Recomendaciones de ciberseguridad para usuarios

Con carácter general debe conocer que su Departamento o Entidad contará con una **Política de Seguridad de la Información** que, en aplicación del Esquema Nacional de Seguridad (ENS), detallará la estructura de **responsables y** desarrollará los detalles sobre el **uso seguro de equipos, servicios e instalaciones**. Son de particular interés para Usted las indicaciones básicas que siguen.

1. Apóyese en su equipo (Responsable TIC y Responsable de Seguridad)

- El **Responsable de Tecnologías de la Información y Comunicaciones (TIC) junto con el Responsable de Seguridad** podrán facilitarle mayores indicaciones sobre el uso seguro de los elementos que se citan seguidamente o sobre otros que pueda necesitar.

2. Uso de dispositivos móviles (móvil, tableta)

- **Proteja su dispositivo móvil con un código de acceso** asociado a la pantalla de bloqueo. Para mayor facilidad puede configurar el desbloqueo con su huella dactilar.
- **Mantenga actualizado el sistema operativo del dispositivo**, así como todas las apps instaladas.
- **Haga uso de las capacidades de cifrado** del dispositivo para proteger sus datos e información.
- **Deshabilite los interfaces de comunicaciones inalámbricas** (wifi, bluetooth) cuando no se vayan a usar.
- **No instale apps que no provengan de fuentes de confianza** como los mercados oficiales de apps.

3. Uso de redes sociales

- **Use contraseñas fuertes** para proteger su perfil combinando números, letras y caracteres especiales, que no sigan un patrón y que sean largas (6 caracteres o más).
- **No use la misma contraseña** para varias redes sociales, y para servicios de su Departamento o Entidad.
- **Configure su perfil** adecuadamente para proteger su privacidad.
- **Piense antes de escribir** o de compartir contenidos.
- **Sea cauto** con contenidos atractivos o impactantes, enlaces, reclamos, ofertas o con la publicidad de apps novedosas o muy solicitadas.

4. Uso del correo electrónico

- **No haga clic** en ningún enlace que solicite datos personales o bancarios.
- **No abra ningún enlace** ni descargue ningún fichero adjunto procedente de un correo electrónico que presente cualquier indicio o patrón fuera de lo habitual.
- **Antes de abrir cualquier fichero descargado desde el correo, asegúrese** de la extensión y no se fíe del icono asociado al mismo.
- **No confíe únicamente en el nombre del remitente**. Compruebe que el dominio del correo recibido es de confianza. Si un correo procedente de un contacto conocido solicita información inusual contacte por teléfono u otra vía de comunicación para corroborar la legitimidad.

5. Uso del portátil

- **Aplique un código de acceso robusto** (6 caracteres –nºs, letras, caracteres especiales- o más).
- **Deshabilite las conexiones inalámbricas** (wifi, bluetooth, etc.) mientras no vayan a utilizarse.
- **Mantenga actualizado el software y use una configuración de seguridad** aprobada por el responsable TIC de la entidad.

6. Uso de servicios de almacenamiento en la nube

- **Use los servicios de almacenamiento en la nube que su Responsable TIC ponga a su disposición**.

7. Cómo actuar ante un incidente de seguridad

- **Póngalo en conocimiento a la mayor brevedad posible** del responsable TIC o del Responsable de Seguridad de su Departamento o Entidad.

Para más información véase '[Principios y recomendaciones básicas en Ciberseguridad]'