Ciberseguridad en el teletrabajo

Una guía de aproximación para el empresario

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa

ÍNDICE

ÍNDICE

1 INTRODUCCIÓN

Se puede definir el teletrabajo como la actividad laboral que se desarrolla desde otros lugares que no sean las propias instalaciones de la organización.

Los teletrabajadores pueden utilizar varios terminales también conocidos como *endpoints*, como ordenadores de sobremesa, portátiles, teléfonos inteligentes o tabletas, para leer y enviar correo electrónico, acceder a sitios web, crear y editar documentos, así como otras muchas tareas propias de su labor diaria. Estos dispositivos pueden ser controlados por la organización, por terceros (contratistas/prestadores de servicios, interlocutores comerciales o proveedores de la organización) o por los propios usuarios cuando utilizan sus dispositivos para trabajar, lo que se conoce como BYOD[1]. La seguridad del teletrabajo también se ve afectada por el uso de estos dispositivos y de otros medios de almacenamiento extraíbles (memorias usb, discos duros, etc.), así como por el uso de aplicaciones en la nube y mecanismos de acceso remoto a la red y servidores de la empresa.

La mayoría de los teletrabajadores utilizan el acceso remoto (a través de VPN, escritorio remoto, etc.), lo que permite que los usuarios de una organización puedan acceder a los recursos informáticos de la empresa desde ubicaciones externas distintas de las instalaciones de la empresa.

A lo largo de este documento explicaremos las distintas medidas necesarias para garantizar conexiones remotas seguras, proteger los dispositivos de teletrabajo, el uso seguro de la nube y las herramientas colaborativas y la seguridad en movilidad.

1 El modo de trabajo en el que se permite la utilización de dispositivos móviles personales para acceder y utilizar los recursos corporativos es lo que se conoce como BYOD (por sus iniciales en inglés, Bring Your Own Device, tráete tu propio dispositivo). Para más información consulta: Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario

2 POLÍTICA DE TELETRABAJO

Si queremos disponer de un entorno de teletrabajo seguro, el primer paso será establecer una política organizativa en la que se definan las normas a cumplir en los distintos escenarios o respecto al uso de los distintos sistemas y métodos de acceso. Esta política deberá contemplar distintos aspectos, como los siguientes, siempre teniendo en cuenta que cada organización tendrá sus necesidades particulares. Estos son algunos elementos que ha de definir esta política:

- **Relación de usuarios que disponen de la opción de trabajar en remoto.** Será necesario llevar un control de las personas que por su perfil dentro de la empresa o las características de su trabajo tienen la opción de teletrabajar.

- **Procedimientos para la solicitud y autorización del teletrabajo.**

- **Aplicaciones y recursos a los que tiene acceso cada usuario.** Cada usuario tendrá acceso solo a las aplicaciones y recursos que requiera para realizar su trabajo, dependiendo del rol que desempeñe en la empresa. Se detallarán las aplicaciones colaborativas y de teleconferencia permitidas así como sus condiciones de uso evitando utilizar programas no controlados por la empresa, práctica conocida como Shadow IT[2] .

- **Mecanismos de acceso seguro mediante contraseña.** Para las credenciales de acceso se utilizarán siempre contraseñas robustas y el doble factor de autenticación siempre que sea posible, y forzando su cambio periódico. Este mecanismo puede estar ligado a la gestión de cuentas de usuario y control de accesos a través de servicios de directorio[3] LDAP[4] .

- **Configuración que deberán tener los dispositivos desde los que se establezcan las conexiones remotas:** sistema operativo, antivirus, control de actualizaciones, etc., tanto si son corporativos como si son aportados por el trabajador (BYOD). En el caso del BYOD, podemos controlar su configuración a través del *fingerprinting* de dispositivos, es decir, registrando una «huella di-

2 El término Shadow IT engloba dispositivos, *software y servicios de TI utilizados dentro de las organizaciones y los cuales se encuentran fuera de su propiedad o control*

3 Un servicio de directorio (SD) es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores y sobre los recursos de red que permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. https://es.wikipedia.org/wiki/Servicio_de_directorio

4 El protocolo ligero de acceso a directorios (en inglés: Lightweight Directory Access Protocol, también conocido por sus siglas de LDAP) hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. https://es.wikipedia.org/wiki/Protocolo_ligero_de_acceso_a_directorios

2

"Si queremos disponer de un **entorno de teletrabajo seguro**, el primer paso será establecer una **política organizativa** en la que se definan las normas a cumplir en los distintos escenarios o respecto al uso de los distintos sistemas y métodos de acceso."

gital» del dispositivo autorizado generada con datos de uso: navegador y *plugins* instalados, operador de telefonía, ubicación, horarios, etc.).

» **Procedimiento y tecnología para cifrar los soportes de información** para proteger los datos de la empresa de posibles accesos malintencionados y garantizar así su confidencialidad e integridad.

» **Definición de la política de almacenamiento en los equipos de trabajo [REF - 1] así como de almacenamiento en la red corporativa [REF - 2].**

» **Procedimiento y planificación de las copias de seguridad periódicas de todos los soportes** y comprobar regularmente que pueden restaurarse.

» **Uso de conexiones seguras a través de una red privada virtual** o VPN, del inglés *Virtual Private Network*, en lugar de las aplicaciones de escritorio remoto. De este modo, la información que intercambiamos entre nuestros equipos viaja cifrada a través de Internet. Se ha de evitar el uso de aplicaciones de escritorio remoto si no es a través de una VPN. Estas herramientas pueden crear puertas traseras *(backdoors*[5]*)* **[REF - 3]** a través de las cuales podría comprometerse el servicio o las credenciales de acceso de usuario y por lo tanto permitir el acceso a los equipos corporativos. Además, al usar este tipo de aplicaciones podemos estar aceptando ciertos términos y condiciones de uso que podrían otorgar algún tipo de «privilegio» a las mismas sobre nuestros equipos e información.

» **Virtualización**[6] **de entornos de trabajo** para eliminar los riesgos asociados al uso de un dispositivo propio.

» En el caso de utilizar dispositivos móviles para teletrabajar, la política debe incluir **la utilización de aplicaciones de administración remota [REF - 4].** Definir los criterios para evitar el uso de redes wifi públicas y utilizar las conexiones 4G/5G en su lugar.

» **Formar a los empleados [REF - 5]** antes de empezar a teletrabajar.

5 Puerta trasera: Se denomina *backdoor* o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.

6 La virtualización es la creación a través de software de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento o cualquier otro recurso de red. https://es.wikipedia.org/wiki/Virtualización

3 OBJETIVOS DE SEGURIDAD EN EL ACCESO REMOTO

Tanto si trabajamos en las instalaciones de la empresa como si teletrabajamos, debemos proteger el principal activo de la organización, **la información.** La seguridad de la información se articula sobre cinco dimensiones, que son los pilares sobre los que aplicar las medidas de protección:

- **Disponibilidad:** asegurar que los usuarios puedan acceder a los recursos cuando lo necesiten.
- **Autenticidad:** garantizar los procesos de autenticación y control de acceso para que solo las personas autorizadas puedan acceder a la información.
- **Integridad:** proteger la exactitud y estado completo de la información detectando cualquier cambio intencional o no intencional en las comunicaciones.
- **Confidencialidad:** asegurar que los datos almacenados por el usuario o en tránsito en las comunicaciones no puedan ser leídos por partes no autorizadas.
- **Trazabilidad:** establecer los procedimientos y mecanismos para proporcionar los datos necesarios que permitan llevar a cabo un análisis de seguridad en caso de sufrir un incidente.

Además de estas consideraciones, debemos tener en cuenta las principales leyes que afectan a la empresa desde el punto de vista de la seguridad de la información y cumplir con lo estipulado en las mismas **[REF - 6]**:

- La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE).
- La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) y el Reglamento General de Protección de Datos (RGPD).
- La Ley de Propiedad Intelectual (LPI).

3

"Tanto si trabajamos en las instalaciones de la empresa como si teletrabajamos, debemos **proteger el principal activo de la organización, la información.**"

Para lograr estos objetivos de seguridad, todos los componentes de las soluciones de teletrabajo y acceso remoto, incluyendo los dispositivos cliente[7], los servidores de acceso remoto y los servidores internos a los que se accede a través del acceso remoto, deben estar configurados correctamente para minimizar las posibles **amenazas** que se detallan a continuación:

- **Falta de controles de seguridad física:** en ciertas ocasiones los dispositivos destinados al teletrabajo se utilizan en lugares fuera de la organización como por ejemplo en hoteles, cafeterías, en salas de conferencias, etc. Esta condición aumenta el riesgo de que los dispositivos se pierdan o sean robados, lo que lo convierte a su vez en una posible pérdida de datos corporativos si no están convenientemente protegidos. Es muy importante tener en cuenta este tipo de situaciones a la hora de aplicar las medidas de seguridad necesarias para este tipo de dispositivos y proteger la información de accesos no deseados. **[REF - 7]**

- **Errores de configuración:** para asegurar una configuración óptima en nuestros equipos es aconsejable que únicamente el personal técnico indicado pueda instalar, actualizar y eliminar *software*.

- **Redes no seguras:** las organizaciones no tienen control sobre las redes que usan sus empleados para teletrabajar. Es una práctica habitual utilizar redes abiertas e inseguras (aeropuertos, cafeterías, etc.) que un ciberdelincuente podría aprovechar para acceder a la información que contiene el dispositivo utilizado para el trabajo en remoto.

- **Dispositivos infectados en redes corporativas:** la inclusión del BYOD en el ámbito empresarial ha sumado factores de riesgo, como el uso de dispositivos que están infectados con algún tipo de *malware* a consecuencia del uso personal. El problema surge cuando una vez infecta-

7 La arquitectura **cliente-servidor** es un modelo de diseño de software en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados **servidores**, y los demandantes, llamados **clientes**. Un cliente realiza peticiones a otro programa, el **servidor**, quien le da respuesta. https://es.wikipedia.org/wiki/Cliente-servidor

3

dos se conectan a la red de la empresa, pudiendo propagar el *malware* a otros dispositivos.

