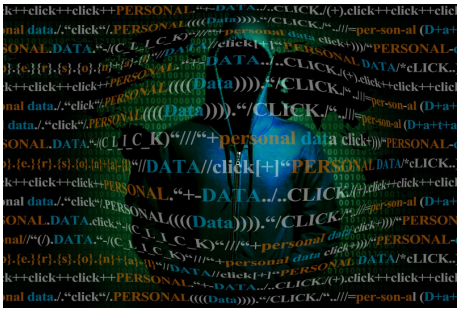
UNIVERSIDAD DE GRANADA

Centro de Servicios Informáticos y Redes de Comunicación

Medidas necesarias para prevenir ciberincidentes en equipos de RedUGR

04/03/2022

seguridad



La **Secretaría General de la Universidad de Granada** informa de las medidas necesarias para prevenir los ciberincidentes en el uso de los equipos informáticos conectados a la RedUGR.

Durante los últimos meses se ha producido un incremento de ciberincidentes que amenazan la seguridad de la información de las Administraciones Públicas en general y de las Universidades en particular. En consonancia con las recomendaciones del Centro Criptológico Nacional (CCN-CERT) y a los efectos de prevenir ciberataques a nuestros sistemas de información se insta a quienes dispongan de un equipo informático conectado RedUGR a seguir las siguientes indicaciones:

1.- Extremar la precaución de mantener apagados los equipos informáticos siempre que no estén en uso o no sea imprescindible mantenerlos operativos. Se recuerda que con el sistema GUFI de CSIRC es posible encender el ordenador de forma remota en caso necesario. La información para configurar el equipo y usar este arranque remoto se encuentra en:

https://csirc.ugr.es/informacion/servicios/redugr/gufi

2.- Por otra parte, siguiendo las directrices del CCN-CERT referentes a extender la instalación del centro de vacunación contra el ransomware proporcionado por el propio CCN-CERT denominado microCLAUDIA, se recomienda la instalación dicho software en los equipos informáticos, siempre que el sistema lo permita.

- https://microclaudia.ccn-cert.cni.es/

Más información sobre microCLAUDIA en:

https://www.ccn-cert.cni.es/pdf/documentos-publicos/6374-infografia-microclaudia/file.html