Nota de prensa

El Gobierno aprueba el 'Plan de choque de ciberseguridad' en el marco de un nuevo paquete de medidas ante las ciberamenazas

- **El plan incorpora medidas e inversiones que mejoran las capacidades de defensa ante ciberataques de manera más eficaz, contundente y directa**
- **La protección frente a código malicioso, la detección de amenazas en equipos y el refuerzo de las capacidades de recuperación ante desastres son algunas de las medidas del plan**
- **El paquete de actuaciones acordado por el Consejo de Ministros también incluye la actualización del Esquema Nacional de Seguridad**
- **Se promueve la adopción de estándares y políticas de gestión de seguridad en el sector privado para aumentar el nivel de ciberseguridad de los proveedores tecnológicos del sector público**
- **Se acelera el despliegue del Centro de Operaciones de Ciberseguridad de la Administración (COCS) gracias al Plan de Recuperación**

25 de mayo de 2021.- El Consejo de Ministros ha acordado este martes la puesta en marcha de un paquete de actuaciones urgentes en materia de ciberseguridad. El objetivo es reforzar de manera inmediata las capacidades de defensa frente a las ciberamenazas sobre el sector público y sobre las entidades que suministran tecnologías y servicios al mismo.

CORREO ELECTRÓNICO
prensa@economia.gob.es

Pº de la Castellana, 162
28071 - MADRID
TEL: 91 603 79 18 / 20 / 21

El acuerdo aprobado incluye la adopción de un Plan de Choque de Ciberseguridad, la actualización del Esquema Nacional de Seguridad y la promoción de medidas para aumentar el nivel de ciberseguridad de los proveedores tecnológicos del sector público estatal.

Estas actuaciones reforzarán con eficacia la capacidad de prevención, detección, protección y defensa frente a la materialización de las ciberamenazas. Además, se vela porque la transformación digital vaya acompañada de medidas organizativas y técnicas de seguridad proporcionadas a los riesgos, lo que favorece la confianza en el uso de tecnologías digitales por parte de los actores económicos y la ciudadanía.

Plan de Choque de Ciberseguridad

Entre las medidas que incluye este plan de choque figuran la protección frente al código malicioso (especialmente del tipo orientado a la destrucción de la información mediante su cifrado), la extensión de los servicios para la detección de ciberamenazas en equipos de usuario, la implantación de la vigilancia de accesos remotos, el refuerzo de las capacidades de búsqueda de amenazas, la ampliación de las capacidades de ciberinteligencia, la extensión de la aplicación del uso del segundo factor en los procesos de identificación y autenticación, el despliegue de capacidades para la notificación y el seguimiento de los ciberincidentes, la continuidad de negocio y la recuperación ante desastres, la concienciación y la formación, y la revisión de la normativa de ciberseguridad.

Las medidas incluidas en el 'Plan de choque de ciberseguridad' están vinculadas al Plan de Recuperación, Transformación y Resiliencia en su Componente 11 (Inversión 1. Modernización de la Administración General del Estado) y en su Componente 15 (Inversión 7. Ciberseguridad).

Esquema Nacional de Seguridad

La segunda actuación del paquete de medidas acordado por el Gobierno este martes es la actualización del Esquema Nacional de Seguridad, que data de una etapa con un contexto normativo, social y tecnológico que ha

Pº de la Castellana, 162
28071 - MADRID
TEL: 91 603 79 18 / 20 / 21

sufrido una evolución radical. Para ello se tramitará y aprobará de manera urgente un real decreto que sustituya al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

El Esquema Nacional de Seguridad (ENS) ofrece un planteamiento común de principios básicos, requisitos mínimos, medidas de protección y mecanismos de conformidad y monitorización, adaptado al cometido del Sector Público para la gestión continuada de la seguridad para la Administración Digital. El ENS es un esquema de aplicación a las entidades del Sector Público e indirectamente, a las entidades del Sector Privado que colaboren con aquellas en la prestación de servicios públicos. Es un instrumento esencial para que la administración digital sea robusta y confiable.

Seguridad en el sector privado

La tercera actuación consiste en promover e incentivar la adopción de sistemas, estándares y políticas de gestión de seguridad en el sector privado en particular aumentando el nivel de ciberseguridad de los proveedores tecnológicos del Sector Público estatal ante la evidencia de que la ciberseguridad de un organismo también está condicionada a la de sus proveedores tecnológicos.

Implantación del Centro de Operación de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (COCS)

De manera simultánea a la puesta en marcha del paquete de actuaciones urgentes en materia de ciberseguridad, se ejecuta la implantación del Centro de Operación de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (COCS).

El COCS reforzará las capacidades de vigilancia, prevención, protección, detección, respuesta ante incidentes de ciberseguridad, asesoramiento y apoyo a la gestión de la ciberseguridad de un modo centralizado, mediante el correspondiente catálogo de servicios, que mediante optimización y

Pº de la Castellana, 162
28071 - MADRID
TEL: 91 603 79 18 / 20 / 21

economías de escala permita una mejor eficacia y eficiencia, con los ahorros de dinero, esfuerzo y tiempo derivados.

Se trata de una inversión incluida en el Componente 11 del Plan de Recuperación, Transformación y Resiliencia. Su creación está prevista en la Estrategia Nacional de Ciberseguridad 2019.

Pº de la Castellana, 162
28071 - MADRID
TEL: 91 603 79 18 / 20 / 21