- **Acceso remoto a los recursos internos:** permitir el acceso externo a los recursos corporativos implica su exposición a nuevas amenazas, aumentando la posibilidad de que estos se vean comprometidos. Por este motivo, es necesario otorgar acceso a estos recursos solo a los empleados que lo necesiten para el desempeño de su trabajo.

- **Falta de formación:** es habitual que la falta de formación o de conocimiento de las políticas de seguridad de la empresa por parte de los empleados pongan en riesgo la seguridad de la información.

4 MÉTODOS DE ACCESO REMOTO

Existen varias opciones para proporcionar acceso remoto a los empleados de una organización, siendo las más utilizadas VPN, VDI, acceso a través de escritorio remoto, portales de aplicaciones y acceso directo a aplicaciones.

Al planificar qué solución de acceso remoto es la más adecuada para nuestra empresa, se deben considerar cuidadosamente 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.

A continuación detallamos dichos métodos y sus principales medidas de seguridad.

4.1. VPN

Una red privada virtual, también conocida por sus siglas VPN *(Virtual Private Network)*, es una tecnología de red que permite una extensión segura de una red local (LAN[8]) sobre una red pública o no controlada como Internet.

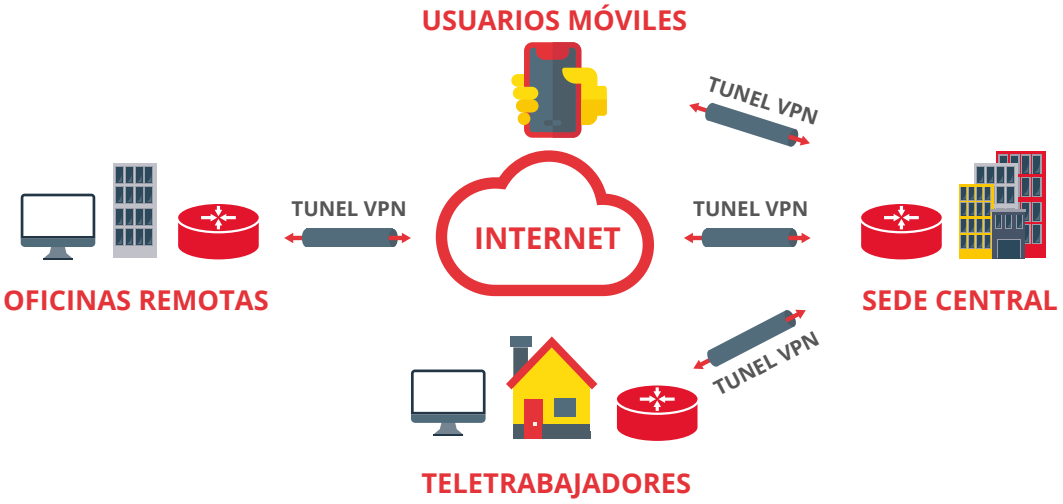


Ilustración 1 Estructura de una VPN para una empresa

8 Una red de área local o LAN (por las siglas en inglés de *Local Area Network*) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

4

"Al establecer una VPN, la **integridad** de los datos y la **confidencialidad** se protegen mediante la autenticidad del cliente, es decir, sólo se permite el acceso a los usuarios autorizados y el cifrado, dificultando que un tercero pueda robar información confidencial."

Las conexiones establecidas utilizando VPN protegen la información que se intercambia, ya que establecen un «túnel» o canal cifrado de comunicación entre nuestro dispositivo y nuestro lugar de trabajo por donde «viajan» nuestros datos confidenciales de manera segura. El *software* VPN cifra la información enviada por los dispositivos, lo que significa que no se puede interceptar el tráfico que se está transmitiendo a través de Internet.

Este sistema funciona aplicando una clave de cifrado a los datos para transformarlos de forma que resulten indescifrables. La información sólo puede ser descifrada por un sistema que también tenga la clave utilizada para cifrar los datos (clave secreta previamente compartida), lo que significa que las redes VPN son bastante difíciles de descifrar. La mayoría de los sistemas VPN en la actualidad ofrecen cifrado AES-256 **[REF - 8]**.

Al establecer una VPN, la **integridad** de los datos y la **confidencialidad** se protegen mediante la autenticidad del cliente, es decir, sólo se permite el acceso a los usuarios autorizados y el cifrado, dificultando que un tercero pueda robar información confidencial. Además de proteger la confidencialidad y la integridad las VPN proporcionan:

- **Autenticación mutua:** proceso por el cual dos partes de una comunicación se identifican y autentican una a la otra simultáneamente, garantizando la legitimidad de los participantes en la comunicación.
- **Protección frente a reenvíos:** asegurando que los datos solo se entregan una vez, evitando la posibilidad de que sean interceptados por un ciberdelincuente o que este inserte paquetes maliciosos en la comunicación.
- **La protección frente al análisis de tráfico:** impidiendo que se pueda extraer información a través del análisis de la comunicación (los datos que se transmiten entre los dos extremos, la cantidad de datos transmitidos, etc.)

Como bien sabemos, nada garantiza la seguridad al cien por cien. Si bien el uso de estas redes reduce el riesgo significativamente, existen factores que afectan a su seguridad como una implementación poco robusta, vulnerabilidades en el *software*, que la clave de acceso se vea comprometida, etc. Por estos motivos, siempre se debe estar al día de las posibles amenazas **[REF - 9]** y salvaguardar la **información**.

4

4.2. Arquitecturas VPN

En términos simples, una VPN crea un "túnel de comunicación" que une cliente y servidor para mantener una comunicación segura y privada entre ellos. Posibilita la ampliación de la red de la empresa haciendo que los recursos informáticos de una ubicación estén disponibles para los empleados de otras ubicaciones.

Se debe valorar las necesidades de seguridad y recursos de tu empresa para decidir si la implementación puede llevarse a cabo por el personal técnico, o por el contrario deber contratarse como un servicio externo **[REF - 11]**. En los siguientes puntos explicaremos los escenarios de VPN más comunes y sus principales características técnicas.

"En términos simples, una VPN crea un **"túnel de comunicación"** que une cliente y servidor para mantener una comunicación segura y privada entre ellos. "

4.2.1. VPN de sitio a sitio

También conocida como VPN *Site-To-Tite* (por su denominación en inglés). Esta implementación se utiliza principalmente para comunicar un sitio con uno o más sitios remotos (por ejemplo, la sede principal de la empresa y una sede secundaria) a través de una red pública como Internet, estableciendo una conexión segura.

En este escenario, los dispositivos cliente (terminales) no necesitan ningún *software* VPN, ni precisan ningún tipo de configuración adaptada para el uso de la misma. Requiere de dos dispositivos servidores VPN, uno en cada sitio que se quiera conectar.

Existen dos tipos de implementaciones VPN de sitio a sitio:

- **Basada en intranet:** si una empresa tiene una o más ubicaciones remotas a las que desea unirse en una sola red privada puede crear una VPN de intranet para conectar cada LAN separada a una sola WAN[9].

- **Basada en extranet:** cuando una compañía tiene una relación cercana con otra compañía (como un socio, proveedor o cliente), puede construir una extranet VPN que conecte las LAN de esas compañías. Esta extranet VPN permite a las empresas trabajar juntas en un entorno de red seguro y compartido, a la vez que impide el acceso a sus intranets independientes.

9 Una red de área amplia, o WAN (*Wide Area Network* en inglés), es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.

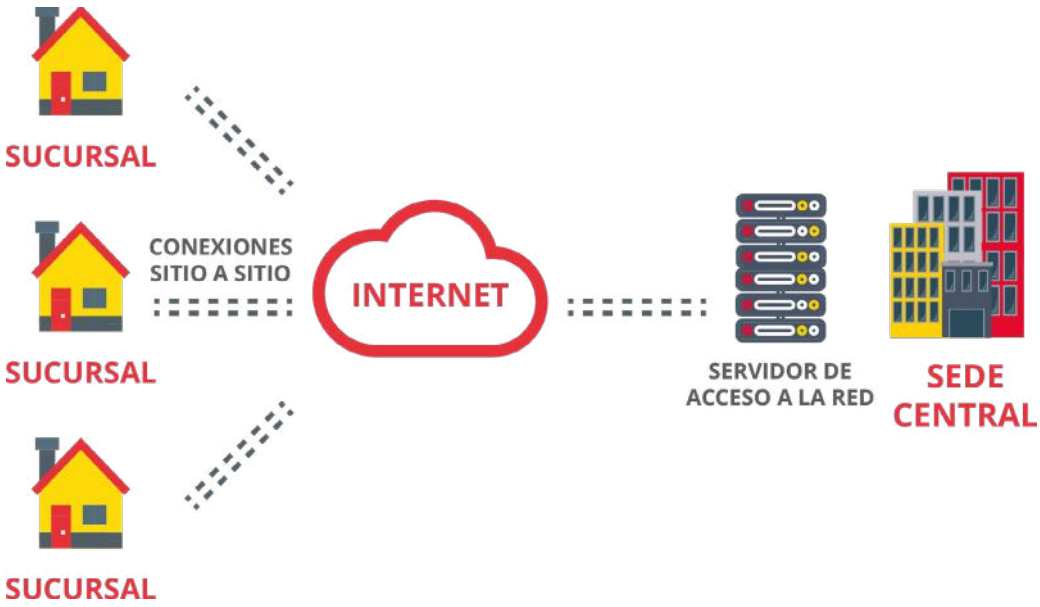


Ilustración 2: VPN de sitio a sitio basada en Intranet

4.2.2. VPN de acceso remoto

Se utiliza principalmente para salvaguardar las comunicaciones entre el dispositivo del teletrabajador y la red interna de la empresa. Se puede utilizar este tipo de VPN para hacer que una red de oficina esté disponible de forma remota para los usuarios autorizados, como por ejemplo los empleados que trabajan desde casa o en el transcurso de un viaje, y por tanto necesitan acceder de forma remota a las aplicaciones y a la información corporativas utilizando Internet como vínculo de acceso.

