

SEGURIDAD Y TELETRABAJO



SEGURIDAD Y TELETRABAJO. LA UNIÓN HACE LA FUERZA

Si bien el teletrabajo ya era un concepto que se estaba empezando a implementar paulatinamente en las empresas, en poco tiempo y por diversas circunstancias, **muchas organizaciones se han visto obligadas a implementar este modelo de trabajo.**

El teletrabajo ha llegado a la vida de muchos trabajadores de manera acelerada para poder dar continuidad a los negocios en el marco de la transformación digital. Es a causa de esta aceleración que **es vital juntar los conceptos de teletrabajo con seguridad** para un buen funcionamiento.

Estamos en un momento donde la digitalización ha venido para quedarse y más ahora, cuando las circunstancias lo permiten. Muchas empresas han tenido que adaptarse rápidamente a tener a su totalidad de la plantilla distribuida y que el empleado empezara a realizar sus trabajos desde casa. **Se ha realizado este cambio drástico al teletrabajo sin ser conscientes de todas las implicaciones que tiene y de las vulnerabilidades que crea**, más en un momento donde los ciberataques no paran de aumentar.

“El cibercrimen es el delito número 1 en el mundo. En España, el número de ataques a PYMES aumentó un 186%. Los incidentes alcanzan un número de 55 billones.”

Fuente: OCDE (Organización para la Cooperación y el Desarrollo Económicos)





El aumento de trabajadores que ahora mismo teletrabajan no ha parado de aumentar, llegando prácticamente a su totalidad. Esta implementación que, en un principio se quería realizar de manera escalonada, ha terminado siendo una obligación para muchas empresas.

Esto ha causado una incertidumbre inicial para muchas empresas, que se han visto obligadas a que sus trabajadores trabajen desde casa sin precedente alguno. **Ni la empresa ni el empleado se sentían preparados para realizar el cambio, pero se han visto forzados a aceptarlo.**

"El 79% de los trabajadores ya realizan teletrabajo."

Fuente: Estudio global sobre teletrabajo PGI

"El 78% de los españoles se declara satisfecho con esta modalidad."

"El **teletrabajo** se sitúa como un **criterio decisivo** a la hora de elegir un empleo."

Fuente: El Economista

Desde un inicio de la pandemia, para proteger y tratar de evitar todas las vulnerabilidades creadas por la situación, fue esencial juntar la idea de teletrabajo con seguridad ya que, en general, **desde casa los trabajadores no tienen la seguridad y muchas de las facilidades que en la oficina o en las instalaciones de la empresa sí tienen.**



- No tienen las mismas **instalaciones** y la misma **red segura** que hay en la empresa.
- El material cambia si la empresa no cede **material informático**.
- Cambia la **comunicación entre empleados y superiores** (se digitaliza la comunicación).
- No hay la misma **seguridad** y se pierde **control digital**.





Es por eso que, con la implementación del teletrabajo, las empresas deben ser más cuidadosas y precavidas con sus trabajadores y **dotar a toda la organización con seguridad y protocolos** adecuados para así evitar problemas futuros o tratar de no crear nuevas vulnerabilidades antes inexistentes.

¿Cómo aplicar un plan de acción para garantizar la ciberseguridad en el teletrabajo?

Actualmente el cómo aplicar un plan de acción para garantizar la ciberseguridad en el teletrabajo es uno de los mayores retos a los que se enfrentan las organizaciones y, en concreto, los equipos de IT. A causa de la aplicación del teletrabajo **las aplicaciones, los datos, los usuarios y sus dispositivos están saliendo de la zona de control de la empresa** por lo que la probabilidad de ser atacados es mayor, aumenta exponencialmente.

"El 76% de los encuestados espera un **aumento en el acceso en remoto** en el corto plazo."

Fuente: estudio IDC

Desde Tranxfer queremos recordaros las claves para la seguridad en el teletrabajo:

● Establecer una conexión segura VPN

Los empleados necesitan acceder de manera remota a la información y a los recursos almacenados en las redes corporativas. Por eso es vital poder establecer una conexión segura para que nadie pueda acceder a esta información. **Es importante crear una red privada virtual o VPN como solución a problemas de red y así evitar posibles vulnerabilidades.** Con el uso de VPN se podrá proteger la información que transita entre el cliente y el servidor.





● Evitar BYOD

El concepto de **Bring Your Own Device (BYOD)** se está popularizando y esto supone un problema para el personal de IT, ya que tienen menos control sobre los dispositivos que los usuarios utilizan para acceder a las aplicaciones y datos corporativos. Cuando el trabajador usa un dispositivo personal, el cual también usa de manera lúdica, pone en peligro a la organización. Para una buena seguridad en el teletrabajo **la empresa debería brindar a cada uno de sus empleados los dispositivos electrónicos necesarios para que se usen exclusivamente para trabajar.**

● Doble autenticación

Por parte de la empresa y del empleado será vital hacer una **autenticación del contenido que se manda y se abre.** Con esto se logra que solo las personas elegidas puedan acceder a la documentación enviada. También será necesario verificar quién entra en cada dispositivo y en los distintos contenidos de la empresa.

● Zero Trust

El concepto Zero Trust parte de la idea de que **las organizaciones no tendrían que confiar en ninguna entidad interna o externa** que entre en su perímetro. Asume que puede haber atacantes tanto dentro como fuera de la red.



