CONSEJOS TELETRABAJO Y SEGURIDAD

Estas semanas, por las circunstancias que todos conocemos, se ha vivido un éxodo de empleados -cuyas funciones lo permitían- desde sus lugares habituales de trabajo hacia sus domicilios.

En base a la preparación previa e infraestructura de cada compañía, este éxodo se ha materializado de una forma más o menos adecuada.

En el fondo, **las organizaciones han entregado una "ciberllave" de su empresa a cada uno de estos empleados, confiando que éstos hagan un uso adecuado y responsable de ella, esta "ciberllave"** permite acceso desde fuera de la empresa a determinados contenidos y servicios, muchos de ellos vítales y valiosos.

Apoyado en las buenas prácticas, contratos de confidencialidad y charlas de concienciación, confiamos que esta extraordinaria situación no genere otros inconvenientes diferentes a los propios de trabajar en un lugar que no es el habitual y usando métodos de comunicación menos directos que el diálogo verbal y cercano entre compañeros.

Interconectar redes domésticas -a menudo poco protegidas y descuidadas- con redes corporativas es algo serio, muchas veces, la mejor intención de cada usuario no es suficiente para garantizar la integridad y privacidad de servicios y datos.

Trataremos de compartir con ustedes una serie de medidas aplicables a cualquier entorno de teletrabajo:

- Siempre que sea posible, trataremos de llevar a los entornos domésticos, nuestros equipos de trabajo, preservando el perfil de conexión a red doméstica como de tipo "Público", de esta manera separaremos con mayor solidez el entorno corporativo y el doméstico.

- **Procuraremos evitar teletrabajar en una red pública o de terceros, compartida con desconocidos.**

- **Extremaremos precauciones frente al Phishing**, ya conocen el dicho de "a mar revuelto…", en esta situación extraordinaria, se constata un aumento de este tipo de prácticas fraudulentas, que siempre aumenta proporcionalmente al grado de uso de los medios digitales como servicios web y correo electrónico. Desconfíen de correo electrónico sospechoso, comprueben por otro modo de comunicación la veracidad de los mensajes, aunque sean enviados por contactos aparentemente reales, compruebe siempre la dirección del remitente, tómense tiempo en verificar la fuente, no regalen información.

- En su navegación por internet, revise la dirección por la que navega, **verifique que ésta sea segura** (https o candado cerrado a la izquierda de la misma).

- No emplee **contraseñas** fáciles u obvias, no guarde las contraseñas junto con el servicio que representa, no las comparta con otras personas.

- **Mantenga todos los sistemas y aplicaciones actualizados.** Un entorno informático al día cierra vulnerabilidades y puertas abiertas, detrás de los programas que emplea, hay personas que se equivocan -como todos- y para resolver esas equivocaciones que generan inestabilidad y mermas de seguridad, están los parches y actualizaciones, no las menosprecie, no los posponga.

- **Utilice antivirus en los equipos de trabajo, recuerde emplear uno de categoría corporativa**, los antivirus gratuitos no son malos, pero piense cómo esas empresas se cobran la gratuidad del trabajo que lleva desarrollarlos.

- **Realice copias de seguridad de su trabajo periódicamente,** dedíquele tiempo de vez en cuando a simular una restauración al azar de un documento.

Respecto al modo de interconectar hogar y oficina, existen varias técnicas, sin entrar en aspectos técnicos y buscando abarcar todos los entornos, siempre tenemos que procurar lo siguiente:

- **La comunicación entre el equipo de trabajo y la empresa ha de ser encriptada,** la información que viaja entre ambos puntos puede ser capturada y si no se encuentra codificada, será leída o escuchada por quien no debe. Imagine a alguien que acerca su oreja a la puerta de su despacho.

- **No se apoye en aplicaciones gratuitas basadas en web para confiar Teletrabajo,** la comunicación es más lenta, no garantiza un SLA ni alta disponibilidad, pueden comerciar con nuestros datos y debido a la alta demanda de este servicio, corremos el riesgo que estas empresas cambien sus reglas de juego. Este modo de trabajo, además, precisa que el ordenador de trabajo habitual se quede en la oficina, siempre encendido y acceda desde otro equipo desde fuera, ¿no sería mejor llevar el equipo de trabajo donde fuese necesario y disponer de un único ordenador conectado siempre de forma segura a los recursos que el servidor de la empresa ofrece?

- De nada vale tener la mejor infraestructura si ésta no se encuentra debidamente configurada. **Otorgue solo los permisos y servicios necesarios a cada empleado, haga que esa persona solo pueda conectarse a su zona de trabajo.** Cuando se activa un virus de tipo Cryptolocker, éste se propaga a lo largo y ancho que los permisos del usuario que lo activa le permite. Cuando toda medida de prevención falla, solo nos queda confiar en las medidas de restricción que hayamos otorgado.

- **Dispongan de herramientas corporativas que faciliten la comunicación entre empleados**, creando grupos de trabajo y compartiendo información entre ellos. **No confíe en sistemas de chat tipo "whatsapp", comercializan con la información que propagan.**

Desde nuestra división **IT Servicies**, le podemos ayudar a implantar el teletrabajo de una forma segura y ágil, poniendo a su disposición soporte telefónico y asistencia remota a cada uno de sus empleados para conseguir que todo funcione igual o mejor que antes.