Esta configuración requiere de dos dispositivos:

- Un dispositivo *hardware* instalado en la red de la organización, denominado concentrador de VPN o VPN *Gateway*, que conecta la red de la organización con los clientes VPN de forma segura.

- Un dispositivo *software* o cliente VPN en el lado del usuario que conecta de forma segura a los dispositivos cliente, como por ejemplo ordenadores o *smartphones* de empleados que trabajan en remoto, con las redes de la organización.

Estas dos arquitecturas pueden funcionar bajo distintos protocolos VPN. Para ampliar información consulta este enlace **[REF - 12]**.

4

Ilustración 3: VPN de acceso remoto

4.3 Cómo saber si una VPN es confiable

Una vez analizadas las necesidades de nuestra organización y antes de tomar la decisión final sobre la VPN que vamos a implantar, debemos leer atentamente las condiciones de contratación y la política de privacidad. Estas son algunas recomendaciones:

- Antes de confiar en una VPN **debemos informarnos**, consultar quién la ofrece, las **condiciones del servicio**, su funcionamiento, su rendimiento, etc.

- Revisaremos también la **compatibilidad** con el sistema operativo utilizado en la organización y con los navegadores además de verificar su **escalabilidad** es decir, cuántas conexiones permite.

- Si se trata de una aplicación para el móvil, **habrá que revisar los permisos** que solicita para su instalación, su nivel de aceptación y buscar información sobre su desarrollador. No se deben instalar aplicaciones que soliciten accesos excesivos a tus datos o a datos que nada tengan que ver con el servicio.

- Seleccionaremos una VPN que **cifre todo el tráfico y que cifre extremo a extremo**. Hay VPN que cifran sólo hasta su servidor o que sólo cifran determinado tipo de tráfico **[REF - 11]**.

- Lee con detenimiento la **política de privacidad** sobre todo si comparten información con terceros. Escogeremos preferentemente para usos profesionales VPN no gratuitas y sin publicidad. Las aplicaciones gratuitas suelen requerir permisos para compartir los datos de la organización con terceros con el objeto de enviar anuncios.

- Comprobaremos que tenemos personal formado para su **auditoría y mantenimiento** o que nuestro proveedor TI **[REF - 10]** ofrece estos servicios.

4

4.4 Infraestructura de escritorio virtual o VDI

Una infraestructura de escritorio virtual, o VDI por sus siglas en ingles *Virtual Desktop Infrastructure*, es una tecnología que consiste en virtualizar **[REF - 13]** los entornos de trabajo de los empleados y alojarlos en una ubicación controlada por la empresa. Este tipo de solución encaja tanto para situaciones de teletrabajo en las que gran parte de la plantilla está fuera de la oficina, como también cuando habitualmente hay trabajadores con una elevada movilidad, como comerciales, flotas de reparto, soporte in situ, etc.

Para el empleado es muy similar a trabajar desde su puesto en la oficina ya que puede disponer del mismo sistema operativo y aplicaciones con las que ya trabajaba pero desde cualquier dispositivo: ordenadores portátiles, *smartphones* o *tablets*, **accediendo** a su entorno de trabajo personal generalmente a través de un navegador web.

"Una infraestructura de escritorio virtual, o VDI por sus siglas en ingles Virtual Desktop Infrastructure, es una tecnología que consiste en **virtualizar los entornos de trabajo** de los empleados y alojarlos en una ubicación controlada por la empresa."

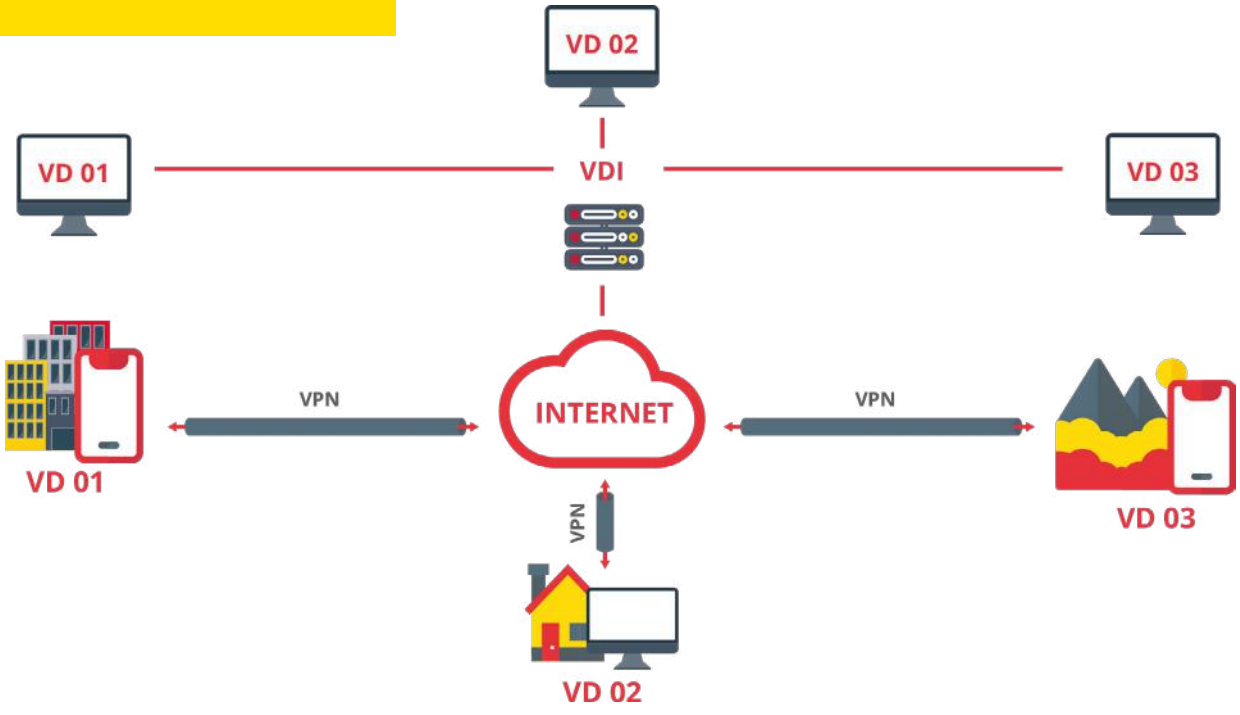


Ilustración 4: Infraestructura de escritorio virtual o VDI

4

"**Los entornos de trabajo de los empleados son gestionados por la empresa** mediante la solución VDI elegida , pudiendo estar alojada en un servidor propio o en los servidores de una empresa contratada según las necesidades de la organización."

4.4.1. VDI propio o como servicio «DaaS»

Los entornos de trabajo de los empleados son gestionados por la empresa mediante la solución VDI elegida, pudiendo estar alojada en un servidor propio o en los servidores de una empresa contratada según las necesidades de la organización.

- **Instalar VDI en un servidor propio:** su principal ventaja es el control sobre la administración del sistema evitando depender de terceros **[REF - 14]** a los que trasladar nuestros requisitos de seguridad. No obstante, hay que contar con personal técnico que realice la implementación, así como considerar el tiempo de despliegue y el gasto económico que conlleva la adquisición de *hardware*.

- **VDI como servicio o DaaS *(Desktop as a Service)*:** consiste en contratar a una empresa externa todo lo relacionado con la puesta en marcha y mantenimiento del sistema VDI. Los escritorios virtuales de los empleados pueden seguir siendo gestionados internamente y así aplicar las mismas medidas y políticas de seguridad que si el VDI estuviera ubicado en un servidor propio. El principal inconveniente de este modelo es que la privacidad de la información gestionada puede verse comprometida. Para evitarlo, además de leer detenidamente la política de privacidad y seguridad del servicio contratado, tendremos que detallar nuestros requisitos de seguridad y privacidad y firmar un acuerdo de nivel de servicio.

4.5. Ventajas de utilizar un sistema VDI

Ya sea propio de la empresa o contratado como servicio, presenta varias ventajas frente a otros sistemas de teletrabajo.

4.5.1. Movilidad

Los sistemas VDI son adecuados para entornos con elevada movilidad, como es el caso de comerciales, técnicos, altos cargos, etc. Estos trabajadores dispondrán de un entorno de trabajo igual al que tendrían en un dispositivo corporativo desde cualquier ubicación con acceso a Internet.

Además, disponer de un sistema VDI en la empresa puede permitir a los empleados realizar teletrabajo desde sus casas sin comprometer la seguridad de la empresa y la información que gestiona.

4

"**Ventajas de utilizar un sistema VDI** Ya sea propio de la empresa o contratado como servicio, presenta varias ventajas frente a otros sistemas de teletrabajo."

4.5.2. Entorno seguro

Los sistemas VDI son entornos de trabajo seguros, ya que los escritorios de los empleados son controlados por la empresa. Cualquier política de seguridad que se aplique a los dispositivos físicos de la organización **[REF - 15]** puede trasladarse a los escritorios virtuales de los empleados.

La información que se gestiona en los escritorios virtuales está bajo las mismas medidas de seguridad que si se trabajara en dispositivos físicos. En todo momento la información está alojada en servidores controlados por la empresa y no es almacenada en el dispositivo utilizado para teletrabajar.

4.5.3. Ahorro de costes

Los sistemas VDI requieren de una menor inversión económica en el *hardware* utilizado comparado con otros sistemas de teletrabajo. Esto se debe a que todas las herramientas necesarias son ejecutadas en el servidor, por lo que la carga de trabajo de los dispositivos es pequeña. Además permitiría a la empresa implementar una política de BYOD, *Bring Your Own Device* **[REF - 16]**, con el consecuente ahorro en terminales.

Por otro lado, el despliegue de escritorios virtuales también es un proceso relativamente sencillo que requiere poco tiempo, lo que se traduce en un menor gasto de tiempo para el personal técnico de la organización.

