Prodana
Consultores

INFÓRMATE

Decálogo de ciberseguridad ante el teletrabajo por el Covid-19

Los recientes comunicados tanto del Ministerio de Sanidad como del Gobierno de distintas Comunidades Autónomas, cerrando colegios y aconsejando el teletrabajo en aquellas zonas donde exista un riesgo de transmisión más elevado del Covid-19, ha pillado en jaque a bastantes empresas y a la Administración Pública donde, hasta ahora, no se había planteado un escenario similar con tanta urgencia
En aquellos casos donde el teletrabajo sea posible, se deberían tener en cuenta ciertas medidas de seguridad, sobre todo, si los trabajadores van a utilizar sus dispositivos personales y no los corporativos.

A continuación, se desglosa un decálogo de recomendaciones mínimas en materia de ciberseguridad a la hora de implementar teletrabajo de manera urgente

- **Política de uso de medios tecnológicos:** la empresa debe implementar esta política, estableciendo qué puede hacer y qué no puede hacer el trabajador con los dispositivos y sistemas propiedad de la empresa (teléfonos móviles corporativos, portátiles corporativos, entre otros). Es esencial que en esta política se incluya si el trabajador tiene o no alguna expectativa de privacidad usando los medios corporativos.

- **Medios propios del trabajador:** en caso de que su empresa no disponga de dispositivos móviles corporativos, debe establecer una política de uso de medios propios que incluya requisitos de seguridad. Eso sí, recuerde que no puede imponer al trabajador la utilización de medios propios al servicio de la empresa.

Decálogo de ciberseguridad ante el teletrabajo por el Covid-19

- **Digitalización urgente:** el teletrabajo supone digitalización, abandono en la medida de lo posible del papel. Es necesario que aquella documentación en papel que necesite estar disponible en los próximos meses esté digitalizada y disponible. Utilice herramientas colaborativas entre sus trabajadores para facilitar la comunicación y la gestión de proyectos.

- **Sincronización:** utilice algún sistema para sincronizar lo que sus empleados guardan en los portátiles con los sistemas centralizados, de esa manera no perderá información.

- **Políticas de seguridad a través de un dominio:** es necesario que los equipos en régimen de teletrabajo sigan las mismas reglas que aquellos que están físicamente en las oficinas, de ahí la importancia de contar con un servidor de dominio que fuerce a dichos dispositivos a seguir las reglas internas de seguridad.

- **Cifrado en las comunicaciones:** las conexiones entre los dispositivos en régimen de teletrabajo y los servidores centrales deben estar cifradas. Para ello deberían establecerse redes privadas virtuales o VPN, o bien acceder por escritorio remoto.
  Si el acceso a las aplicaciones corporativas se realiza a través de internet, no olvide comprobar que la dirección de la web comienza con "https"(comunicación cifrada) y no "http" (no cifrada). Esa "s" es toda una diferencia. Las versiones más modernas de los navegadores avisan al usuario de que la navegación no es segura si la comunicación no está cifrada. Tenga en cuenta que el certificado utilizado de cifrado debe estar actualizado. No se debe hacer uso de redes WIFI abiertas o públicas.

- **Cifrado de dispositivos:** recuerde que teletrabajando la seguridad física de la oficina no existe. Es imprescindible que los dispositivos se encuentren cifrados en caso de pérdida o robo. Recuerde que todos los sistemas operativos más utilizados por la gran mayoría incluyen gratuitamente esta función:
  - Windows: escriba "Bitlocker" en la barra de búsqueda de Windows, y tendrá la opción de administrar esta funcionalidad.
  - Mac: OSX dispone de la función "Filevault" en Preferencias del Sistema - Seguridad y Privacidad
  - IOS: El cifrado del dispositivo está por defecto en el momento en el que usted establece un código de bloqueo para acceder al terminal.
  - Android: Puede cifrar su dispositivo en Ajustes - Seguridad - Cifrar teléfono.

- **Usuarios individuales:** es necesario abandonar los usuarios genéricos por varios motivos fundamentales. Entre estos, destaca la seguridad, ya que, si dispone de usuarios genéricos, no va a poder saber quién entra realmente al sistema. Adicionalmente las contraseñas deben ser robustas y deben caducar, o bien, implementar un sistema de doble factor. Aunque recuerde, el doble factor con envío de SMS no es precisamente seguro en muchos casos, es preferible a través de token o aplicación de autenticación. Recuerde además que el correo electrónico es una fuente inagotable de secretos empresariales, el acceso al mismo debe ser tan seguro o más que al resto de aplicaciones (incluida la caducidad de contraseña o doble factor).

- **Habilite la traza de auditoría en las aplicaciones y bases de datos,** de modo que pueda conocer quién hace qué en cada momento sobre los sistemas y aplicaciones.

- Los **sistemas operativos de servidores, portátiles y móviles deben estar actualizados** para evitar vulnerabilidades de seguridad que pudiesen ser aprovechadas por un tercero malintencionado.