oesia
grupo

TELETRABAJO

Medidas de seguridad necesarias para asegurar la continuidad de negocio

2020

TELETRABAJO

Medidas de seguridad necesarias para asegurar la continuidad del negocio

El teletrabajo ha pasado de ser una opción a una necesidad, por ello recomendamos una serie de medidas con el fin de aumentar la seguridad en el trabajo en remoto y su eficacia.

El hecho de tener que trabajar desde el mismo espacio físico en el que habitualmente dedicamos para descansar o realizar actividades de ocio, supone un reto. Por ello, recomendamos diversificar el espacio, en caso de ser posible, y diferenciar las zonas dedicadas a descanso y ocio de las de trabajo. Otra recomendación es mantener la rutina con la que previamente acudíamos a la oficina, como, por ejemplo, una ducha antes de empezar a trabajar, cambiarnos de ropa para asimilar que las funciones son distintas, seguir los horarios de la jornada, etc.

Desde **Grupo Oesía** trabajamos para que el teletrabajo se realice de forma segura y para ello ofrecemos una serie de recomendaciones para aumentar la seguridad de todos nuestros dispositivos y garantizar la continuidad de negocio, clave para todos los actores sociales en estos momentos.

Recomendaciones de Seguridad para profesionales:

- **Utilización de contraseñas robustas:** la renovación periódica de contraseñas y la condición de que estas sean robustas aumenta la seguridad, sobre todo en aquellos recursos que contengan información esencial.
- **Eludir la suplantación de identidad (Phishing):** estos días especialmente hemos de tener cuidado con la comunicación electrónica que recibimos.

Hemos de verificar el remitente, enlaces incluidos en el mensaje, contenido adjunto que podamos encontrar y el propio contenido del mensaje, puesto que los ciberdelincuentes usan la ingeniería social lograr sus objetivos.

- **Segregación de funciones en los dispositivos:** es lógico, sobre todo al principio, no diversificar funciones con nuestros dispositivos al teletrabajar en el mismo espacio físico en el que estamos acostumbrados a descansar o realizar actividades de ocio. Sin embargo, este hecho es vital para proteger nuestros dispositivos de trabajo y a la propia organización. Cada dispositivo tiene una función específica y tenemos que diferenciar bien lo que podemos y lo que no podemos hacer con cada dispositivo, puesto que el endpoint únicamente se usa para trabajar. Nunca debemos combinar nuestros diferentes dispositivos con las distintas utilidades que puedan ofrecernos.
- **Proteger nuestra Red Wifi:** es esencial cambiar periódicamente la contraseña de nuestra red Wifi con el objetivo de que nadie ajeno al domicilio tenga acceso a esta. La utilización de otro tipo de redes como Bluetooth o NFC también supone un riesgo para los activos de la organización. Hemos de asegurarnos que las redes con las que trabajamos son seguras y permiten que la información manejamos este a salvo.
- **Actualización de dispositivos y Software**: mantener los dispositivos y aplicaciones o programas actualizados tal y como nos advierten los fabricantes de software o sistema operativo es esencial para aumentar la seguridad en el puesto de trabajo. Esta pequeña acción corrige las vulnerabilidades conocidas y mantiene seguro los dispositivos de la organización.
- **Conexión segura**: trabajemos siempre de forma segura, utilizando las redes VPN (Red Privada Virtual) proporcionadas por la organización para acceder a los recursos necesarios a la hora de desempeñar el trabajo.

Recomendaciones de Seguridad para empresas:

- **Verificar**: no supongamos nada, verifiquemos. Hemos de comprobar la información, quién tiene acceso a la misma, quién puede dar dichos accesos y asegurarla mediante la autenticación multifactor.
- **Protección de los Endpoint**: debemos anticiparnos a la actividad de los cibercriminales. Enfrentarse a amenazas como la fuga de datos e información empresarial o los distintos tipos ataques a dispositivos que acaban en la red de la organización es esencial para garantizar la continuidad de negocio y colaborar estrechamente con la situación que sufrimos en la actualidad.
- **Pruebas de resistencia a la infraestructura**: igual que surge la necesidad de proteger los dispositivos, es necesario realizar pruebas a la infraestructura que colaborara con dicha protección. El uso de VPN o SDP es esencial para garantizar la continuidad de negocio en estos momentos de teletrabajo, y se recomienda encarecidamente la realización de test o pruebas de esfuerzo y estrés, para asegurar que la infraestructura permite el volumen de tráfico generado por los dispositivos conectados.
- **Definición de permisos y datos**: clasificar los datos e información de la organización es esencial para reducir la superficie de ataque por parte de ciberdelincuentes. De la misma forma, escoger que profesionales pueden acceder a cada tipología de datos reduce, de nuevo, la superficie de ataque.

Contacte con nosotros
si quiere asegurar sus servicios en la nube:

cert@oesia.com

Ciberseguridad | oesia

ciberseguridad.oesia.com