● Cifrado de comunicaciones

El cifrado de comunicaciones es el **proceso de codificación o encriptación de datos** para que sólo pueda leerlo alguien con los medios para devolverlo a su estado original. Con este cifrado se logra que el receptor pueda acceder a la información solo si es la persona que el remitente decide.

¿CÓMO TRANXFER PUEDE AYUDAR A SOLUCIONAR ESTOS PROBLEMAS?

Con el uso de Tranxfer se pueden **solucionar muchos de los problemas planteados con anterioridad y lograr seguridad en el teletrabajo**. Tranxfer ofrece:



● Envío y recepción de archivos de forma segura

Tranxfer asegura el **envío y la recepción de archivos** de la manera más segura y con trazabilidad gracias a sus características técnicas.

● Elige tus preferencias de envío y visualización

Con Tranxfer se puede **elegir y privar a usuarios de ver documentos** para tener un control total de todos los archivos y documentos que se envían. También se puede hacer uso del **módulo de "sólo visualización"** donde se generará una marca de agua en los documentos de manera automática y el receptor sólo podrá ver los archivos, ni descargarlos ni editarlos.

● Previene la entrada y salida de Malware

Tranxfer contiene un **Antivirus Integrado** para **prevenir malwares**. Este está en actualización constante, funciona con multiproceso flexible y escalable y hace uso de un escáner de línea de comandos y herramienta avanzada.



● Controla la fuga de información

Con el **módulo DLP** de Tranxfer se logra **controlar y evitar la salida no autorizada de información** fuera de la compañía. Este módulo constituye una barrera de seguridad para prevenir fugas de información no deseadas, ya sean voluntarias o involuntarias.

¿CÓMO TRANXFER PUEDE AYUDAR A SOLUCIONAR ESTOS PROBLEMAS?

● Encriptación end to end (E2E)

Con la **encriptación E2E** Tranxfer logra **mantener la confidencialidad e integridad de los archivos** de extremo a extremo. Blindamos de E2E las transferencias empleando técnicas de **Firma Digital** para así garantizar que se dispone de la versión genuina del archivo.

● Doble factor de autenticación

Tranxfer hace uso del doble factor de autenticación **vía correo electrónico o SMS** para garantizar que los documentos o archivos lleguen al receptor adecuadamente.



● Plugin de O365

El Plugin de Office 365 sirve **para trabajar de forma integrada en el correo del usuario** y así hacer el teletrabajo más sencillo y eficiente. Con este plugin también evitas tener programas en funcionamiento de manera innecesaria.

Desde Tranxfer nos gusta mucho una frase que dijo **Miguel Monzó, nuestro Chief Technology Officer**, que define perfectamente cómo se debe relacionar teletrabajo, o trabajo en general, con seguridad. Dice lo siguiente:

“Las claves de la seguridad empiezan y terminan con la concienciación del empleado.”

Fuente: Miguel Monzó Montes, Chief Technology Officer de Tranxfer



¡OFRECE TRANXFER!

Con TRANXFER podrás proteger a tu organización de forma fácil

- Enviar **archivos y recibir archivos sin límite de peso, y de forma segura.**
- La herramienta ofrece **trazabilidad y auditoría continua**; monitoring, acuse de recepción, lecturas y/o descargas.
- Políticas avanzadas de seguridad y una interfaz de usuario y administrador de fácil uso, en versión **web o plugin O365.**
- Disponemos de **API y Plugins** para integrar en otros sistemas.
- Podemos integrarnos con el **SIEM, Active Directory** y ofrecemos distintas modalidades de despliegue.

Fugas de información | Incumplimiento de GDPR | Entrada de malware

 Envío de archivos por parte de usuario y descargas por parte de destinatarios protegidas con certificado de navegador https.	 Opción de sólo visualización del archivo, con marca de agua personalizada por destinatario.	 Acuse de recibo. Evidencia de acceso, descarga, visualización y expiración. Trazabilidad total extremo a extremo.
 Encriptación extremo a extremo y "zero knowledge".	 Doble factor de autenticación, vía correo electrónico o SMS.	 Módulo DLP de protección de pérdida de información. Control de destinatarios y contenidos.
 Módulo de reporting completo de seguimiento de actividad que permite control y análisis de la actividad diferenciando por usuarios, grupos, destinatarios, información enviada, etc...	 Todos los archivos enviados son escaneados por Antivirus integrado en la plataforma.	 Eliminación automática de archivos tras periodo de expiración del envío. No hay opción a vulnerabilidades o accesos no autorizados.
 Certificación de contenido por checksum/hash para identificación unívoca del archivo		

¿QUIERES UN FREE TRIAL? - Contáctanos para mas info



La herramienta preferida de los CISOs para luchar contra el **Shadow IT** y reforzar su plan de director de seguridad para el intercambio de archivos

- Envía y recibe archivos de forma segura
- Elige tus preferencias de envío y visualización
- Previene la entrada y salida de Malware
- Controla la fuga de información
- Encriptación end to end



Más de **1 millón** de usuarios licenciados
Más de **5 millones de receptores**

Contáctanos para más información: info@tranxfer.com

O a través de nuestras redes sociales:



<https://www.linkedin.com/company/tranxfer>



<https://twitter.com/tranxfer>