4.5.4 . Escalabilidad

Los sistemas VDI se caracterizan por ofrecer una elevada escalabilidad, adaptándose a las circunstancias cambiantes de la empresa con más flexibilidad que otras opciones. Si se requiere aumentar el número de puestos de trabajo, el administrador puede crear nuevos escritorios virtuales, y cuando este volumen de trabajo descienda, podrá eliminarlos también de forma sencilla. Además, también puede asignar más recursos a un empleado si puntualmente los necesita.

4

"Ya que las tecnologías móviles están cada vez más presentes en el entorno empresarial, **la infraestructura móvil virtual (VMI)** es una muy buena opción a considerar a la hora de mejorar la seguridad en nuestra organización."

4.5.5. Consideraciones de seguridad en el uso de VDI

Medidas de seguridad relativas al control de acceso y a las comunicaciones:

- Cuando se habilita en la empresa un sistema VDI, el control de acceso por parte de los usuarios debe ser lo más robusto posible, para evitar accesos no autorizados al sistema. Para ello el acceso debería contar con doble factor de autenticación **[REF - 17],** como puede ser el uso de dispositivos o aplicaciones que generan una contraseña de un solo uso u OTP (del inglés *One Time Password*). De esta manera se reduce el riesgo de que un tercero sin autorización acceda al sistema.

- La utilización de redes privadas virtuales o VPN es la solución ideal para proteger las comunicaciones entre el dispositivo del empleado y el escritorio virtual evitando posibles fugas de información.

4.6. VMI

Ya que las tecnologías móviles están cada vez más presentes en el entorno empresarial, la infraestructura móvil virtual (VMI) es una muy buena opción a considerar a la hora de mejorar la seguridad en nuestra organización.

Aunque el acceso al servidor de terminales y las tecnologías VDI están destinadas principalmente a los equipos de teletrabajo, existe una tecnología emergente que proporciona capacidades similares para los dispositivos móviles: la infraestructura móvil virtual (VMI). Así como una solución VDI proporciona un escritorio virtual seguro a un ordenador de teletrabajo, también VMI facilita un entorno de dispositivo móvil virtual seguro a un dispositivo móvil de teletrabajo. Una infraestructura móvil virtual permite acceder a aplicaciones móviles remotas desde un dispositivo móvil. Como las aplicaciones se ejecutan en servidores corporativos, no es posible perder sus datos o que los roben, incluso si se pierde el dispositivo o es sustraído.

Resulta muy útil para separar entornos de trabajo y personales en un mismo dispositivo. Es además muy práctico si un empleado deja su puesto de trabajo ya que la empresa sólo tiene que bloquearle el acceso al sistema remoto y toda la información corporativa deja de ser accesible para ese usuario.

4

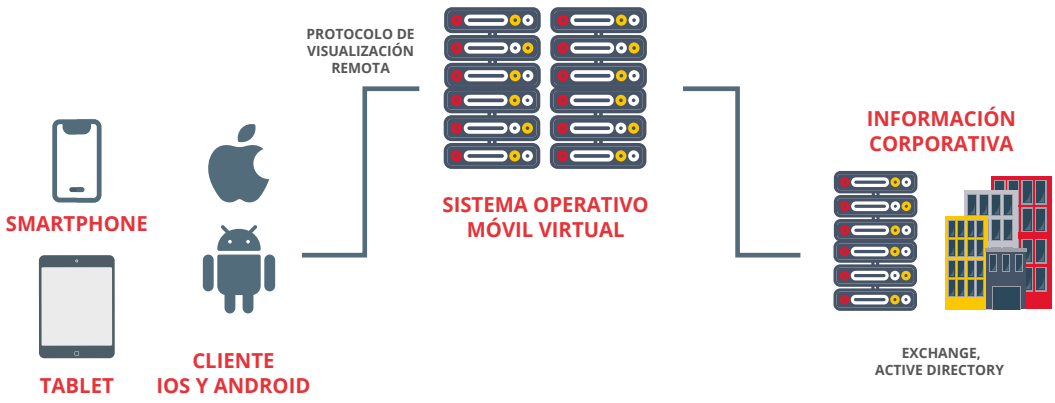


Ilustración 5: infraestructura VMI

4.7. Aplicaciones de escritorio remoto

Las aplicaciones de acceso de escritorio remoto **[REF - 19]** proporcionan al teletrabajador la posibilidad de controlar remotamente un equipo, siendo habitual conectarse al equipo del que se es usuario en la oficina de la organización, desde un dispositivo cliente de teletrabajo.

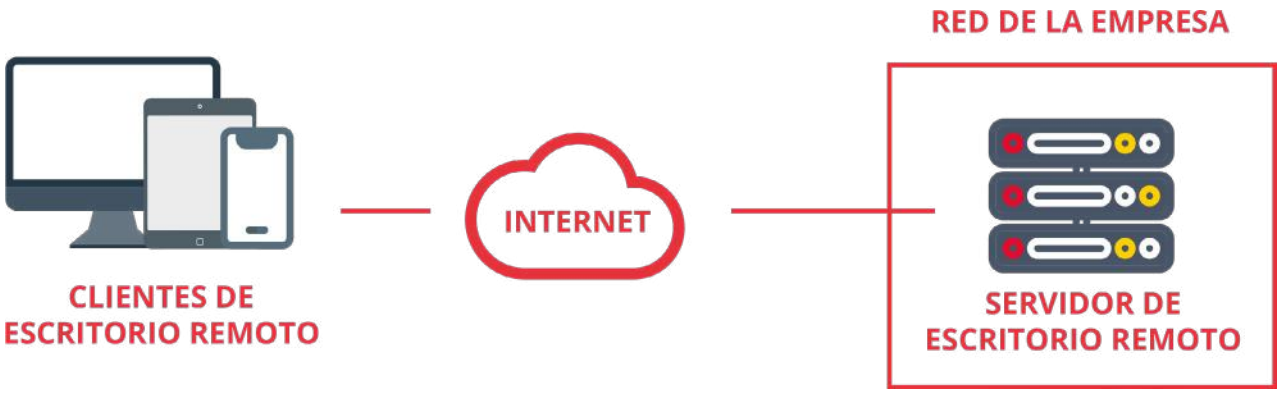


Ilustración 6: Modelo de acceso remoto

En este modelo de conexión, el teletrabajador tiene control de teclado y ratón sobre el ordenador remoto y ve la pantalla de ese equipo en la pantalla del dispositivo con el que está trabajando. Uno de los escritorios remotos más conocido es RDP, ya que se encuentra integrado en el sistema operativo Windows, aunque existen otras muchas opciones **[REF - 10]** . El acceso remoto al escritorio permite al usuario acceder a todas las aplicaciones, datos y otros recursos como si utilizara su ordenador en la oficina. El funcionamiento se basa en que un programa cliente de acceso de escritorio remoto o *plug-in* de navegador web está instalado en cada dispositivo cliente de teletrabajo, y se conecta directamente con la correspondiente estación de trabajo interna del empleado en la red interna de la organización.

4

"Las aplicaciones de **acceso de escritorio remoto** proporcionan al teletrabajador la posibilidad de controlar remotamente un equipo, siendo habitual conectarse al equipo del que se es usuario en la oficina de la organización, desde un dispositivo cliente de teletrabajo."

A simple vista puede parecer un buen método para conectarnos remotamente, ya que la instalación de estas aplicaciones es muy sencilla y no requiere de altos conocimientos técnicos para su implantación. La parte negativa es que estas herramientas pueden crear puertas traseras *(backdoors)* **[REF - 3]** a través de las cuales podría comprometerse el servicio o las credenciales de acceso de usuario y por lo tanto permitir el acceso a los equipos corporativos. Además, al usar este tipo de aplicaciones podemos estar aceptando ciertos términos y condiciones de uso que podrían otorgar algún tipo de privilegio a las mismas sobre nuestros equipos e información como por ejemplo la cesión de los datos recabados con fines comerciales. Recuerda leer siempre con atención «la letra pequeña» en concreto, los términos y condiciones y la política de privacidad, antes de implementar una solución de escritorio remoto.

Otro problema grave de seguridad con el *software* de escritorio remoto es que está descentralizado; es decir, en lugar de que la organización tenga que proteger un único servidor de puerta de enlace VPN, es necesario proteger cada estación de trabajo interna a la que se puede acceder a través del acceso de escritorio remoto. Debido a que se puede acceder a estas estaciones de trabajo internas desde Internet, por lo general necesitan estar protegidas con el mismo rigor que los servidores de acceso remoto. Elevar la seguridad a un nivel aceptable requeriría una cantidad significativa de tiempo y recursos, así como la implementación de controles de seguridad adicionales.
Si a pesar de no ser la opción más recomendada, optas por utilizar aplicaciones de escritorio remoto en tu organización, será necesario aplicar las siguientes recomendaciones de seguridad:

- Revisar que todo el *software* esté actualizado a la última versión y comprobar[10] que los equipos no están afectados por vulnerabilidades, como por ejemplo la Vulnerabilidad en el escritorio remoto de Windows de versiones antiguas.

10 Puedes estar al día de todas las novedades de seguridad para mantener tus sistemas seguros en la sección de Protege tu empresa: Avisos de seguridad

4

- No utilizar el puerto por defecto[11] (3389).
- Cambiar el usuario por defecto, nunca usar uno del tipo «admin», «administrador», etc.
- Utilizar siempre contraseñas robustas **[REF - 20]**.
- Implantar políticas de bloqueo de cuenta o *lock-out,* las cuales bloquean el acceso al servicio tras un número pre-establecido de intentos de autenticación fallidos.
- Aplicar el doble factor de autenticación siempre que sea posible **[REF - 17]**.
- Utilizar listas de control de acceso mediante NLA (por sus siglas en inglés *Network Level Authentication*). Mediante esta tecnología, los usuarios deben autenticarse en la red de la empresa antes de poder hacerlo en el servidor de escritorio remoto.
- Así mismo, es recomendable crear reglas específicas en el cortafuegos **[REF - 18]** de la empresa que restrinjan el acceso al servidor de escritorio remoto a un conjunto de máquinas controlado.

