Temáticas para el Teletrabajo

El teletrabajo es una alternativa cada vez más utilizada por todo tipo de empresas.

Sus beneficios son amplios, desde aprovechar el talento remoto hasta facilitar la conciliación familiar, pasando por mejoras para los trabajadores en movilidad o para los que ofrecen soporte en el cliente. Pero implementar esta modalidad puede entrañar riesgos para la privacidad y seguridad de la empresa si no se aplican una serie de políticas y recomendaciones.

Por ello, y para mantener la seguridad de tu organización en unos niveles adecuados, debes tener en cuenta las siguientes consideraciones si deseas implementar el teletrabajo en tu empresa.

Definir la política de teletrabajo

Cuando la empresa permite a los empleados teletrabajar, es recomendable elaborar una política para tal fin, con el objetivo de especificar los aspectos técnicos y organizativos que definen el teletrabajo en la empresa. Es una buena práctica establecer de forma clara los usos permitidos de los servicios empresariales, y las características y configuraciones de las tecnologías que se han de utilizar para el acceso remoto, como: tipo de dispositivo, redes permitidas, franjas horarias, wifi doméstica, etc. Si estos requisitos no están descritos en la política de teletrabajo, la empresa **puede llegar a sufrir un incidente de seguridad,** comprometiendo la privacidad de la información y de los clientes.

Las siguientes políticas de seguridad serán de ayuda a la hora de elaborar las normas y directrices que debe seguir la empresa y sus empleados a la hora de teletrabajar.

Objetivos de seguridad

Independientemente de si el trabajo se realiza en la sede de la empresa o en la modalidad de teletrabajo, el **principal objetivo** será proteger la seguridad de la información. Para ello se deben asegurar las cinco dimensiones sobre la que se sustenta la ciberseguridad:

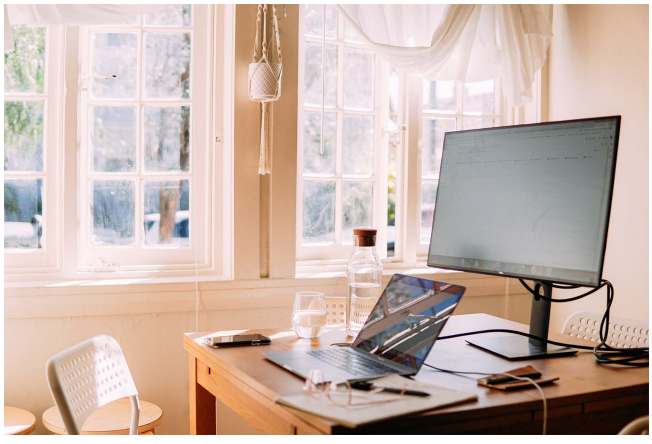
- Disponibilidad: asegurar el acceso a los recursos cuando sea necesario.
- Autenticidad: garantizar que la información está libre de modificaciones no autorizadas.
- Integridad: es la propiedad de la información por la que se garantiza que los datos son legítimos, es decir, no han sido modificados o alterados sin permiso.
- Confidencialidad: se garantiza que la información únicamente es accesible por personal autorizado.
- Trazabilidad: permite llevar un registro de la actividad llevada a cabo sobre un determinado activo.

Amenazas

Habilitar el teletrabajo en la empresa abre la puerta a nuevas amenazas que pueden afectar a la seguridad y privacidad de la información, tanto de los dispositivos cliente como de los servidores, las principales que deben tenerse en cuenta son:

• Ausencia de controles de seguridad física: cuando se teletrabaja, los dispositivos pueden quedar expuestos a personas que no deben tener acceso a los mismos, como por ejemplo en hoteles, salas de espera o incluso en casa. Es importante **aplicar las medidas de seguridad necesarias** para evitar accesos no autorizados a estos dispositivos y a la información que gestionan, como habilitar una clave de desbloqueo o el cifrado de la información almacenada en el dispositivo.

