍA // La Diputación de Castellón también mantiene la vista puesta en esta cuestión y su personal dispone de una guía con consejos para evitar ataques y proteger la información con la que trabajan.

A nivel municipal, algunos ayuntamientos también han tomado medidas. Uno de ellos es el consistorio de la capital de la Plana, que ya sufrió un ciberataque el año pasado. El portavoz del equipo de gobierno, José Luis López, explicó que «dentro del plan de ciberseguridad que tenemos en el ayuntamiento estamos ahora en un nivel muy alto de alerta», atendiendo así a los llamamientos de entidades superiores.

También la Universitat Jaume I ha impuesto recientemente la obligación de cambiar las claves de acceso a la red interna a toda la comunidad educativa. ≡

+ información

LOS CONSEJOS PARA PREVENIR

DISPOSITIVOS

- Una guía interna distribuida entre el personal de la Diputación recomienda evitar modificar la configuración de los dispositivos, instalar aplicaciones no verificadas y no conectar dispositivos USB de origen desconocido.

NAVEGACIÓN

- Evitar acceder a páginas web no confiables o clicar enlaces sospechosos, así como escribir la dirección en la barra del navegador. También se recomienda eliminar cualquier correo sospechoso, como los que procedan de una persona desconocida o una dirección distinta al dominio oficial. No mandar datos bancarios.

CONTRASEÑAS

- No compartir las credenciales de acceso, tanto el usuario como la contraseña, con terceras personas, así como tener claves diferentes o cambiarlas con frecuencia.

PROTECCIÓN

- Realizar copias de seguridad de la información y almacenarlas en lugares seguros o dispositivos físicos adicionales para no perder la información ante un ataque.