"Para evitar esta situación y ofrecer un extra de seguridad y privacidad a las comunicaciones, lo más recomendable es **utilizar a la vez una VPN y el escritorio remoto.** "

En general, habilitar el acceso al escritorio desde Internet no es recomendable, puesto que, en caso de existir una vulnerabilidad o configuración inadecuada, los ciberdelincuentes lo tendrán más fácil para entrar en la red corporativa. Para evitar esta situación y ofrecer un extra de seguridad y privacidad a las comunicaciones, lo más recomendable es **utilizar a la vez una VPN y el escritorio remoto**. Cuando un empleado desee acceder a su cuenta por medio del escritorio remoto, primero deberá acceder a la VPN, la cual proporcionará el acceso al escritorio remoto, así se contará con dos sistemas distintos que harán el sistema más robusto.

11 Comúnmente, la conexión al servicio de escritorio remoto de Windows se hace por medio del puerto 3389. Si se cambia por otro distinto, se dificultará los ataques automatizados que llevan a cabo los ciberdelincuentes. Esto se conoce como seguridad por oscuridad.

4

4.8. Soluciones en la nube

Las soluciones en la nube ofrecen gran versatilidad y un modelo diferente a la hora de compartir y almacenar información cuando teletrabajamos. Por este motivo, además de las implementaciones explicadas anteriormente contemplamos las distintas opciones a la hora de utilizar las soluciones en la nube para llevar a cabo las funciones diarias fuera de la oficina.

4.8.1. Portales para aplicaciones

Otra de las opciones para implementar soluciones de acceso remoto en la organización son los portales para aplicaciones. Un portal es un servidor[12] que proporciona el acceso a una o más aplicaciones corporativas a través de una interfaz única centralizada. La mayoría de estos portales están basados en web, por lo que el teletrabajador solo necesita utilizar un navegador como cliente para acceder a las aplicaciones de la empresa y poder realizar las funciones relativas a su trabajo. Cada empleado tendrá un perfil configurado en el que se le dará acceso solo a aquellas aplicaciones necesarias para desempeñar su trabajo.

"Otra de las opciones para implementar soluciones de acceso remoto en la organización son los **portales para aplicaciones**. Un portal es un servidor que proporciona el acceso a una o más aplicaciones corporativas a través de una interfaz única centralizada. "

En términos de seguridad, los portales protegen la información que se intercambia entre los dispositivos cliente y el portal, proporcionando control de acceso y autenticación entre otros servicios de seguridad.

Los portales y las VPN comparten características de seguridad y se diferencian en la ubicación del *software* cliente de la aplicación y de los datos asociados. En la VPN, el *software* y los datos están en el dispositivo cliente y en un portal se encuentran en el servidor del portal, aunque estos se pueden configurar para permitir la descarga de contenido del portal y almacenarlo en el dispositivo cliente o en otros dispositivos fuera del entorno seguro.

12 Si el portal de aplicaciones está alojado en un servidor de la empresa este ya no sería considerado un servicio en la nube, si bien el concepto y la utilidad del portal de aplicaciones es el mismo.

4

"Las **tecnologías colaborativas** nos mantienen en contacto con nuestro equipo de trabajo cuando desempeñamos nuestras tareas fuera de la organización"

En este caso debemos focalizar la seguridad en cada dispositivo que acceda al portal, ya que se trata de la puerta de entrada a la información de la organización. Es necesario recordar que las aplicaciones en la nube son aquellas provistas por un proveedor gratuitamente o a modo de suscripción, dejando en sus manos la disponibilidad, seguridad y soporte de las mismas así como la información que contienen **[REF - 21]**.

4.8.2. Herramientas colaborativas

Las tecnologías colaborativas **[REF - 22]** nos mantienen en contacto con nuestro equipo de trabajo cuando desempeñamos nuestras tareas fuera de la organización: paquetes ofimáticos, videoconferencias, pizarras virtuales, intercambio de documentos y ficheros, chats, etc.

Al utilizar estas herramientas debemos ser capaces de proporcionar la seguridad necesaria a la información que se intercambia y por ello establecer una serie de pautas básicas de seguridad, como las que exponemos a continuación.

- **Establecer comunicaciones solo con usuarios conocidos:** aunque parezca obvio, no se debe otorgar acceso a la red o establecer una comunicación con usuarios que no se encuentren dentro de nuestra lista de contactos. A la hora de poner en marcha un sistema de multiconferencia o videoconferencia, las medidas de seguridad deben girar en torno al control de accesos y a la protección de la información. Este tipo de medidas, que deben ser conocidas y acatadas por todos los empleados, son las mismas que se

otorgarán a cualquier solicitud externa. Cabría la posibilidad de invitar a alguien cuyo sistema estuviera comprometido, lo que permitiría la propagación e infección a las distintas redes conectadas a través de este sistema de conferencia. En definitiva, deberemos usar el sentido común y únicamente permitir el acceso a aquellas solicitudes que sean de confianza y que únicamente accedan a la información que sea estrictamente necesaria para llevar a cabo el trabajo.

- **Prevenir la pérdida de datos y gestionar el almacenamiento:** una de las grandes ventajas de celebrar reuniones online o utilizar tecnologías de intercambio de información, es la capacidad de exponer en común y plantear nuevas ideas, sacar conclusiones o llegar a acuerdos. Será fundamental que la información surgida durante la reunión no se pierda cuando esta finalice. En la mayoría de las soluciones de videoconferencia y pantalla compartida, se ofrece algún tipo de capacidad de grabación de audio, visual o de texto. Estas grabaciones se almacenan en la nube, lo que aumenta el riesgo de pérdida de confidencialidad. Por lo tanto, cifrar este tipo datos será fundamental para preservar su integridad y confidencialidad.

- **Mantener la disponibilidad de la red:** las tecnologías colaborativas dependen de la conexión a Internet. Esta conexión deberá ser constante y confiable. Una pérdida de conexión hará que el intercambio de información no se pueda llevar a la práctica. Para evitar este tipo de problemas, debemos asegurarnos de que la conexión de red cuente con el suficiente ancho de banda para asegurar su funcionamiento óptimo. Además, también deberán funcionar otro tipo de herramientas, como los antivirus o los cortafuegos, ya que serán nuestra principal defensa ante ataques de código malicioso, denegación de servicio entre otras amenazas.

- **Integración con el resto de tecnologías:** este tipo de herramientas deberá integrarse con el resto de tecnologías TI de la organización, evitando problemas derivados de la incompatibilidad de sistemas o con las medidas de seguridad. La aparición de los servicios en la nube ha simplificado mucho este proceso eliminando gran parte de la molestia que podría ocasionar la administración de *hardware*.

4

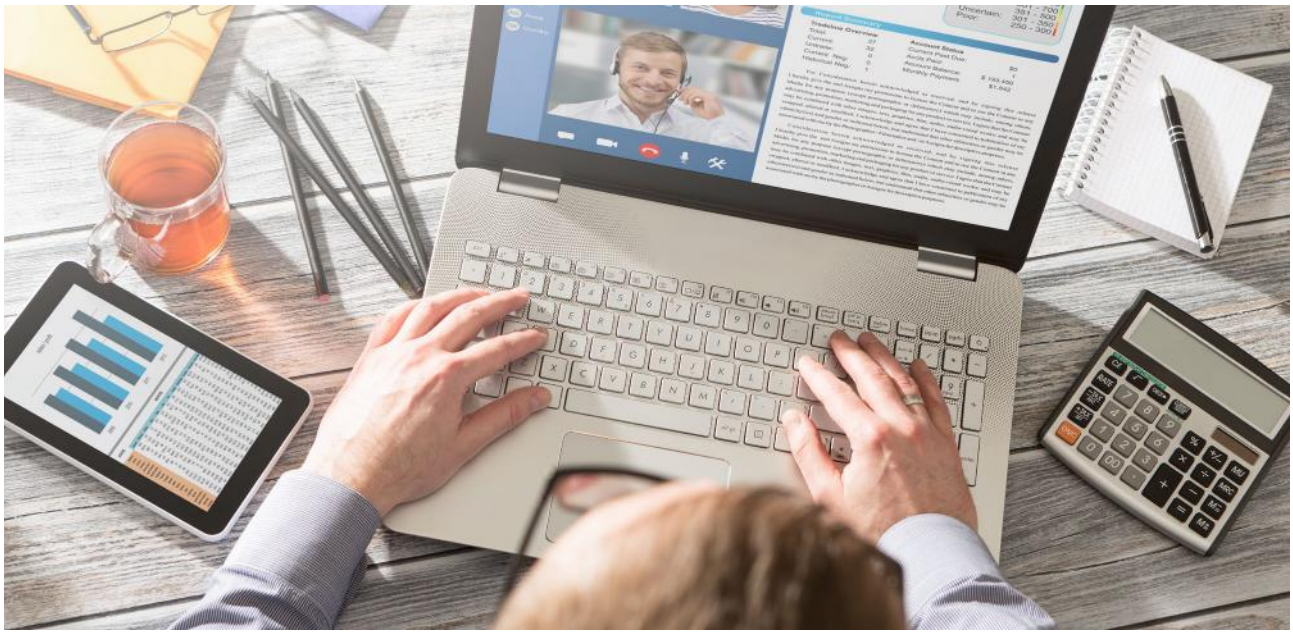
4.8.3. Recomendaciones de seguridad en el uso de aplicaciones de videollamada

Las aplicaciones de videollamada son herramientas fundamentales para mantener el contacto directo del equipo de trabajo. Puesto que existe una amplia variedad de estas aplicaciones nos centraremos en las pautas generales de seguridad a la hora de utilizar estas herramientas.

