CORREO DEL RESPONSABLE DE SISTEMAS E INNOVACIÓN TECNOLÓGICA SOBRE RECOMENDACIONES EN RELACION CON EL TRABAJO NO PRESENCIAL Y EL CANAL DIGITAL

Para hacer frente a la epidemia de coronavirus, se están generalizando el trabajo no presencial y el canal digital. En este escenario, muchos usuarios no habituados a trabajar en remoto tienen que adaptar sus hábitos de trabajo, incluyendo la aplicación de pautas de ciberseguridad.

Interesa la protección frente a ciberdelincuentes que puedan intentar realizar campañas de "phishing" en las que, haciéndose pasar por personal de la organización, en especial de atención a usuarios, pretendan obtener credenciales de acceso a los sistemas.

También interesan pautas o recomendaciones de protección que los usuarios pueden aplicar en el uso de sus ordenadores, dispositivos móviles, correo electrónico, redes sociales, almacenamiento en la nube, y cómo actuar en caso de un posible incidente.

Los siguientes recursos facilitan orientación ágil para usuarios y es **muy importante su lectura y comprensión**:

- Recomendaciones ante ataques de phishing para personal en teletrabajo
- Recomendaciones frente a phishing y desinformación en relación con COVID19
- Recomendaciones de ciberseguridad para usuarios

En el Consorcio lo tenemos relativamente fácil, ya que nos conocemos casi todos. Aplicando algunas de las directrices de los documentos anteriores, desde Sistemas e Innovación Tecnológica queremos 'aterrizar' en consejos directos algunas de las precauciones a aplicar para los que estáis en casas teletrabajando:

1. No deis vuestro identificador de Teamviewer a nadie que os lo pida, salvo que se identifique y le reconozcáis la voz. Como mecanismo adicional en caso de duda, y mientras dure esta situación, deberéis preguntar por la **frase de paso**: "La tostada siempre cae del lado de la mantequilla"

2. Utilizad la conexión VPN sólo cuando sea necesario. Los recursos son finitos, y aunque de momento no se han notado problemas, éstos pueden surgir si usamos la conexión VPN como si estuviésemos en OOCC.

3. Hay que mantener el equipo lo más actualizado posible, especialmente el antivirus. Si el sistema os pide actualizaciones que no podéis hacer, enviad un mensaje a soporte@bombersdv.es y alguno de nuestros técnicos os llamará para actualizar el equipo o la aplicación.

4. La desconfianza y el sentido común, en esta situación especialmente, medidas de seguridad muy útiles, ya que se están propagando campañas de phishing y de fraudes

de todo tipo con la excusa del COVID-19, como constata el Centro Criptológico Nacional del CNI. Ante cualquier duda, preguntadnos.

5. El uso del equipo proporcionado es exclusivamente para realizar las funciones propias del puesto, en modalidad no presencial. Como en modalidad presencial, están prohibidos cualesquiera otros usos del equipo.

6. No está permitido intentar usar equipos no corporativos del Consorcio para el trabajo en modalidad no presencial.

7. Si recibís correos de personas cercanas solicitando información u ofreciendo ficheros, aseguraos de que la persona que os lo ha enviado sea la que dice ser. Os puede dar pistas la forma de escribir o las palabras que usan.

8. Nunca deis vuestras contraseñas ni permitáis que usen vuestros certificados digitales.

9. Para intercambiar ficheros, utilizad únicamente los sistemas proporcionados por el Consorcio: carpetas compartidas Windows, Nextcloud, etc....