FASTREANDO

Protege tus datos y trabaja desde casa de manera segura.

Resumen.
Durante los últimos años son más las empresas que se suman a la adopción del trabajo remoto o en alternancia, ya que esto brinda a los colaboradores mayores comodidades y beneficios. El trabajo remoto, conlleva a riesgos de ciberseguridad, especialmente si no se cuenta con una infraestructura informática adecuada que lo mitigue.

Riesgos de Seguridad Comunes en el trabajo desde casa:

- **Phishing:** La forma de atraer a la victima es hacerse pasar por alguna entidad de confianza que por medio de correo electrónico o mensaje de texto envían un enlace infectado que al abrirlo a tan solo un clic se instala involuntariamente malware o incluso ransomware en los computadores.

- **Contraseñas Débiles:** Las contraseñas débiles utilizadas por los colaboradores facilitan a los hackers el acceso no solo a sus computadores personales, sino también a los datos confidenciales de la empresa. Los atacantes utilizan diferentes métodos para piratear las contraseñas, sin embargo, la aplicación de buenas prácticas en la creación y almacenamiento disminuye el riesgo.

- **Redes Wifi no Seguras:** Al estar conectado en una red Wifi no segura, como la redes Wifi-públicas de cafeterías, hoteles, restaurantes, aeropuertos, entre otras; les facilita el trabajo a los ciberdelincuentes al momento de hackear los dispositivos para robar datos personales e información significativa para la empresa.

- **Uso de Dispositivos Personales para el Trabajo:** Aunque resulta ser más dinámico trabajar con los equipos personales, no se tiene en cuenta que estos dispositivos no están bajo las medidas de seguridad y la infraestructura de TI de la empresa, siendo así más vulnerables a las ciberamenazas. El hecho de visitar

cualquier sitio web que deseen e instalar cualquier aplicación o programa de software que, de otro modo, al no ser bloqueado de acuerdo con las políticas de seguridad y reglas activadas por el antivirus de la empresa, se convierte en un objetivo fácil para los hackers.

- **Compartir Archivos sin Encriptar:** El intercambio de archivos sin seguridad por medio de correo electrónico sin cifrar puede poner en riesgo los datos críticos de la empresa, se les facilita a los hackers interceptar y robar la información, el uso de unidades personales de almacenamiento en la nube e incluso el intercambio de archivos entre pares facilita que cualquiera pueda manipular y tener acceso a la misma.

Algunas recomendaciones de seguridad para trabajar desde casa:

- **Protege tu red Wifi:** Al estar conectado a una red inalámbrica se necesita de una contraseña para acceder a la red, por lo tanto, esta debe ser fuerte para determinar que el internet sea seguro. Una forma de minimizar el riesgo es cambiar la contraseña periódicamente.

- **Seguridad Física:** Lo ideal es tener bajo llave o en un espacio exclusivo todo lo relacionado con el trabajo, esto evitando que la información sea manipulada o que cualquiera pueda acceder con facilidad a los datos y archivos de la empresa.

- **Bloquea los dispositivos**: Así como por políticas de seguridad se debe bloquear el equipo cuando no se está presente en el sitio o espacio de trabajo, de igual manera aplica esta buena práctica en casa, evitando algún incidente que afecte el trabajo y minimizando el riesgo de exposición de la información.

- **Desactivar la transmisión de nombres de red**: Al momento de configurar la red Wifi, se puede elegir que el nombre de la red sea visible para todo aquel que tenga activado el WIFI, sin embargo, es mejor que sea invisible y que para conectarse, el usuario tenga que teclear el nombre de la red, si alguien intenta vulnerar la red, no será fácil hackearla, pues el primer paso es ver la red.