El **CERT de Seguridad e Industria** realiza una consulta a las grandes infraestructuras críticas españolas para medir su capacidad de resistencia ante un ataque informático.

¿Está su entidad preparada para resistir un ciberatque? Esta es la principal pregunta que ha enviado el CERT de Seguridad e Industria a treinta y dos entidades que operan infraestructuras críticas de nuestro país.

Sectores como energía, sistema financiero, agua, TIC, industria nuclear, administración y transporte, que prestan servicios esenciales para la ciudadanía, cuyo funcionamiento es indispensable, y que un ataque informático contra las mismas podría acarrear consecuencias de gran impacto contra la sociedad, están siendo consultados mediante un extenso cuestionario, para evaluar como protegen sus instalaciones frente a posibles ataques informáticos.

El CERT de Seguridad e Industria tiene constancia de 17.888 incidentes de ciberseguridad ocurridos en España durante el año 2014, que fueron gestionados por el CERTSI_ de los cuales 63 afectaron a empresas estratégicas.

Según revela un informe de la ENISA, más del 50% de los ataques con éxito se deben a la dejadez y negligencia en aspectos clave de ciberseguridad. Esta cifra se lleva repitiendo los últimos tres años, por lo que es necesario mejorar la concienciación en ciberseguridad.

Desde el CERTSI_ se quiere evitar casos como el ocurrido contra el banco americano JPMorgan Chase que afectó a 76 millones de hogares y a 7 millones de pequeñas empresas, o el caso de una **fábrica de acero en Alemania** que sufrió graves daños porque los cibercriminales impidieron apagar un horno.

Ciberresiliencia

La ciberresiliencia es la capacidad de un proceso, nación, organización o negocio para anticipar, resistir, recuperarse, y evolucionar para mejorar sus capacidades frente a condiciones adversas, estrés o ataques a los recursos tecnológicos que necesita para

funcionar.

Mediante un **formulario con 54 cuestiones diseñadas para extraer métricas e indicadores de cibersiliencia** de las organizaciones frente a ataques informáticos, el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), órgano de la Secretaría de Estado de Seguridad del Ministerio del Interior encargado de la protección de las Infraestructuras Críticas, junto con el Instituto Nacional de Ciberseguridad (INCIBE), organismo dependiente de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, pretende extraer un **informe del estado de la ciberresiliencia en las IICC Españolas** que permita un plan de acción para la mejora de la protección de la ciberseguridad y la resiliencia.

El informe anual del estado de la ciberresiliencia en las IICC Españolas permitirá de esta manera dar una respuesta para conocer si las empresas estratégicas de nuestro país están preparadas para resistir a un ciberataque, y tomar las medidas necesarias para que nuestro país sea ciberresiliente.