



Boletín CYBER-GC

Marzo 2022

La Unidad de Coordinación de Ciberseguridad de la Guardia Civil (UCCIBER), acaba de publicar su Boletín de Ciberseguridad (CYBER-GC) en el que nos informa de las últimas novedades y contenidos relacionados con este ámbito así como los casos de éxito y avance en la digitalización de los procesos de diferentes organizaciones e instituciones.

En ese sentido, la Agencia Europea de Seguridad en las Redes y de la Información de la Unión Europea (ENISA) ha publicado su Estrategia Internacional en la que establece sus prioridades en este ámbito y desarrolla herramientas e instrumentos capaces de combatir de forma más eficaz los ciberataques.



Esta estrategia responde a la necesidad de cooperar internacionalmente para crear un Europa en la que se pueda confiar y sea cibersegura.

A nivel estatal, el Gobierno y las Comunidades Autónomas están afrontando un aumento de la inversión en ciberseguridad. A medida que la tecnología va ganando relevancia, también aumentan los riesgos de seguridad, todas estas gestiones de los organismos se centralizarán en el nuevo Centro de Operaciones de Ciberseguridad (SOC) específico para la Administración General del Estado y sus organismos públicos.



Los resultados de organismos públicos especializados en el sector, se publican en los informes del CCN-CERT perteneciente al Centro Criptológico Nacional (CCN).

En estos documentos se abordan las ciberamenazas conocidas y se detallan los elementos clave para establecer el marco de gobernanza de la ciberseguridad. Cabe recordar que la gestión de la ciberseguridad requiere de un marco de gobernanza en el que se designen a los organismos o unidades responsables de dicha gestión y se definan sus competencias en este ámbito que deberán ser conocidas por toda la organización.



NOTICIAS DE INTERÉS

La Guardia Civil desarticula una organización criminal internacional especializada en blanqueo de capitales a través de criptomonedas.

La Guardia Civil, con la Operación MAUNA ha logrado la desarticulación de una organización criminal especializada en el blanqueo de capitales a través de criptomonedas procedentes de diferentes hechos delictivos cometidos por otros actores.

La investigación, desarrollada por la Unidad Central Operativa se inició a raíz de ciertas actividades y movimientos de blanqueo de capitales vinculados al narcotráfico, lo que dio origen a toda la Operación.

España es el país con más ataques informáticos a través de la función de escritorio remoto

Según la compañía de seguridad informática ESET Malware Protection & Internet Security, España se ha convertido en el país con mayor número de ataques informáticos a través del protocolo de escritorio remoto, función que permite acceder y controlar un ordenador a través de la red.



Durante el año 2021 se produjeron el doble de estos ataques que en Italia (segundo país en la lista). Francia, Alemania y Polonia ocupan consecutivamente la tercera, cuarta y quinta posición en la lista.

CONCLUSIÓN

Aunque parece apreciarse una cierta tendencia descendente en la consumación de ciertos delitos informáticos, la recomendación es seguir incidiendo en la lucha contra las ciberamenazas, que constituyen uno de los principales desafíos que contempla la Estrategia de Seguridad Nacional.

Es fundamental seguir desarrollando la transformación digital sin desatender la ciberseguridad de las organizaciones y priorizando la defensa de los derechos de los usuarios de servicios digitales.

https://www.guardiacivil.es/es/servicios/consejos/en_internet.html