Ciberseguridad en el Teletrabajo

La **ciberseguridad** en el **teletrabajo**, en tiempos de **confinamiento**.

¿Cómo garantizar conexiones remotas seguras, proteger los dispositivos de teletrabajo, el uso seguro de la nube, las herramientas colaborativas, y la seguridad en movilidad?

Top 5 de las Políticas de Teletrabajo

Se sugiere que toda organización pueda establecer una política organizativa, en la que se definan las normas a cumplir en los distintos escenarios, o respecto al uso de los distintos sistemas y métodos de acceso.

Aquí te presentamos las 5 básicas:

1. **Relación de usuarios que disponen de la opción de trabajar en remoto:**
   Identificar y documentar qué usuarios, o personal, es o no candidato a trabajar vía remota.

2. **Aplicaciones y recursos a los que tiene acceso cada usuario:**
   Tendremos que definir cuidadosamente el tipo de acceso/credenciales que otorgaremos al personal. Todo dependerá de las aplicaciones y recursos que requiera para realizar su trabajo, y del rol que desempeñe en la organización.
   Se detallarán las aplicaciones colaborativas y de teleconferencia permitidas, así como sus condiciones de uso evitando utilizar programas no controlados por la empresa, práctica conocida como *Shadow IT*.

3. **Mecanismos de acceso seguro mediante contraseña:**
   Para las credenciales de acceso se utilizarán siempre contraseñas robustas y de ser posible con doble factor de autenticación, forzando su cambio periódico. Este mecanismo puede estar ligado a la gestión de cuentas de usuario y control de accesos.

4. **Configuración que deberán tener los dispositivos desde los que se establezcan las conexiones remotas:**
   Garantizar que el sistema operativo, antivirus, y software en general tenga las actualizaciones correspondientes, evitando usar equipos poco fiables y de uso común siempre que sea posible, tanto si son corporativos como si son aportados por el trabajador.

5. **Uso de conexiones seguras a través de una red privada virtual o VPN:**
   De este modo, la información que intercambiamos entre nuestros equipos viaja cifrada a través de Internet. Se ha de evitar el uso de aplicaciones de escritorio remoto si no es a través de una VPN.
   Estas herramientas pueden crear puertas traseras (*backdoors*), a través de las cuales podría comprometerse el servicio o las credenciales de acceso de usuario, y por lo tanto permitir el acceso a los equipos corporativos.

Campaña Institucional de Seguridad de la Información

CENTRO NACIONAL DE CÁLCULO MÉXICO I. P. N.

Instituto Politécnico Nacional
"La Técnica al Servicio de la Patria"