- **Utilizar un plan empresarial en lugar de uno básico:** si utilizamos planes básicos o gratuitos de las herramientas colaborativas, no podremos aplicar todas las opciones para mejorar la seguridad de la aplicación ya que estarán limitadas. Por ello, siempre es recomendable decantarse por un plan empresarial verificando que cuenta con las medidas necesarias para hacer un uso seguro.

- **Activar la sala de espera y bloquear la reunión:** esta funcionalidad añade a los participantes de una conferencia en un entorno previo a la reunión, así el administrador de la sala puede comprobar si los asistentes son solo los permitidos. Desde esta sala de espera, verificando la identidad de cada participante invitado, les dará paso a la reunión o se la denegará si no está autorizado. Una vez que todos se hayan incorporado a la llamada, se bloqueará el acceso a nuevos participantes.

"Las aplicaciones de **videollamada son herramientas fundamentales** para mantener el contacto directo del equipo de trabajo. "



4

- **Requerir contraseña para acceder a la reunión:** muchas aplicaciones de videollamada cuentan con esta configuración habilitada por defecto. Verifícalo para forzar su uso en caso de que esté deshabilitada. Utiliza siempre una contraseña robusta **[REF - 20]** para evitar accesos de terceros no autorizados.

- **Poner atención al enviar la convocatoria:** es necesario compartir el enlace para que los participantes se puedan unir a la videollamada. Para ello, es recomendable utilizar las funciones de compartición de las propias aplicaciones y evitar el uso de redes sociales o canales de comunicación inseguros para lanzar la convocatoria.

- **Video y micrófono apagados por defecto:** algunas funciones por defecto, como la cámara o el micrófono activados, pueden dar lugar a situaciones poco deseables. Además, los participantes que se unan a una videollamada tampoco deben compartir su escritorio de forma predeterminada ya que esto podría provocar fugas de información. El administrador será quien permita que los usuarios muestren su escritorio cuando sea preciso.

  La recepción de video permanecerá deshabilitada por defecto y solo se utilizará cuando sea necesario. De esta forma se evitan posibles fugas de información y se reduce el consumo de ancho de banda. El micrófono también permanecerá apagado cuando no sea necesario su uso.

  Así mismo, conviene recordar que cuando compartimos nuestra pantalla con el resto de usuarios de la reunión se debe evitar compartir información confidencial, como: nombres de usuario o nombre de dispositivo, documentos confidenciales, nombres de archivos o directorios sensibles y direcciones web del navegador.

  Si el administrador pretende grabar la reunión, se lo comunicará previamente a todos los participantes.

4

- ***Software* oficial y actualizado:** las herramientas deben descargarse siempre desde la web oficial del desarrollador o desde repositorios oficiales. Nunca se descargará de enlaces obtenidos en medios como el correo electrónico, aplicaciones de mensajería instantánea o redes sociales, ya que puede dirigir a sitios web fraudulentos.

  Estas herramientas siempre estarán actualizadas a la última versión disponible y si fuera posible se marcará la opción de actualizaciones automáticas o que la aplicación avise al usuario en caso de existir una nueva actualización.

- **Conocer la política de privacidad de la herramienta:** antes de decantarse por una herramienta de videoconferencia, se debe conocer la política de privacidad que sigue el proveedor, para saber qué tratamiento realiza sobre la información confidencial. Algunas herramientas pueden seguir políticas cuya protección para los clientes no es tan robusta como la que requiere el cumplimiento del RGPD **[REF - 23]**, por lo que siempre hay que saber cómo actúan sobre los datos tratados.

- **Cifrado de las comunicaciones:** esta será una de las medidas de seguridad imprescindibles con las que debe contar la aplicación para asegurar que las comunicaciones no puedan ser espiadas por un tercero. Generalmente todas las principales aplicaciones cuentan con mecanismos de cifrado pero es conveniente comprobarlo antes de utilizarla.

5 SEGURIDAD DEL SERVIDOR DE ACCESO REMOTO

Habitualmente, cuando teletrabajamos necesitamos acceder a los recursos corporativos para desempeñar nuestro trabajo diario sin ningún tipo de restricción. Son los servidores de acceso remoto los que permiten que los dispositivos externos puedan acceder a los recursos internos, así como proporcionar un entorno de teletrabajo seguro y aislado. Un servidor comprometido podría permitir el acceso no autorizado a los recursos de la empresa y a los dispositivos cliente de teletrabajo para obtener información confidencial. Al implantar medidas de seguridad en estos servidores protegemos la información corporativa y por ende la continuidad de negocio.

Los servidores de acceso remoto deben mantenerse actualizados, utilizar una configuración de seguridad definida por la organización y deben ser gestionados únicamente por administradores autorizados. Se debe evaluar cuidadosamente la seguridad de cualquier solución que se ejecute en el servidor de acceso remoto ya que una vulnerabilidad en cualquiera de estas aplicaciones puede comprometer todo el servidor de acceso remoto, con los peligros que eso conlleva. Sin duda, la mejor práctica para garantizar la seguridad es tener el servidor de acceso remoto dedicado solo para este servicio.

5.1. Dónde colocar el servidor de acceso remoto

Los servidores de acceso remoto suelen estar situados en el perímetro de la red de la organización. Esta colocación es la más común porque las políticas de seguridad de la empresa se suelen aplicar a toda la red corporativa. Incluso si una política de seguridad particular se aplica a una subred de la organización, la mayoría de los servidores de acceso remoto pueden restringir el acceso a las subredes y, por lo tanto, pueden colocarse en el perímetro de la organización.

Ilustración 7: Servidor de acceso remoto en la red corporativa

5

5.2. Autenticación, autorización y control de acceso remoto

Los recursos informáticos accesibles mediante conexión remota solo deberían estar disponibles para los usuarios que realmente los usan y necesitan y no de forma generalizada. Para asegurar que el acceso está restringido adecuadamente, los servidores de acceso remoto deben verificar a cada teletrabajador antes de conceder cualquier acceso a los recursos e información de la organización así como utilizar tecnologías de autorización para asegurar que sólo se puedan utilizar los recursos necesarios que han de ser aprobados previamente para cada usuario. Además, tener contraseñas para los distintos servicios, reduce el impacto en otros recursos en caso de que alguna de estas contraseñas se viera comprometida.

> "Los recursos informáticos accesibles mediante conexión remota solo deberían estar disponibles para los **usuarios que realmente los usan y necesitan** y no de forma generalizada. "

Siempre que sea posible, la organización debe implementar la autenticación mutua, que permita a los usuarios remotos verificar la legitimidad del servidor antes de introducir sus credenciales, por ejemplo utilizando un certificado digital presentado por el servidor y así garantice su legitimidad. Algunos métodos de acceso remoto **[REF - 11]**, incluyen la autenticación obligatoria del servidor durante la configuración del canal de comunicaciones seguras.

Después de verificar la identidad de un usuario remoto se pueden realizar comprobaciones en el dispositivo cliente de teletrabajo para determinar a qué recursos internos debe permitirse el acceso a los usuarios. Estos controles se suelen denominan **controles de salud, idoneidad, detección o evaluación.** En estos controles, el servidor de acceso remoto comprueba en el dispositivo cliente distintos aspectos como: que cumpla la configuración de seguridad de la organización, que el antivirus este actualizado, que el sistema operativo esté correctamente parcheado, etc. También se pueden emitir certificados digitales a los dispositivos cliente para que se autentiquen como parte de estas comprobaciones.

6 SEGURIDAD DEL *SOFTWARE* CLIENTE DE ACCESO REMOTO

Otro aspecto importante a la hora de garantizar la seguridad de nuestras conexiones remotas es la configuración del *software* de acceso remoto. Muchos de estos clientes tienen características y configuraciones de seguridad que pueden ser configuradas remotamente por un administrador de sistemas, por lo que se recomienda que esta tarea sea realizada por el personal técnico y no por el usuario del *software* cliente. Si no se protegen adecuadamente, un posible atacante podría utilizar las capacidades de gestión remota para obtener acceso a los recursos internos de la organización. Además, para asegurar que la gestión remota está debidamente protegida se deben cifrar las comunicaciones de red y realizar la autenticación mutua de los puntos finales.

Las organizaciones deben planificar cómo se gestionarán los dispositivos cliente de teletrabajo que proporcionan a los teletrabajadores, como por ejemplo personal del servicio de asistencia técnica que acceda de forma remota a un dispositivo para realizar la resolución de los problemas que se reporten.

7 PRINCIPALES AMENAZAS PARA LOS TERMINALES DE TELETRABAJO

Permitir a los teletrabajadores acceder de forma remota a los recursos de la organización ofrece a los ciberdelincuentes oportunidades adicionales para vulnerar la seguridad de la empresa. Si los dispositivos no están correctamente protegidos supone un riesgo adicional no sólo para la información a la que accede el teletrabajador, sino también para los demás sistemas y redes de la organización.

Actualmente existen muchas amenazas que afectan a la seguridad de los dispositivos cliente de teletrabajo. Estas amenazas materializadas por ciberdelincuentes tienen diferentes motivaciones, incluyendo causar daño material y reputacional a la organización, robar propiedad intelectual, cometer robo de identidad y otras formas de fraude.

La principal amenaza contra la mayoría de los dispositivos cliente de teletrabajo es el *malware*, incluyendo virus, gusanos, troyanos, *rootkits*, *spyware* y *bots* **[REF - 3]**. Las amenazas de *malware* pueden infectar los dispositivos cliente a través de muchos medios, como el correo electrónico, los sitios web, las descargas y el uso compartido de archivos, la mensajería instantánea y las redes sociales. El uso de medios o dispositivos extraíbles no autorizados, como las memorias *flash*, es otro mecanismo muy común de transmisión del *malware*. Además de las anteriores, otra amenaza a destacar contra los dispositivos cliente de teletrabajo es la pérdida o el robo del dispositivo, ya que alguien con acceso físico a un dispositivo tiene muchas opciones para intentar ver o copiar la información almacenada en él. Un atacante con acceso físico también podría infectar con ***malware*** el dispositivo y así conseguir que le proporcione acceso a los datos a los que se accede o se introducen en dicho dispositivo, como por ejemplo las contraseñas de los usuarios que se escriben en el teclado de un ordenador portátil (*keylogger*).

