Medidas de seguridad para el Teletrabajo

Con la expansión del teletrabajo en un gran número de empresas, el cibercrimen está experimentando un aumento sin precedentes. Muchos dispositivos utilizados en el hogar carecen de una configuración adecuada, y nuestros hábitos suelen ser diferentes a los que seguimos en un entorno laboral. Esto nos convierte en un objetivo vulnerable para los hackers. Revisa las especificaciones técnicas de tu equipo y adopta buenas prácticas.

- **1. Mantén tu sistema operativo actualizado**

  Utiliza versiones originales y actualizadas de los sistemas operativos. Las actualizaciones incluyen mejoras que corrigen vulnerabilidades de seguridad, evitando que los ciberdelincuentes puedan acceder.

  Trabaja con sistemas operativos originales actualizados. Las actualizaciones instalan mejoras que cierran brechas de seguridad que permiten a los piratas acceder a nuestros dispositivos.

- **2. Protege el dispositivo**

  Evita compartir contraseñas de trabajo por aplicaciones de mensajería o en redes sociales.

  - Recuerda utilizar siempre contraseñas robustas y cambiarlas cíclicamente.
  - Usa contraseñas largas (al menos 12 caracteres) que incluyan mayúsculas, minúsculas, números y símbolos.
  - No reutilices la misma contraseña para diferentes servicios.
  - Utiliza un gestor de contraseñas (como LastPass, Bitwarden, o 1Password) para almacenar y generar contraseñas seguras.
  - Desconecta el equipo al final de la jornada.
- **3. Protege la información**
  - Evita el almacenamiento local. No descargues ficheros con datos personales de usuarios en tu equipo. Puedes trabajar con estos ficheros remotamente en las carpetas compartidas de tu unidad o servicio.
  - Minimiza el papel.
  - Revisa y elimina la información residual.
  - Utiliza auriculares para garantizar la privacidad en las reuniones virtuales.
  - Recuerda el deber de confidencialidad.
  - Cifra los datos sensibles
- **4. Usar un software antivirus confiable**

  El antivirus detecta y elimina software malicioso, como virus, troyanos o

ransomware, que podría comprometer tu equipo.

¿Cómo hacerlo?

- Instalar un antivirus de confianza como Bitdefender, Norton, Kaspersky o usar las soluciones gratuitas como Windows Defender (ya integrado en Windows).
- Realizar escaneos periódicos para detectar posibles amenazas.
- Para evitar Ransoware en la UGR tenemos una utilidad llamada Microclaudia, puede solicitar e instalarla siguiendo este enlace

- **5. Activa la autenticación de dos factores (2FA)**

  La autenticación en dos pasos añade una capa extra de seguridad, pidiendo un código adicional (que se recibe en el móvil o en una aplicación) además de la contraseña.

  ¿Cómo hacerlo?

  En la mayoría de los servicios (correo electrónico, redes sociales, aplicaciones de trabajo), puedes activar el 2FA en las configuraciones de seguridad de cada cuenta.

  Usar aplicaciones de autenticación como Google Authenticator, Authy o incluso la opción de recibir el código por mensaje de texto.

- **6. Protege el correo electrónico**
  - Ojo con la descarga de archivos y con la apertura de enlaces.
  - Cifra mensajes y archivos con datos personales
- **7. Intenta que al ordenador de trabajo en casa no accedan otras personas de la unidad familiar**

  La intervención de otras personas puede suponer riesgos de seguridad.

- **8. Consulta la página de seguridad del Servicio de Informática para estar al día**
  - Algunos consejos con aspectos de seguridad de la información en teletrabajo.
  - Normativa, buenas prácticas, noticias y alertas de seguridad...
- **9. Contacta con la oficina de protección de datos**

  Contacta con la Oficina de Protección de Datos de la UGR para cualquier duda o incidencia:

  protecciondedatos@ugr.es