arsys

# Cómo implementar el teletrabajo seguro en la empresa

Consideraciones básicas que tener en cuenta al implementar el teletrabajo en la empresa: política, objetivos, amenazas, métodos de acceso.

El teletrabajo está cada vez más asentado entre empresas y trabajadores que, a raíz de la pandemia del coronavirus, han acelerado su adopción y pueden disfrutar de sus ventajas y beneficios.

Algunas de estas ventajas son la conciliación de la vida familiar y laboral, el ahorro de costes fijos que se produce al necesitar menos espacio físico en las oficinas o su impacto positivo en el medio ambiente al reducirse el uso de desplazamientos en vehículos privados. Además, también favorece la productividad de los trabajadores.

Pero no todo es color de rosa. O, al menos, no lo es si no se toman las medidas adecuadas y no se planifica correctamente el teletrabajo. En esta guía vamos a tratar de ordenar todo lo que se ha de tener en cuenta al implantar el teletrabajo en una empresa. Si no se aplican buenas políticas podemos multiplicar los riesgos para la privacidad y seguridad de la empresa.

# Definir una buena política de teletrabajo

Las políticas bien definidas tienen la virtud de ser las mejores guías posibles para evitar problemas. Por eso, una buena **política de teletrabajo** debe especificar todos los aspectos técnicos y organizativos que lo definen.

En la política debe detallarse todo de una manera muy clara y con un lenguaje sencillo y práctico, de manera que no haya ninguna duda o ambigüedad sobre lo que se está estableciendo. Entre otras cosas, debemos incluir los usos permitidos de los servicios empresariales, así como las características y configuraciones de todas las tecnologías implicadas en el acceso remoto. Por ejemplo:

- Qué tipo de dispositivo se va a utilizar
- Las redes a las que se permite acceder
- En qué franjas horarias se pueden utilizar los dispositivos
- Si se permite la wifi doméstica, o no, y qué se debe hacer para que sea segura.

Es la única manera de tener un guion rápido que todos los empleados pueden seguir para mantener la seguridad de los datos y las conexiones.

# Los objetivos de seguridad, bien claros

Otro punto clave para el teletrabajo es la especificación de los objetivos de seguridad que se deben cumplir a toda costa. La posibilidad de trabajar en remoto es muy atractiva, pero ya sabemos que, por desgracia, **el factor humano sigue siendo decisivo** cuando hablamos de ciberataques.

Además, este punto aplica también al trabajo presencial porque el principal objetivo será proteger la seguridad de la información. Es necesario garantizar:

- La disponibilidad, es decir, que se pueda acceder a los recursos siempre que sea necesario.
- La autenticidad, o lo que es lo mismo, se debe garantizar que la información está libre de modificaciones no autorizadas.
- La integridad, lo que garantiza que los datos son legítimos, que no han sido modificados o alterados sin permiso. Es una característica similar a la anterior, pero en esta dimensión se incluye a los datos en tránsito (es decir, que no pueden ser modificados en el tránsito, directa o indirectamente).
- Confidencialidad, por la cual se garantiza que la información sólo puede ser accedida por el personal autorizado.
- Trazabilidad, que es la característica que permite llevar un registro de toda la actividad sobre un determinado activo, desde el acceso, pasando por la manipulación, los cambios o cualquier otra acción.

# Conocer las amenazas

Hay que estar familiarizados con los principales **términos asociados a la ciberseguridad**, y conocer muy bien aquellas amenazas que pueden poner en riesgo los datos y a la propia empresa.

Debemos tener presentes temas tan decisivos como:

- La correcta configuración de redes, dispositivos y software.
- Los controles de acceso físico a los dispositivos utilizados en remoto.
- Los accesos no autorizados y la pérdida (o robo) de los dispositivos.
- La falta de formación del personal.
- El uso de aplicaciones colaborativas o almacenamiento Cloud (entre otras cosas) no autorizados en la política IT.

Las amenazas son múltiples, por tanto, cuantas más seamos capaces de detallar, mejor preparados estaremos.

# La protección de los dispositivos

Aunque es el último punto, no es el menos importante. Es necesario dotar a los dispositivos de todas las herramientas necesarias para **garantizar su seguridad** desde cualquier ubicación. De la misma manera, los servidores de acceso para los teletrabajadores deben contar con todas las capas de protección disponibles.

# Especificar los métodos de acceso remoto

No hay teletrabajo sin métodos de acceso remoto, por eso es imprescindible no dejar este punto al azar. Sólo se puede teletrabajar accediendo a los sistemas de la manera que se especifique en la política IT de la compañía. Si dicha regulación establece utilizar una **VPN y un servicio VDI** con controles de acceso específicos, esa será la única manera de trabajar en remoto.

arsys

www.arsys.es

www.facebook.com/arsys.es

twitter.com/arsys

www.linkedin.com/company/arsys-internet/

www.instagram.com/arsys.es/