• Errores de configuración: el software que permite el teletrabajo, tanto en dispositivos cliente como servidores, debe estar configurado siguiendo unos requisitos de seguridad. Por ello es recomendable que lo realice **personal especializado.**



• Redes inseguras: cuando se teletrabaja, es habitual utilizar redes consideradas inseguras ya que no están bajo el control de la empresa. Para evitar accesos no autorizados a la información en tránsito es recomendable utilizar soluciones VPN, las cuales **protegen toda la información** en tránsito incluso en redes inseguras como redes wifi públicas.

• Dispositivos inseguros: el uso de dispositivos inseguros, bien sean propiedad de la empresa o del empleado en BYOD, pueden suponer un riesgo. Las principales amenazas a tener en cuenta son la **infección por malware y el software desactualizado,** por ello hay que contar con antivirus en todos los dispositivos y todo el software actualizado a la última versión disponible.

• Accesos no autorizados: permitir el acceso a sistemas corporativos a través de Internet siempre entraña riesgos, y el teletrabajo no es una excepción. Desde empleados sin autorización a ciberdelincuentes, todos ellos pueden intentar acceder de forma fraudulenta a la información corporativa. Para evitarlo se deben habilitar **mecanismos de autenticación robustos** y, siempre que sea posible, habilitar un doble factor de autenticación.

• Falta de formación: la falta de formación o conocimiento de las políticas de seguridad de la empresa por parte de los empleados pueden poner en r**iesgo la seguridad de la información.**

• Software desactualizado o fuentes no confiables. No mantener actualizado el software tanto de los dispositivos cliente, como de los servidores que corporativos, incluidos los que permiten llevar a cabo el teletrabajo, puede suponer un riesgo para la seguridad de la empresa. De igual forma, instalar software no autorizado o procedente de fuentes no legítimas **puede suponer el origen de un incidente de seguridad.**

• Robo, pérdida o destrucción del dispositivo. Los dispositivos que permiten el teletrabajo, sobre todo aquellos utilizados por trabajadores con movilidad, se caracterizan por ser portátiles y de tamaño y peso contenidos. Estas características los hacen **susceptibles a pérdidas y robos,** lo que puede suponer un riesgo para la información gestionada si esta no está protegida adecuadamente.

• Aplicaciones colaborativas. Las aplicaciones colaborativas, además de permitir interactuar con otros empleados de la empresa o colaboradores, **pueden suponer un riesgo si no están configuradas adecuadamente** ya que pueden abrir la puerta a los ciberdelincuentes.

• Almacenamiento cloud. Utilizar servicios de almacenamiento en la nube que no han sido aprobados en la política de la empresa, o utilizarlos sin seguir unas medidas de privacidad mínimas **pueden poner en riesgo la información que se almacena.**

Métodos de acceso remoto

Para permitir el acceso remoto de los empleados a los recursos corporativos, existen varias opciones, siendo **las más utilizadas el uso de VPN o redes privadas virtuales** en combinación con otros sistemas, como VDI «virtual desktop infrastructure», acceso a través de escritorio remoto, portales de aplicaciones y acceso directo a aplicaciones.

Seleccionar la opción más adecuada para la empresa es crucial, considerándose las implicaciones de seguridad de cada método y si cumple con los requisitos de seguridad necesarios para llevar a cabo las tareas corporativas que van a realizarse en remoto.

Protegiendo el servidor y los dispositivos cliente

Tanto los servidores que permiten el acceso remoto a los recursos empresariales, como los dispositivos utilizados por los empleados, deben contar con ciertos requisitos de seguridad que eviten accesos no autorizados a la información corporativa.

La propia formación de los empleados, aplicar una política de actualización de software o configurar adecuadamente la red doméstica son algunas de las consideraciones a tener en cuenta y que permitirán teletrabajar **bajo los mismos requisitos de seguridad** que si se estuviera haciendo desde la sede empresarial.

Fuente de información: www.incibe.es