Fujitsu da 10 consejos para la protección de datos de los teletrabajadores

En esta época de crisis a causa del **Coronavirus**, Fujitsu ha revelado algunos consejos útiles ya que la seguridad es uno de los temas que mantiene a los CIO despiertos por la noche por su preocupación por la pérdida o fuga de información sensible de diversos dispositivos del usuario.

Con el cierre de oficinas un alto porcentaje de **empleados trabajan ahora desde sus hogares**, por lo que, el **sistema de seguridad** se ha visto modificado para los profesionales de la información al acelerar el permiso del trabajo móvil y la colaboración entre equipos globales. Para los **profesionales de TI,** el desafío es proteger redes corporativas, datos y servicios mientras se habilita **fácil acceso a la información, rapidez y eficiencia en la comunicación** para impulsar la productividad.

Cada organización debe **evaluar y analizar sus políticas de seguridad** contra las amenazas actuales y futuros entornos para identificar dónde están los controles adicionales necesarios, siempre teniendo en cuenta la necesidad de equilibrar la seguridad con el acceso. Entonces se trata de gestionar el **riesgo creciente en estos entornos laborales remotos**. Es importante identificar el equilibrio adecuado para cada empresa. Conozca estos pasos prácticos:

1.- **Usa contraseñas inteligentes.**

Si los ladrones se apoderan de un dispositivo, ya sea digital o físicamente: necesitan crear una identidad y acceso robusto con contraseñas seguras, diferentes para cada cuenta y para cambiarlas regularmente.

2.- **Usa biometría que incluso es más inteligente que las contraseñas.**

Los sensores integrados en los portátiles para leer huellas dactilares ofrecen una alternativa más segura, y mejoran la experiencia del usuario al reemplazar múltiples contraseñas. Se sugiere usar más tecnologías biométricas avanzadas como Fujitsu PalmSecure, sistema que autentica las identidades de los usuarios al reconocer patrones de las venas de la palma de la mano que son exclusivas del individuo.

3.- **Haz una copia de seguridad de los datos y elimina la información de las unidades usadas.**

Para garantizar que la protección de datos sea completamente a prueba de auditorías es vital contar con la limpieza adecuada del disco, ya que los datos almacenados en discos duros antiguos no se eliminan correctamente, o no se eliminan en absoluto.

4.- **No dejes que los ladrones se apoderen de sus datos.**

¿Y si uno de sus dispositivos es robado? Evalúa soluciones avanzadas de protección contra robos que rastrean dispositivos y emiten alertas de manipulación de forma automática o permitan borrar de forma remota datos confidenciales.

5.- **Mantente actualizado y sigue poniendo parches.**

Los equipos deben ser configurados para actualizaciones automáticas del funcionamiento del sistema, software, controladores y BIOS para eliminar vulnerabilidades de seguridad, y protegerse contra malware y virus.

6.- **Bloquear dispositivos.**

Una cerradura de seguridad en portátiles ofrece una buena práctica para evitar robos. Se sugiere personalizar los equipos para que sean menos atractivos para los ladrones.

7.- **Proteger claves de cifrado.**

Tu próxima línea de defensa es cifrar archivos valiosos e información sensible. Pero si la clave de cifrado está almacenada dentro del dispositivo, puede ser pirateado y utilizado para descifrar tu información. La tecnología SmartCard es ideal para generar y almacenar claves de cifrado, en combinación con PIN o huella digital también se puede utilizar para protección de acceso.

8.- **Cifrar todo el disco.**

Para máxima seguridad, el cifrado de disco completo es la respuesta. Esto debe realizarse dentro del BIOS en lugar del sistema operativo.

9.- **Administra la seguridad en dispositivos propiedad del usuario.**

A medida que más dispositivos personales acceden a datos y servicios corporativos, se abren nuevos agujeros de seguridad. Para mantener estas brechas cerradas, un dispositivo móvil robusto necesita un sistema de gestión. Una alternativa es implementar una solución de infraestructura de escritorio virtual, para que los datos confidenciales se almacenen en un servidor seguro en lugar de que estén en los dispositivos del usuario.

10.- **Crea un plan de acción.**

Como mencionamos, primero debes evaluar tu seguridad de información para establecer dónde se puede fortalecer la protección. Una vez que sepas dónde están las brechas, necesitas claramente definir lo que hay que hacer para lograr las mejores prácticas de seguridad de información. Es importante en esta etapa establecer equilibrio entre la seguridad más estricta y la experiencia de usuario perfecta que los empleados necesitan para colaborar y mantenerse productivos.