Generalmente, los terminales de teletrabajo deben tener los mismos controles de seguridad que los que están físicamente en la empresa: aplicar las actualizaciones de seguridad, servicios innecesarios desactivados, etc. Sin embargo, debido a las amenazas a las que se enfrentan los dispositivos cliente en entornos externos, se recomiendan controles de seguridad adicionales, pudiendo ser necesario ajustar algunos controles de seguridad para que funcionen eficazmente en entornos de teletrabajo. En el siguiente apartado se exponen las recomendaciones para asegurar los terminales de teletrabajo y los datos que contienen.

7

Si el uso de controles de seguridad adicionales instalados en los dispositivos de teletrabajo no es factible o aplicable, se pueden estudiar otras medidas como proporcionar un entorno seguro para el teletrabajo a través del uso de tecnologías VDI o VMI, es decir, proporcionar a los teletrabajadores dispositivos previamente configurados para que puedan arrancar su equipo de teletrabajo en un entorno seguro, o adoptar soluciones de gestión de dispositivos móviles (*Mobile Device Management,* MDM) y de gestión de aplicaciones móviles (*Mobile Application Management,* MAM) para la mejora y aplicación de la seguridad en los dispositivos móviles.

Las organizaciones deberían ser responsables de asegurar sus propios dispositivos cliente de teletrabajo y también deberían exigir a sus usuarios que mantengan niveles de seguridad apropiados. Es importante que los empleados conozcan cómo se protege su puesto de trabajo **[REF - 24]**.

"La principal amenaza contra la mayoría de los dispositivos cliente de teletrabajo es el ***malware***, incluyendo virus, gusanos, troyanos, *rootkits*, *spyware* y *bots* **"**

8 ASEGURAR LOS EQUIPOS DE TRABAJO

Una de las consideraciones más importantes para los equipos de teletrabajo es la aplicación de actualizaciones de seguridad de sistemas operativos y aplicaciones. Por lo general todas las aplicaciones tienen que estar actualizadas, siendo las más críticas las que se utilizan por motivos de seguridad (por ejemplo, *software* anti*malware*, cortafuegos) o las de acceso remoto, y las que son objetivos frecuentes de ataques como navegadores web, clientes de correo electrónico y clientes de mensajería instantánea. Para los equipos de teletrabajo administrados por sus usuarios (dispositivos personales **[REF - 25]**), la mejor opción será activar las actualizaciones automáticas.

Las organizaciones deben contar con una política de actualizaciones de los equipos de teletrabajo **[REF - 26]**. Las organizaciones también deberían animar a los usuarios a actualizar completamente sus equipos de teletrabajo antes de llevarlos de viaje o a otros entornos no controlados y por tanto menos seguros.

Otras medidas de seguridad que son particularmente importantes para el teletrabajo incluyen las siguientes:

- Tener cuentas de usuarios separadas con privilegios limitados y adecuados para cada perfil de usuario que vaya a usar el equipo de teletrabajo. Esto reduce la probabilidad de que un ciberdelicuente obtenga un acceso con privilegios al equipo.

- Configurar el bloqueo de sesión que impida el acceso al equipo después de haber estado inactivo durante un período de tiempo (por ejemplo, 5 minutos). Esto impediría que un delincuente con acceso físico al equipo pudiera acceder fácilmente a la sesión actual en un descuido del usuario. Sin embargo, esta medida no frustra a un atacante que roba un PC o tiene acceso a él durante un período de tiempo prolongado; ya que el bloqueo de sesión se puede eludir mediante diversas técnicas.

- Proteger físicamente los equipos de teletrabajo mediante el uso de cerraduras de cable u otros elementos disuasorios contra el robo. Esto es lo más importante para los equipos de teletrabajo en entornos externos no confiables.

8

“Una de las consideraciones más importantes para los equipos de teletrabajo es la aplicación de actualizaciones de seguridad de sistemas operativos y aplicaciones.”

- Existen soluciones que proporcionan un sistema operativo de inicio en un medio extraíble de sólo lectura con *software* cliente de acceso remoto preconfigurado. En la mayoría de los casos, estas soluciones pueden configurarse para evitar que los usuarios almacenen archivos en el disco duro local, guarden los archivos en medios extraíbles y transfieran información desde el sistema operativo conocido a otra ubicación. Las soluciones de sistemas operativos de arranque hacen que la seguridad lógica del PC de teletrabajo sea mucho menos importante, aunque no son la solución a todos los problemas de seguridad (por ejemplo, podría existir alguna vulnerabilidad en el sistema operativo del medio extraíble).

- Cifra tus soportes **[REF - 29]** de información para proteger los datos de tu empresa de posibles accesos malintencionados y garantizar así su confidencialidad e integridad.

9 ASEGURAR LOS DISPOSITIVOS MÓVILES DE TELETRABAJO

Los dispositivos móviles, incluidos los que se usan simultáneamente de manera personal y profesional (BYOD), deben estar contemplados en las políticas de seguridad de la empresa, ya que existen riesgos inherentes a su uso como el robo o pérdida, infección por *malware*, accesos no autorizados a recursos de la empresa o fugas de información. Si no existen estas políticas o no contemplan los usos permitidos de los móviles, estaremos expuestos a sufrir incidentes de seguridad.

Para la elaboración de estas políticas podemos utilizar las soluciones de gestión de dispositivos móviles (MDM) y las soluciones de gestión de aplicaciones móviles (MAM) diseñadas para controlar el uso de dispositivos móviles.

Podemos utilizar las soluciones MDM para aplicar las políticas de seguridad que consideremos necesarias. Por ejemplo, podríamos utilizar este *software* para requerir el uso de un PIN para desbloquear un dispositivo móvil, permitir que las tecnologías de cifrado protejan los datos confidenciales almacenados, así como determinar si un dispositivo móvil ha sufrido modificaciones de *software* para evadir las restricciones del fabricante (comúnmente conocido como *rootear* en el caso de los móviles Android o *jailbreak* en el caso de los iPhone).

El *software* de gestión de dispositivos móviles también se puede utilizar para realizar un borrado remoto cuando un dispositivo móvil se ha perdido o ha sido robado y así evitar el acceso no autorizado a cualquier dato confidencial que contenga. Una organización puede establecer diferentes políticas de gestión de dispositivos móviles para cada categoría, como por ejemplo, los emitidos por la organización, controlados por terceros y BYOD, y así tener en cuenta todos los diferentes niveles de acceso. Además proporciona un entorno que aísla las aplicaciones y los datos de la empresa del resto del dispositivo pudiéndose requerir una autenticación robusta para acceder al entorno empresarial, que a su vez está cifrado para proteger los datos y aplicaciones confidenciales de la organización, y para minimizar la fuga de datos de esas aplicaciones a otras aplicaciones y servicios que se ejecutan en el dispositivo.

En el caso de que el dispositivo se pierda o el empleado abandone la organiza-

9

"Los dispositivos móviles, incluidos los que se usan simultáneamente de manera personal y profesional (BYOD), deben estar contemplados en las **políticas de seguridad de la empresa**."

ción, el entorno protegido puede borrarse de forma remota para eliminar los datos de la empresa.

La opción más completa para mantener la seguridad de estos dispositivos es el *software* conocido como UEM, **[REF - 27]** por sus siglas en inglés *Unified Endpoint Management*, que permite administrar de forma centralizada todos los dispositivos de la empresa de manera remota. Esta herramienta aúna las características de la gestión de dispositivos móviles o MDM anteriormente descritos y la gestión de movilidad empresarial EMM *(Enterprise Mobility Management)*, simplificando así el coste en tiempo y recursos en las labores de administración. Los UEM, además de permitir a la empresa gestionar los dispositivos móviles, proporcionan las herramientas necesarias para administrar otros elementos corporativos como impresoras, dispositivos IoT **[REF - 28]** o equipos de sobremesa.

Las organizaciones pueden aprovechar estas capacidades de gestión de la seguridad, por ejemplo, restringiendo la instalación y el uso de aplicaciones de terceros, o proporcionando una serie de aplicaciones autorizadas. No obstante, las capacidades de seguridad y las acciones apropiadas varían ampliamente según el tipo de dispositivo, las aplicaciones que necesite tener instaladas y los permisos solicitados por estas. Por ello, las organizaciones deben proporcionar a los administradores de dispositivos y a los usuarios las pautas necesarias para protegerlos, ya que ambos, administradores y usuarios, son responsables de la seguridad de los dispositivos móviles de teletrabajo **[REF - 30]**.

Entre los consejos de seguridad generales para dispositivos móviles destacamos:

- Limitar las capacidades de red, como por ejemplo el uso del Bluetooth y redes inalámbricas compartidas, priorizando en estos casos el uso de la redes móviles (3G/4G/5G). Existe la posibilidad de que algunos protocolos inalámbricos expongan al dispositivo a un posible ataque por parte de los ciberdelincuentes.

- Los dispositivos que se conectan a Internet deben disponer de *software antimalware* e incluso de cortafuegos habi-

9

litados para evitar ataques y accesos no autorizados.

- Aplicar las actualizaciones y parches del fabricante cuando sea necesario para proteger el dispositivo de los ataques que explotan vulnerabilidades conocidas y no parcheadas.
- Cifrar los datos almacenados en el dispositivo.
- Requerir autenticación antes de acceder a los recursos de la organización.
- Restringir las aplicaciones que pueden o no instalarse mediante listas blancas o negras.
- Dada la similitud entre las funciones de los dispositivos móviles, especialmente a medida que aumentan sus capacidades y las de los equipos de sobremesa o portátiles, las organizaciones deberían considerar aumentar las medidas de seguridad hasta equipararlas con las de los equipos que se utilizan en las instalaciones de la empresa.

10 PROTECCIÓN DE DATOS EN TERMINALES DE TELETRABAJO

El teletrabajo suele implicar la creación y modificación de información en función de la actividad diaria como por ejemplo el manejo del correo electrónico, documentos de texto y hojas de cálculo, etc. Debido a que esos documentos pueden contener datos sensibles de la organización, deben ser tratados con la seguridad que requieren. Las dos medidas principales que se pueden tomar para proteger los datos en los dispositivos de teletrabajo son asegurarlos en el propio dispositivo de teletrabajo y realizar copias de seguridad periódicas en una ubicación controlada por la empresa. Adicionalmente, se podría contemplar la opción de no permitir que la información se almacene en dispositivos de teletrabajo, sino almacenarla de forma centralizada en la organización.

Información sensible, como por ejemplo registros de personal, registros médicos o registros financieros, que se almacenan o se envían a o desde dispositivos de teletrabajo, debe ser protegida para que no sea accesible ni modificable. Los teletrabajadores a menudo olvidan que almacenar información sensible en un dispositivo externo, o imprimir esta información en una impresora pública, también puede poner en peligro su confidencialidad. Una divulgación no autorizada de información sensible podría además de tener consecuencias legales **[REF -23]**, dañar la imagen de la organización y por consiguiente la confianza de los clientes hacia la misma.

En cualquier caso, las organizaciones deben proporcionar las medidas de seguridad a aplicar a los usuarios responsables de los dispositivos móviles de teletrabajo sobre cómo deben protegerlos. Consulta estas dos políticas de seguridad para ampliar la información:

- Política de uso de dispositivos móviles corporativos **[REF - 30]**.
- Políticas de uso de dispositivos móviles no corporativos **[REF - 25]**.

11 COPIA DE SEGURIDAD DE DATOS EN DISPOSITIVOS DE TELETRABAJO

La mayoría de las organizaciones poseen políticas para realizar copias de seguridad de los datos de forma regular. Esta política de copias de seguridad debe contemplar también los datos de los equipos de teletrabajo y de los dispositivos móviles asignados a esta tarea. Sin embargo, una política de este tipo puede necesitar disposiciones diferentes para las copias de seguridad realizadas en las instalaciones de la organización en comparación con las ubicaciones externas.

Si los datos de los que se va a realizar la copia de seguridad contienen información confidencial o necesitan que se proteja su confidencialidad por otras razones, existen consideraciones de seguridad adicionales si la copia de seguridad se realiza en una ubicación externa.

En el caso de que los datos estén siendo respaldados remotamente desde el dispositivo de teletrabajo hasta un sistema de la organización, las comunicaciones que transportan esos datos deben ser cifradas y así garantizar su integridad. Si se están haciendo copias de seguridad de los datos localmente (por ejemplo, en medios extraíbles, discos duros externos o unidades *flash*), la copia de seguridad debe estar protegida con la misma rigurosidad que los datos originales, es decir, si los datos originales están cifrados, entonces los datos de la copia de seguridad también deberían estar cifrados.

Consulta nuestra guía «Copias de seguridad: una guía de aproximación para el empresario» **[REF - 31]** para conocer todas las medidas referentes a las copias de seguridad en el entorno empresarial.

12 RESUMEN

Después de leer esta guía seguro que tienes más claro por qué es necesario tener en cuenta las medidas de seguridad a la hora de teletrabajar. A modo de resumen, consulta este apartado siempre que necesites recordar los pasos más importantes a la hora de trabajar fuera de la organización.

- **Red privada virtual o VPN:** conéctate a través de una VPN para evitar que los ciberdelincuentes puedan espiar tus comunicaciones.
- **VPN + escritorio remoto:** evita riesgos derivados de las vulnerabilidades o configuraciones inadecuadas. Si utilizas el escritorio remoto, que sea a través de VPN.
- **Dispositivos corporativos la mejor opción:** cuentan con las políticas de seguridad que la empresa estima oportunas y tienen instalado el *software* necesario para realizar el trabajo.
- **Dispositivos personales:** siempre bajo una política BYOD.
- **Crea un entorno de trabajo seguro:** tanto en tu casa como en tu oficina respeta la política de protección del puesto de trabajo.
- **Protege tu conexión a Internet:** se utilizará preferiblemente la red doméstica, y se evitará utilizar redes wifi públicas. **[REF - 32]**
- **Red de datos móvil como plan B:** Cuando no sea posible utilizar la red doméstica para teletrabajar o cualquier otra red considerada segura como alternativa, utiliza la red de datos móvil 4G o 5G.
- **Periodo de implantación y pruebas:** valora diferentes escenarios y configuraciones antes de comenzar a teletrabajar.
- **Elabora una política de teletrabajo:** y forma a tus empleados para que puedan seguirla.

13 REFERENCIAS

[REF - 1]. **Incibe, Políticas de seguridad para la pyme – Almacenamiento en los equipos de trabajo** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-en-los-equipos-trabajo.pdf

[REF - 2]. I**ncibe, Políticas de seguridad para la pyme – Almacenamiento en la red corporativa** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-red-corporativa.pdf

[REF - 3]. **Incibe, Glosario de términos de ciberseguridad: una guía de aproximación para el empresario** https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

[REF - 4]. **Incibe, Cómo prevenir incidentes en los que intervienen dispositivos móviles** https://www.incibe.es/protege-tu-empresa/blog/prevenir-incidentes-los-intervienen-dispositivos-moviles

[REF - 5]. **Incibe, kit de concienciación** https://www.incibe.es/protege-tu-empresa/kit-concienciacion

[REF - 6]. **Incibe, Leyes en ciberseguridad que afectan a tu empresa** https://www.incibe.es/protege-tu-empresa/blog/leyes-ciberseguridad-afectan-tu-empresa

[REF - 7]. **Incibe, Protección de la información** https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

[REF - 8]. **Incibe, Políticas de seguridad para la pyme** – Uso de técnicas criptográficas https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf

[REF - 9]. **Incibe, Avisos de seguridad** https://www.incibe.es/protege-tu-empresa/avisos-seguridad

[REF - 10]. **Incibe, Catálogo de empresas y soluciones de Ciberseguridad** https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad

[REF - 11]. **vpnMentor - Diferentes tipos de VPN y cuándo usarlas** https://es.vpnmentor.com/blog/diferentes-tipos-de-vpn-y-cuando-usarlas/

[REF - 12]. **vpnMentor - ¿Qué protocolo VPN debería utilizar?** https://es.vpnmentor.com/blog/que-protocolo-vpn-deberia-utilizar/

[REF - 13]. **Incibe, Sistemas VDI y teletrabajo, la dupla perfecta en tiempos del COVID-19** https://www.incibe.es/protege-tu-empresa/blog/sistemas-vdi-y-teletrabajo-dupla-perfecta-tiempos-del-covid-19

[REF - 14]. **Incibe, Contratación de servicios** https://www.incibe.es/protege-tu-empresa/que-te-interesa/contratacion-servicios

[REF - 15]. **Incibe, Políticas de seguridad para la pyme** https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[REF - 16]. **Incibe, Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario** https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

[REF - 17]. **Incibe, Dos mejor que uno: doble factor para acceder a servicios críticos** https://www.incibe.es/protege-tu-empresa/blog/dos-mejor-uno-doble-factor-acceder-servicios-criticos

[REF - 18]. **Incibe, Firewall tradicional, UTM o NGFW. Diferencias, similitudes y cuál elegir según tus necesidades** https://www.incibe.es/protege-tu-empresa/blog/firewall-tradicional-utm-o-ngfw-diferencias-similitudes-y-cual-elegir-segun

[REF - 19]. **Incibe, ¿Es seguro tu escritorio remoto?** https://www.incibe.es/protege-tu-empresa/blog/seguro-tu-escritorio-remoto

[REF - 20]. **Incibe, Desempolvando Políticas de seguridad: las contraseñas** https://www.incibe.es/protege-tu-empresa/blog/desempolvando-politicas-seguridad-las-contrasenas

[REF - 21]. **Incibe, Protege tu información, aplica estas recomendaciones de seguridad en servicios de almacenamiento cloud** https://www.incibe.es/protege-tu-empresa/blog/protege-tu-informacion-aplica-estas-recomendaciones-seguridad-servicios

[REF - 22]. **Incibe, Herramientas colaborativas: medidas básicas de seguridad** https://www.incibe.es/protege-tu-empresa/blog/herramientas-colaborativas-medidas-basicas-seguridad

[REF - 23]. **Incibe, Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario** https://www.incibe.es/protege-tu-empresa/guias/ganar-competitividad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario

[REF - 24]. **Incibe, Políticas de seguridad para la pyme – Protección del puesto de trabajo** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/proteccion-puesto-trabajo.pdf

[REF - 25]. **Incibe, Políticas de seguridad para la pyme – Uso de dispositivos móviles no corporativos** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-dispositivos-moviles-no-corporativos.pdf

[REF - 26]. **Incibe, Políticas de seguridad para la pyme – Actualizaciones de *software*** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/actualizaciones-*software*.pdf

[REF - 27]. **Incibe, Cómo prevenir incidentes en los que intervienen dispositivos móviles** https://www.incibe.es/protege-tu-empresa/blog/prevenir-incidentes-los-intervienen-dispositivos-moviles

[REF - 28]. **Incibe, Seguridad en la instalación y uso de dispositivos IoT: una guía de aproximación para el empresario** https://www.incibe.es/protege-tu-empresa/guias/seguridad-instalacion-y-uso-dispositivos-iot-guia-aproximacion-el

[REF - 29]. I**ncibe, Uso de técnicas criptográficas** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf

[REF - 30]. I**ncibe, Políticas de seguridad para la pyme – Uso de dispositivos móviles corporativos** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-dispositivos-moviles-corporativos.pdf

[REF - 31]. **Incibe, Copias de seguridad: una guía de aproximación para el empresario** https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

[REF - 32]. **Incibe, Seguridad en redes wifi: una guía de aproximación para el empresario** Seguridad en redes wifi: una guía de aproximación para el empresario

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa