Guía de seguridad en el teletrabajo

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

GENERALITAT VALENCIANA

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

Sobre CSIRT-CV

CSIRT-CV es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007, como una apuesta de la **Generalitat Valenciana** por la seguridad en la red. Fue una iniciativa pionera al ser el primer centro de estas características que se creó en España para un ámbito autonómico.

Está formado por un equipo multidisciplinar de personal técnico especializado en los distintos ámbitos de la seguridad y dedicado a desarrollar medidas preventivas y reactivas para mitigar los incidentes de seguridad en sistemas de información dentro del ámbito de la Comunidad Valenciana, que abarca tanto la Administración Pública, como PYMES y ciudadanos.

CSIRT-CV ha certificado su Sistema de Gestión de Seguridad de la Información con AENOR según la norma UNE-ISO/IEC 27001:2014 cuyo alcance son los sistemas de información que dan soporte a los servicios prestados a la Generalitat Valenciana para la prevención, detección y respuesta antes incidentes de seguridad en las TICs.

Datos de contacto

CSIRT-CV Centro de Seguridad TIC de la Comunitat Valenciana

http://www.csirtcv.gva.es/

https://www.facebook.com/csirtcv

https://twitter.com/csirtcv

Licencia de uso

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

1 Acerca de esta guía

Esta guía surge como respuesta a los riesgos derivados del teletrabajo, los cuales muchas veces no son tenidos en suficiente consideración.

Si bien aplica a cualquier tipo de teletrabajo, se centra especialmente en la creciente tendencia a trabajar esporádicamente desde casa con equipos propios o a la necesidad durante periodos vacacionales de conectar con el entorno laboral, ya sea para llevar el seguimiento de tareas o proyectos, como para solventar temas urgentes cuando por la distancia no es posible trasladarse físicamente al lugar habitual de trabajo.

Aunque no es el objetivo directo de esta guía, se hará también especial hincapié en los riesgos derivados de la utilización de dispositivos personales en el entorno corporativo (también conocido como Bring Your Own Device - BYOD), así como a usuarios que conecten de continuo desde casa o remotamente desde otras ubicaciones (como puede ser la oficina del cliente).

2 Marco organizativo

Antes de entrar en temas técnicos, configuraciones, o salvaguardas para la información, ante un escenario de teletrabajo se debe **establecer un marco normativo** interno con el fin de procedimentar y estandarizar el modo y las condiciones bajo las cuales la dirección desea que se desarrolle el teletrabajo.

Dependiendo del tamaño y naturaleza de la organización puede ser necesario definir normativas y pautas que abarquen los siguientes puntos:

- Tipos de usuarios que dispondrán de modalidad de teletrabajo y los permisos de acceso remoto de que dispondrán.
- Procedimientos para la solicitud y autorización del teletrabajo.
- Procedimiento de conexión remota de emergencia para solventar problemas e incidencias puntuales.
- Posible utilización de equipos personales para el teletrabajo así como las medidas de seguridad aplicables a los mismos.
- Criterios para la conexión de equipos no confiables al entorno corporativo, ya sea remota o localmente.
- Medidas de seguridad extraordinarias aplicables a los dispositivos utilizados para el teletrabajo.
- Normativas referentes al almacenamiento de información de negocio fuera de las instalaciones, ya sea en equipos de la organización, equipos personales de empleados o dispositivos extraíbles.
- Cualquier otra que se considere necesaria por la organización.

Aunque el listado de recomendaciones anterior no es exhaustivo, todas las que figuran se consideran especialmente críticas. Téngase en cuenta que cualquier forma de teletrabajo debería estar **aprobada formalmente** por la dirección y se debería llevar un control de qué usuarios utilizan esta modalidad. Esta recomendación permite, entre otras ventajas, llevar un control del equipamiento que el usuario utiliza y saca de las instalaciones, permite la localización del usuario en caso de incidentes, facilita la justificación de ausencia de la oficina en caso de accidentes personales durante la jornada laboral, pero lo más importante es que permite implantar y aplicar a quien corresponda las diferentes medidas técnicas y organizativas dependiendo del perfil del usuario, la información que maneja, y los riesgos a los que está expuesto.

A la hora de aplicar controles y salvaguardas a los activos que participan del teletrabajo, habrá que definir dos niveles de requisitos: los **requisitos genéricos** que aplican a toda la organización y otros concretos y muy **específicos para el teletrabajo**:

- Los **controles generales** son aquellos que toda la organización debe cumplir independientemente del tipo de trabajo, y que sin un correcto seguimiento pueden quedar sin implantar ya sea por utilizar equipos propios del usuario, por el desconocimiento del usuario o por las diferencias tecnológicas en los entornos de trabajo. Algunos ejemplos pueden ser la periodicidad de las copias de seguridad, actualizaciones automáticas de software, ejecución y actualización periódica del antivirus, tiempos de bloqueo de equipos por inactividad, control de acceso de usuarios, o similares, los cuales no siempre están correctamente configurados o tenidos en cuenta en una instalación personal o domestica.

- Los **controles adicionales** aplicables al teletrabajo abarcan aquellos de los que no siempre se dispone de forma genérica ya sea en el lugar de teletrabajo o en el entorno organizativo. Hablamos de capas extra de cifrado de información, clausulas de responsabilidad adicionales, cumplimiento de procedimientos específicos, contraseña en BIOS, software para asistencia remota y localizar el equipo en caso de pérdida o robo, inventario de información del dispositivo, procedimientos de emergencia para revocar los permisos del usuario (también en caso de pérdida), o herramientas de borrado remoto de dispositivos.

La correcta aplicación de estos dos tipos de controles debería ser suficiente para garantizar unos niveles aceptables de seguridad, pero pueden tener el problema de limitar demasiado el uso del equipo fuera del entorno laboral, por lo que si el equipo también es utilizado para fines personales es posible que se acaben deshabilitando salvaguardas o se degrade la seguridad del sistema. Es por ello que si la conexión a los sistemas va a ir más allá de interactuar con interfaces web en aplicaciones poco críticas o enviar información por correo electrónico, debería establecerse un nivel adicional de seguridad introduciendo el concepto de **equipo o conexión confiable**, el cual se explicará en el siguiente apartado.

3 Equipo y sistema operativo

Puede parecer evidente que cualquier equipo que vaya a conectase a los entornos corporativos, ya sea propiedad de la organización, proveedor o del empleado, debe cumplir con unos mínimos de seguridad como puede ser tener el sistema operativo actualizado o contar con un antivirus robusto, pero por desgracia esto son buenas prácticas para cumplir mínimos lo cual no implica que se pueda considerar ese equipo como confiable.

Partiendo de que con las amenazas actuales es prácticamente imposible poder considerar un equipo 100% seguro, se puede establecer una línea base a partir de la cual se confiará en el dispositivo: **consideramos como un equipo confiable** aquel que ha sido plataformado y securizado por personal cualificado (implica antivirus, actualizaciones automáticas, bastionado, etc.…), instalando el sistema operativo desde una fuente confiable (soportes originales, fuentes de los que se ha comprobado el hash, o similar), y sobre el cual el usuario no dispone de permisos de administración. Aun así es posible comprometer el equipo, pero para una organización estándar este nivel de seguridad se considera más que aceptable.

Cada organización deberá decidir si esta definición de equipo confiable le es suficiente o si por el contrario es demasiado estricta para el tipo de información que se va a manipular, pero independientemente de donde se sitúe el umbral, éste debe existir de forma clara para poder discernir si dar acceso a un equipo a la infraestructura corporativa o no.

Si por los requisitos del negocio no resultase necesario establecer una política tan estricta en cuanto a la confiabilidad de un equipo, a continuación se incluye una propuesta priorizada de medidas de seguridad a aplicar:

- Instalación del sistema operativo desde una fuente fiable.
- Sistema operativo y aplicaciones actualizadas.
- Software antivirus.
- Cuentas de usuario sin permisos para instalar software.
- Control de acceso robusto.
- Configuraciones seguras en aplicaciones (navegación web, correo electrónico, etc).
- Bloqueo automático por inactividad.
- Software antirootkits.
- Control de software original.
- Cifrado del disco.
- Comprobación periódica de la adecuación de las salvaguardas.

3.1 Equipos no confiables

Si la información a tratar en los equipos de teletrabajo es considerada importante o crítica, pero no se considera el equipo lo suficientemente confiable en los términos mencionados en el apartado anterior, es posible aplicar medidas compensatorias mediante las cuales se pueden conseguir niveles aceptables de seguridad según los requisitos de cada organización:

- **Diferentes cuentas de usuario:** se trata simplemente de tener diferentes cuentas de usuario en el mismo equipo donde se utilizará una para entornos confiables (teletrabajo) y otra para

asuntos personales. Si bien la protección que ofrece esta configuración es fácilmente vulnerable para la mayoría de virus y código malicioso, puede ser una primera línea de defensa poco intrusiva que permite establecer medidas de seguridad diferentes a diferentes perfiles de usuario. Facilitaría pues poner diferentes requisitos para el bloqueo automático del equipo, haría independiente los historiales de navegación y contraseñas guardadas en el equipo, o permitiría clasificar mejor los documentos personales de los profesionales permitiendo incluso cifrar la carpeta de cada usuario.

- **Arranque dual:** resulta una solución mucho más robusta que la anterior. Se trata de instalar en un mismo equipo dos sistemas operativos, iguales o diferentes, de los cuales cada uno se utilizará para un entorno (teletrabajo o personal). Si bien seguiría siendo posible acceder a los datos de las otras particiones, la información puede almacenarse cifrada para evitar que pueda ser modificada desde la otra partición. En la mayoría de casos, esta configuración ayudará también a evitar que un virus descargado en una de las particiones infecte la otra ya que aunque no es técnicamente imposible, es poco frecuente: esta amenaza se ve prácticamente eliminada en caso de que se trate de sistemas operativos diferentes, por ejemplo uno GNU/Linux y otro Microsoft Windows.

- **Distribuciones "live":** antiguamente se las conocía como live-cd aunque ya hace tiempo que es posible instalarlas en memorias USB o en tarjetas de memoria estilo SD. Se trata de instalaciones completas de sistemas operativos que son totalmente independientes de lo que haya en el PC ya que se cargan antes de que el sistema operativo del equipo arranque. Con esta opción se utilizaría, el sistema operativo del PC para temas personales y la distribución live para el teletrabajo, ya que desde la distribución live se puede acceder a la partición instalada en el equipo, pero no al revés. Esta solución tiene como principal desventaja una **disminución del rendimiento** general, aunque con los equipos actuales y según el tipo de tareas a realizar puede no ser un inconveniente. Por otro lado las **ventajas que aporta son enormes**: es extremadamente sencillo de plataformar a gran escala, se pueden diseñar distribuciones corporativas con todo lo necesario preconfigurado, ante un fallo en el sistema es muy sencillo restaurarlos, algunas de estas memorias se pueden proteger contra escritura evitando la instalación de código malicioso, y pueden utilizarse en cualquier PC.

3.2 Protección física de los equipos

Por motivos de movilidad y para poder trabajar indistintamente desde casa o desde la oficina, el modelo de teletrabajo actual utiliza en la mayoría de los casos ordenadores portátiles, tablets, o cualquier otro dispositivo portable cuyas ventajas son de sobra conocidas. No obstante, precisamente por el hecho de ser portables, fáciles de perder, y susceptibles de **ser robados**, deben tomarse medidas especialmente diseñadas para este tipo de dispositivo.

3.2.1 Protecciones anti-robo

Para evitar los robos de equipos portátiles suele ser suficiente tomar algunas medidas de sentido común como **no dejarlo en el coche (aunque no esté a la vista), no dejarlo desatendido, evitar sacarlo de casa si no es necesario, etc.**

Además pueden adquirirse **candados de seguridad** para portátiles, los cuales sirven para anclar el dispositivo a algún elemento del mobiliario, aunque bien es cierto que no son extremadamente robustos y según su calidad pueden romperse con herramientas simples. Su utilidad está más enfocada a proteger el equipo del robo fácil por descuido que no de una intrusión en casa o en la oficina. Como alternativa a los candados que van en la ranura de seguridad del equipo (relativamente poco seguras), existen otros que llevan un arnés enganchado a una placa metálica que se pega en la pantalla por la parte de detrás de forma que si se intenta forzar seguramente la pantalla se parta y el robo dejará de tener sentido. Estos arneses son bastante más robustos aunque estéticamente aparatosos.

Otra solución pasa por adquirir un **armario de seguridad** donde almacenar el equipo y otros artículos de relativo valor, los cuales evitarán que ante una "intrusión relámpago" en el domicilio se sustraiga el equipo de trabajo.

En el siguiente apartado se profundizará sobre la importancia de elegir adecuadamente una funda o maletín para proteger nuestros equipos de daños físicos durante el transporte, pero debemos también tener en cuenta el diseño del mismo dependiendo del tipo de desplazamiento que se hará con el dispositivo. Si por ejemplo se viaja en transporte público se debe considerar una funda con algún tipo de asas que **evite tirones**, a la vez que **no resulte obvio su contenido** evitando maletines de portátil y utilizando mochilas en su lugar.

3.2.2 Borrado remoto

Existen múltiples aplicaciones tanto para dispositivos móviles como para PC que permiten administrar remotamente los dispositivos extraviados o robados. Entre las funcionalidades típicas de estos programas se encuentran el activar el GPS del dispositivo (si lo tiene) para intentar localizarlo, o hacer un borrado completo del equipo si no va a ser posible recuperarlo. Además, algunos de estos programas cuentan con la posibilidad de, por ejemplo, acceder remotamente al equipo para recuperar datos necesarios antes de borrar el disco, monitorizar el uso que se está haciendo del equipo, o incluso activar la webcam para intentar averiguar la identidad del ladrón.

El acceso remoto a nuestro equipo generalmente se hace desde la web del proveedor de la aplicación mediante un usuario y contraseña previamente fijado, por lo que igual que sucede con aplicaciones de escritorio remoto, del estilo de LogMeIn o similar, realmente se está abriendo una puerta trasera al equipo que podría permitir a un atacante que consiguiese comprometer el servicio o las credenciales de acceso del usuario, acceder al terminal. Además el propio proveedor de la aplicación (o sus empleados) podría acceder a nuestro terminal, por lo que es recomendable valorar obtener un software que se gestione y administre desde la propia organización, antes que utilizar servicios web de terceros.

Cabe recordar que estas aplicaciones evidentemente deben instalarse antes de que el dispositivo se extravíe ya que por lo general después será demasiado tarde.

3.2.3 Daños físicos

El tipo de daños al que están expuestos los equipos portátiles en el teletrabajo son relativamente similares a los que pueden suceder en la oficina, aunque fuera de ésta todo puede magnificarse.

Para **el transporte entre oficina y el lugar de teletrabajo** es necesario disponer de una funda o maletín que ofrezca buena resistencia a caídas, golpes, aplastamiento e incluso líquidos. El formato de la misma dependerá del dispositivo, medio de transporte utilizado y número de desplazamientos a realizar. Así pues, no es lo mismo transportar un portátil de grandes dimensiones en una motocicleta, o un tablet en el coche. Como ya se ha comentado, dependiendo del lugar y medio de transporte puede resultar muy recomendable adquirir una funda impermeable sobre todo si se va a transportar a mano, en motocicleta, o cualquier otro medio que no garantice la estanqueidad del dispositivo.

Una vez en el lugar de teletrabajo deben tenerse también algunas consideraciones en cuenta ya que no siempre están tan bien adecuadas para el trabajo como la propia oficina:

- Es recomendable utilizar un **atril** para apoyar el dispositivo. Además de la ergonomía evita que se derramen líquidos sobre él al estar en alto. Además le "asigna" un espacio propio sobre la mesa evitando que quede haciendo equilibrios sobre libros, material de oficina, o que poco a poco se le empuje hasta una esquina donde finalmente caerá.
- Se debe prestar atención al **cableado**. El no estar en la oficina no significa que se puede tener todo desastrado. Un correcto cableado evitará tropiezos que acabarían con el dispositivo.

- **Guardar en lugar seguro** el dispositivo mientras no se utiliza. Aunque no es frecuente tener intrusiones en el lugar de teletrabajo, existen otros peligros con los que no contamos en la oficina: mascotas subiendo a las mesas, niños pequeños intentando alcanzar cualquier cosa de la mesa, o sobrinos en busca de algo conectado a internet para consultar una red social. Si no se está utilizando lo más recomendable es retirarlo.
- Considerar **cambiar el disco duro** por uno SSD. Los discos duros tradicionales funcionan mediante unos discos que giran a gran velocidad y sobre los que planean una serie de agujas que leen los datos las cuales nunca deben tocar los discos, por lo que cualquier vibración o caída en un momento delicado puede conllevar una pérdida total de sus datos. Esta situación se magnifica fuera de la oficina ya que allí rara vez se mueve el equipo mientras este está encendido, mientras que, por ejemplo, en el hogar puede ser más frecuente. Para evitarlo se pueden sustituir estos discos por uno de estado sólido, o SSD, los cuales al no disponer de partes móviles son mucho más resistentes a caídas y vibraciones. Además son más rápidos y reducen el consumo, aunque por otro lado de momento son más caros que los tradicionales.

3.3 Tablets y smartphones

No se debe pensar que trabajar con un dispositivo móvil se reduce únicamente a leer documentos ofimáticos en un tablet. Utilizar estos dispositivos para el entorno laboral implica también enviar y recibir correos electrónicos, atender llamadas de trabajo, almacenar información corporativa, tener acceso remoto a documentos en la nube, o incluso tener conversaciones por mensajería instantánea sobre temas laborales, por lo que son un elemento más a proteger.

Al respecto, CSIRT-cv dispone de una Guía de buenas prácticas en el uso corporativo de dispositivos móviles de recomendada lectura de la que destacan los siguientes consejos:

- Se debe limitar el acceso al dispositivo mediante un bloqueo con contraseña, patrón o similar.
- Se debe cifrar la memoria del dispositivo en caso de contener información sensible.
- Se debe disponer de medidas para poder localizar el dispositivo o hacer un borrado remoto del dispositivo en caso de pérdida o robo.
- Se debe disponer de algún mecanismo lo más automatizado posible para hacer copias de seguridad de la información del dispositivo.
- Se deben tomar medidas para prevenir y detectar malware en los dispositivos móviles.
- No se deben deshabilitar las medidas de seguridad de que disponen los dispositivos. Esto incluye, conseguir permisos de administrador, o permitir instalar software de fuentes no fiables.
- Se deben instalar siempre las últimas actualizaciones de seguridad de los programas y sistemas operativos.
- Se deben desactivar las conexiones inalámbricas que no se utilicen como el Bluetooth, Wi-Fi o NFC.

3.4 BYOD

Se conoce como BYOD (Bring Your Own Device) a la práctica de utilizar dispositivos personales como sustituto de los equipos de trabajo tradicionales, o dicho en otras palabras, **trabajar con el ordenador propio.**

Es una tendencia en auge que las empresas adoptan para reducir costes y (en teoría) aumentar la productividad, y que a la vez permiten al usuario conciliar mejor la vida laborar y personal, simplificar la administración del equipo y ofrecer más libertad y movilidad.

No obstante esta práctica conlleva importantes problemas de seguridad ya que la administración de los equipos que tradicionalmente se ha llevado desde la propia organización, queda generalmente delegada en el buen hacer del empleado, el cual no siempre tendrá los conocimientos suficientes para poder garantizar la seguridad de la información.

Es por ello que se debe realizar un análisis del riesgo antes de decidir implantar una política de BYOD en una organización y, si se considera adecuado, tomar una serie de medidas técnicas y organizativas al respecto:

- Se deben establecer políticas organizativas al respecto indicando lo que se considera un uso adecuado de los equipos y lo que no, además de un compromiso por parte del trabajador para con la seguridad de la información que se trate en el dispositivo.
- Se deben documentar los derechos y obligaciones de cada parte y detallar en qué casos el equipo podrá ser objeto de revisión por parte de la organización. Ésta parte resulta especialmente relevante ya que puede contener información personal, familiar o sensible que el empleado no desea que la organización posea, y que durante una auditoría, revisión rutinaria, cambio de configuración, o similar es posible que sea visualizada.
- Se debe disponer de un mecanismo de reemplazo de equipos en caso de pérdida o avería de los mismos para garantizar que el empleado pueda seguir desempeñando sus tareas habituales.
- Se deben establecer medidas técnicas para garantizar las mismas condiciones de seguridad que tendría la información en caso de estar almacenada en un equipo propio de la organización en lugar del empleado. Para ello se recomiendan cuentas de usuario independientes o incluso el uso de sistemas operativos o máquinas virtuales separadas, además de implantar el resto de controles habituales (borrado remoto, cifrado, copias de seguridad, control de acceso, etc.).
- Se deben establecer medidas para evitar el acceso fortuito a información corporativa por otros usuarios del equipo aparte del propio empleado: familiares o similar.

4 Comunicaciones

A continuación se van a tratar los principales aspectos a tener en cuenta a la hora de crear y configurar la estructura de comunicaciones entre los empleados en teletrabajo y la organización.

La adopción total o parcial de estos mecanismos dependerá de diversos factores que en algunos casos requerirá la incorporación de acciones más específicas según considere la organización.

Estas son las principales consideraciones a tener en cuenta a la hora de utilizar una conexión a internet para conectar con los recursos corporativos:

- No se deben utilizar conexiones poco confiables (conexiones Wi-Fi abiertas, redes públicas de hoteles, bibliotecas, locutorios, etc.) sin algún tipo de cifrado punto a punto como puede ser VPN o conexiones a sitios web protegidos con SSL (los que empiezan por HTTPS). No basta con que la red tenga contraseña para conectar ya que los propietarios de la red podrían monitorizar el tráfico, por lo que se debe aplicar una capa extra de cifrado. Esto aplica especialmente a las redes que se ofrecen gratuitamente a clientes de restaurantes y hoteles, y se vuelve extremadamente necesario en conexiones de locutorios o locales similares.
- Si es posible se recomienda utilizar módems USB con conexiones 3G, también conocidos como "pinchos 3G", los cuales son bastante más seguros que las redes inalámbricas ajenas.
- Los administradores deberán de llevar un seguimiento cercano de las conexiones remotas a los servicios corporativos de teletrabajo. Especialmente se debe prestar atención a los intentos de conexión sospechosos.
- Se deben evitar las soluciones de administración remota gestionadas por terceros como pueden ser LogMeIn o TeamViewer ya que se evaden por completo de cualquier arquitectura de seguridad implantada, además de delegar el acceso a los sistemas a terceros externos a la organización.

4.1 Tipos de teletrabajo

Del mismo modo que no todos los trabajos son iguales, las modalidades de teletrabajo se adaptan a las necesidades de cada negocio, y por lo general poco tienen que ver unas con otras.

No tendrán pues nada que ver las necesidades de alguien que desarrolle software desde casa, las de alguien que principalmente atienda el teléfono, responda a correos electrónicos, gestione proyectos, o haga visitas comerciales.

En los casos más simples, es suficiente con trabajar desde el equipo local y esporádicamente enviar documentación o resultados por correo electrónico, por lo que no será necesario un gran despliegue tecnológico. Bastará con asegurar que se dispone de un equipo protegido frente a las principales amenazas de Internet:

- Disponer de un antivirus
- Utilizar un equipo actualizado
- Utilizar contraseñas robustas
- Verificar que en el acceso a los servidores corporativos se utilicen certificados reconocidos y que el "candado" de la conexión SSL no avisa de peligros u errores.

Para prácticamente cualquier otro tipo de conexión que requiera acceso a la red interna de la organización, lo más frecuente es activar una conexión VPN, de las cuales hablaremos más adelante, y que permiten acceder a todos los servicios internos que los administradores hayan configurado.

Otra capa adicional de seguridad y usabilidad que se puede añadir es que una vez los usuarios han activado la conexión VPN, accedan a un entorno de escritorio remoto dentro de la organización y que sea desde ahí desde donde se trabaje. De esta forma se evita tener que configurar aplicaciones de usuario en el equipo remoto, se garantizan las políticas de seguridad globales (ya que el escritorio remoto está gestionado por los administradores de sistemas) y se reduce drásticamente la posibilidad de infección por software malicioso quedando en la mayoría de los casos únicamente la posibilidad de que se comprometa la seguridad por tener instalado algún software que capture las pulsaciones del usuario, y con ello las contraseñas de acceso. Es precisamente en este tipo de conexiones cuando cobra sentido la utilización de una distribución live que únicamente se utilice para activar la VPN y conectar a un escritorio remoto.

Por último, existen otras soluciones más complicadas como líneas de comunicaciones dedicadas, o conexiones por satélite, pero son muy poco frecuentes debido a su alto coste frente a la seguridad que ofrecen otras soluciones más económicas como la VPN a través de Internet.

4.2 VPN

Las siglas VPN, hacen referencia a las Redes Privadas Virtuales (Virtual Private Network). A grandes rasgos, estas redes hacen que un usuario pueda conectarse de forma segura, para él y para la organización, a servicios o servidores que no se encuentran directamente accesibles a Internet. Mediante un sistema de certificados digitales, estas redes consiguen que el usuario tenga la certeza de que se está comunicando con las aplicaciones correctas (no es posible que le falsifiquen las direcciones de las empresa) y se asegura que todo lo que envíe y reciba está cifrado y a salvo de interceptaciones o robos de información. Además, estas redes también permiten trabajar desde casa como si fuese desde la propia oficina, teniendo acceso a todos los recursos internos que sean necesarios, pudiendo utilizar programas internos, clientes de correo electrónico, e incluso llegar a imprimir remotamente.

La gran expansión que ha tenido esta tecnología se debe en parte a que son relativamente sencillas de utilizar para los usuarios ya que, una vez hecha la configuración inicial, bastará con arrancar un programa e introducir la contraseña para que todo quede configurado.

Estas redes también son muy ventajosas para los administradores de los sistemas ya que trabajan con una única entrada de usuarios a los sistemas. De esta forma evitan tener que disponer un acceso abierto para cada una de las aplicaciones con sus consiguientes riesgos de ataque y sus controles de seguridad.

Otra de las bondades de las redes VPN radica en su robustez y seguridad ya que pueden configurarse, y de hecho es lo más frecuente, para que utilicen autenticación fuerte de doble factor: esto consiste en que se instala un certificado en el equipo del usuario que solo se puede utilizar combinado con su contraseña, por lo que para poder conectar es necesario algo que el usuario tiene (su certificado), y algo que el usuario sabe (su contraseña), evitando así ataques de fuerza bruta o intrusiones porque al usuario le hayan robado su contraseña.

Respecto de los certificados, se presentan en varios formatos, desde tarjetas inteligentes hasta simples ficheros que se importan en el equipo. En caso de que el certificado sea de los que se instalan, debe tenerse en cuenta que si el equipo lo utilizan otros usuarios no debe dejarse instalado al alcance de cualquiera. Si se ha estado utilizando un equipo ajeno o uno de préstamo siempre debe eliminarse cualquier certificado que se haya instalado o la mencionada autenticación de doble factor pierde sentido.

4.3 Herramientas de administración remota

En ocasiones los usuarios deben conectar desde su casa a la oficina, ya sea por motivos de teletrabajo o simplemente comprobar el correo. En los casos en que esto no está permitido o cuando simplemente no se conocen los procedimientos oficiales, algunos usuarios recurren a aplicaciones de gestión remota como pueden ser LogMeIn o TeamViewer. Para utilizarlas basta con instalarla en el equipo de la oficina, dejar el equipo encendido al marcharse y luego conectar desde casa trabajando como si estuviese en el propio equipo.

En este tipo de aplicaciones generalmente se cifran las comunicaciones, además de evitar tener que configurar cortafuegos o similar, por lo que puede parecer que son unas herramientas perfectas, pero realmente se trata de una práctica desaconsejable en la mayoría de las organizaciones.

Al instalar este tipo de aplicaciones en realidad se está abriendo una puerta trasera al equipo y a la red interna de la organización, que tira por tierra muchas de las medidas de seguridad implantadas, como puede ser el filtrado de conexiones mediante cortafuegos, control de conexiones desde VPN, revisiones de usuarios con teletrabajo, robustez de contraseñas, etc., permitiendo que un atacante pueda probar contraseñas directamente contra un servicio web gestionado por un tercero y sobre el que tenemos poco o ningún control.

Además de lo anterior, cabría la posibilidad de que los empleados de estas compañías conectaran a nuestros equipos sin permiso, o incluso una intrusión en sus sistemas daría acceso a todos los equipos clientes, por lo que no son soluciones aconsejables.

5 Seguridad de la información

De momento se han tratado temas referentes a la protección de los equipos y las telecomunicaciones, pero no se debe perder el objetivo principal de esta guía: proteger la información de la organización.

A continuación se detallarán los controles y medidas que se deberían tener en cuenta para proteger directamente la información, especialmente cuando se encuentra almacenada.

5.1 Copias de seguridad

Generalmente, en entornos corporativos se hacen copias de seguridad de forma automática: los servidores disponen de software específico para ello, mientras que los usuarios acostumbran a trabajar contra unidades de red o con perfiles de dominio móviles que hacen que en cada apagado del equipo todos los documentos personales se sincronicen. Lamentablemente, cuando se habla de teletrabajo no siempre se siguen las mejores prácticas en lo referente a las copias de seguridad de la información.

Se debe ser consciente de que cualquier información que se saca de las instalaciones, especialmente en equipos portátiles, corre peligro de ser robada junto con el dispositivo, sufrir un accidente doméstico que inutilice el acceso o que se pierda por una subida de tensión en el lugar de teletrabajo.

El cómo operar dependerá principalmente de la modalidad de teletrabajo:

- **Escritorios remotos:** este viene a ser el único caso donde generalmente se gestionan correctamente las copias de seguridad de los datos del usuario ya que este conecta directamente contra un servidor del entorno corporativo del cual se hacen copias de seguridad completas.
- **Perfil móvil, o sincronización automática:** en estos casos periódicamente se sincroniza de forma automática el contenido del PC del usuario con el entorno corporativo.

  Si bien parece una solución sencilla y cómoda, generalmente los usuarios no tienen los conocimientos necesarios para configurarlo por lo que es necesaria la intervención del departamento de sistemas para configurarlo correctamente, lo cual puede ser especialmente problemático en caso de que el usuario utilice su equipo personal para trabajar desde casa.

  Además, dependiendo del volumen de los datos a transferir esta tarea puede ser extremadamente lenta teniendo en cuenta las pequeñas velocidades de subida que acostumbran a tener las conexiones de particulares, situación que se puede agravar más en caso de conectar mediante un modem 3G o similar, por lo que es necesario tener estos factores en cuenta e intentar optimizar el uso de la conexión sincronizando únicamente los ficheros actualizados recientemente (también llamadas copias incrementales).
- **Sincronización manual:** como su propio nombre indica, no es otra cosa que copiar periódicamente los ficheros actualizados contra algún servidor de la plataforma corporativa. A pesar de lo rudimentario que parece, según las necesidades y profesionalidad del usuario, puede ser una solución totalmente válida siempre y cuando se lleve un control sobre la misma. Los principales problemas de esta solución son que no se hagan las copias con la frecuencia establecida por dejadez, o que la criticidad de la información y su volumen no hagan viable el hacer sincronizaciones manuales.

- **Copias de seguridad offline:** siempre que hablamos de copias de seguridad, automáticamente pensamos en servicios en la nube, en servidores en ubicaciones diferentes, o soluciones relativamente tecnológicas olvidando que las copias locales son otra opción que, según las necesidades, también puede resultar válida. Si se elige este tipo de copia, por lo general se recomienda utilizar un dispositivo externo con el fin de evitar que un fallo físico, o algún tipo de código malicioso corrompa la información almacenada en todo el equipo. Deberán tenerse en cuenta también la posible necesidad de cifrar el soporte donde se almacenen las copias, almacenar el dispositivo bajo llave, o guardarlo en un lugar a salvo de peligros domésticos (fuego, agua, hijos pequeños, etc.).

5.2 Gestión y traslado de contraseñas

Generalmente en un entorno de trabajo presencial, además de necesitar una contraseña para acceder al sistema, es necesario tener conectividad con la red corporativa. Este requisito hace que si la red está correctamente segmentada, si no hay puertas traseras, y si las redes inalámbricas están correctamente configuradas, una contraseña robada sea relativamente poco crítica. No obstante, si hablamos de teletrabajo esta situación puede ser especialmente crítica ya que con una contraseña se podría acceder remotamente a los sistemas.

En caso de disponer de una conexión VPN (ver apartado *4 Comunicaciones*) que dé acceso a todos los demás servicios, debemos custodiar con extremo cuidado esta contraseña y seguir las mejores prácticas posibles: caducidad, complejidad, bloqueo por intentos fallidos, bloqueo por inactividad, revisiones de acceso, etc. Si por el contrario se trata de diferentes servicios (generalmente web) de los cuales cada uno dispone de una contraseña diferente la situación se complica ya que nunca se debe utilizar una única contraseña para todo.

Para poder mantener las diferentes contraseñas y garantizar que no se van a olvidar, es muy recomendable almacenarlas en un gestor de contraseñas, el cual garantizará que están a salvo de robos además de permitir transportarlas, por ejemplo, en una memoria USB o incluso online en caso de necesitar movilidad.

Si no se está familiarizado con los gestores de contraseñas, recomendamos consultar la guía de CSIRT-cv guía disponible en el siguiente enlace.

5.3 Cifrado del disco duro y soportes

Indiscutiblemente proteger la información que se almacena fuera de la oficina es una de las mayores preocupaciones a la hora de disponer de trabajadores en modalidad de teletrabajo, tal vez porque el robo o pérdida de un dispositivo portátil es algo que puede ocurrir con relativa facilidad.

Contra este tipo de fugas de información no es suficiente con poner contraseña a la BIOS del equipo o a la cuenta del sistema operativo, ya que si se saca el disco duro y se conecta a otro equipo, por mucha contraseña que tuviera el portátil o el sistema operativo, la información sería accesible.

Contra este tipo de amenaza, existen 2 soluciones: no almacenar nada de información en el equipo y usarlo únicamente online (algo relativa complicado según el tipo de trabajo), o cifrar la información.

Cifrar la información no es otra cosa que protegerla de forma que sea imposible acceder a ella sin conocer la contraseña de descifrado, incluso accediendo directamente al disco duro.

Existen diferentes soluciones de cifrado cuya elección dependerá de las necesidades de seguridad y usabilidad, pero a grandes rasgos son las siguientes:

- **Cifrar una carpeta o el disco completo mediante el propio sistema operativo:** Los principales sistemas operativos disponen de herramientas de cifrado, ya sea para cifrar las carpetas personales del usuario llegando algunos incluso a permitir cifrar todo el disco duro.

Son soluciones sencillas ya que la mayoría de las veces no necesitan instalar software adicional, además de utilizar la contraseña de inicio de sesión del usuario para descifrar, con lo que el usuario no tiene que hacer acciones extra para acceder a la información. Por contra, este sistema tiene algunos inconvenientes, como pueden ser la imposibilidad de poder utilizar estas carpetas cifradas en otros sistemas operativos, o lo complicado que resulta en ocasiones el recuperar los datos en caso de que el sistema operativo deje de funcionar.

Además si se va a optar por este método de cifrado, es recomendable cifrar únicamente los datos de los usuarios ya que cifrar todo el disco repercutiría negativamente en el rendimiento del equipo, además de informarse de si es posible recuperar los datos con una contraseña maestra en caso de fallo del sistema operativo.

- **Crear un volumen cifrado:** existen herramientas que permiten, en lugar de cifrar una carpeta o un disco duro, crear un único fichero que contendrá la información cifrada. La principal ventaja de estas herramientas es que estos volúmenes cifrados pueden llevarse en una memoria USB y acostumbran a estar disponibles para los principales sistemas operativos. Además ofrecen una mayor sensación de control sobre la información, ya que pueden copiarse con un simple "copiar y pegar" y el fichero cifrado siempre está localizable y disponible para poder recuperarlo en caso de avería del sistema operativo. Por el contrario, resultan más incómodos de utilizar que la solución de utilizar el propio software del sistema operativo, ya que obligarán a que cada vez que se inicia el ordenador se tiene que poner la contraseña del volumen cifrado.

En ambos casos, la seguridad de la información dependerá de la complejidad de la contraseña por lo que resulta necesario utilizar una clave robusta.

5.4 Papel

Aunque estas guías acostumbran a hablar únicamente de la información en formato digital, no se debe perder de vista la documentación en papel ya que su contenido puede ser igualmente importante.

Si bien por lo general en un entorno de teletrabajo la información en papel es menos susceptible de sufrir ataques deliberados (siempre y cuando no haya un trasiego habitual de documentación), el no estar en un ambiente laboral puede hacer que documentación relevante acabe junto con el papel y cartón para reciclar, se utilice para dibujar por detrás o que sufra algún accidente doméstico como que se derramen bebidas sobre él.

Es por ello que se deben de tomar una serie de medidas de sentido común muy similares a las que se siguen en la oficina:

- Se deben almacenar los documentos en lugar seguro mientras no se estén utilizando. Las medidas de seguridad se establecerán en base a los requisitos que su clasificación marque.
- Se tomarán las medidas de seguridad que se consideren oportunas para el transporte de la documentación, las cuales pueden ir desde no dejar la documentación desatendida, hasta utilizar contenedores especialmente preparados para ello.
- Se debe estudiar el modo de destruir la información en papel evitando tirarla directamente al contenedor del reciclaje (habitual en la mayoría de hogares), o peor aún, que se reutilice para labores domesticas (dibujar por detrás, hacer la lista de la compra, etc.).
- Se deben aplicar el resto de buenas prácticas en cuanto a la gestión del papel, como pueden ser no dejar las copias impresas desatendidas en la bandeja de la impresora, o configurar el fax para que no imprima los faxes entrantes hasta que se solicite expresamente, evitando así que queden olvidados en la bandeja de impresión.

5.5 Sistemas de almacenamiento online

Hace ya tiempo que aparecieron multitud de servicios online para almacenar ficheros y trabajar con ellos desde cualquier ubicación ya sea de forma individual como colaborativa. Años atrás se utilizaba masivamente Megaupload y Rapidshare, dejando paso recientemente a Dropbox, seguido de cerca por Google Drive o Skydrive.

El éxito de estas herramientas se fundamenta en todas las siguientes características:

- Sincronización entre diferentes dispositivos
- Copias de seguridad online
- Control de versiones
- Acceso compartido para varios usuarios
- Eliminan la necesidad de utilizar memorias USB
- Aplicaciones nativas para diferentes sistemas operativos, tanto de PC como dispositivos móviles
- Facilitan la conciliación tecnológica de la vida laboral y personal (todo es accesible desde cualquier dispositivo)
- Acostumbran a ser gratuitas (al menos los primeros gigas y casi siempre para uso personal)
- Facilitan el envío por Internet de ficheros de grandes tamaños

A pesar de todas estas características, se deben tener en cuenta los peligros que su utilización conlleva.

En primer lugar se debe valorar el nivel de seguridad de la información que se vaya a cargar en este tipo de servicios ya que ante un ataque a la plataforma sería posible acceder a toda la información del usuario.

Una vez más es posible que los propios empleados de la empresa de almacenamiento online pueda acceder a los datos por lo que dependiendo de la criticidad de la información puede ser necesario tomar medidas adicionales como el cifrado previo de la información, o el uso de medidas de protección de la propia plataforma, generalmente de pago, que aporten capas adicionales de seguridad.

Existen también plugins y complementos que se encargan de cifrar la información de estos servicios, pero dependiendo de la aplicación, una vez más pasamos a delegar la seguridad de nuestros datos en un tercero, por lo que la situación final no siempre es un incremento de la seguridad.

Por otro lado se debe considerar que dependiendo de la naturaleza de los datos se puede incurrir en el incumplimiento de normativas y leyes de protección de datos ya que en muchas ocasiones estos servicios se alojan en grupos de servidores repartidos por todo el planeta por lo que es muy difícil saber donde está realmente la información, así como saber qué legislación le aplica. Al respecto se debe ser extremadamente cuidadoso con datos de carácter personal especialmente sensibles.

Tampoco pueden descuidarse otros temas como los contratos de prestación de servicio que ofrecen estas plataformas ya que no siempre se comprometen a garantizar la disponibilidad de la información, pudiendo tener fallos técnicos que les dejen sin conectividad durante días, o pudiendo llegar al extremo de cerrar de un día para otro (o ser confiscados los servidores, como ya le sucedió a Megaupload) dejando al usuario sin posibilidad de recuperar sus datos.

Si se desea ampliar información sobre este tema, CSIRT-cv dispone de una guía completa de uso seguro de Dropbox en el siguiente enlace, cuyos consejos son extensibles al resto de servicios similares.

6 Seguridad de los RRHH

Es sabido que el usuario es el eslabón más débil de la cadena de la seguridad de la información ya que además de estar expuesto a los riesgos tecnológicos, puede ser víctima de ataques de ingeniería social (engaños), robos, agresiones físicas, extorsión, etc.…

Por desgracia, existen pocas medidas de seguridad que aplicar sobre las personas más allá del sentido común y la formación, por lo que es precisamente en estos puntos donde más esfuerzos se tienen que invertir.

Cualquier usuario que realice su actividad mediante teletrabajo debe estar familiarizado con todos los conceptos que aparecen en esta guía, debe entender los riesgos a los que se enfrenta por no utilizar una arquitectura tradicional, y se le debe informar de las responsabilidades adicionales con respecto a la información y servicios de que disponga en comparación con un puesto de trabajo presencial.

6.1 Ingeniería social

Se conocen como ataques de ingeniería social aquellos que tratan de conseguir información mediante engaños a los usuarios.

Los más frecuentes suelen ser correos electrónicos o llamadas telefónicas suplantando a algún compañero, proveedor o cliente y solicitando cualquier tipo de información, o llegando incluso a suplantar al soporte técnico y pedir al usuario que ejecute comandos en su equipo o que comparta las contraseñas de acceso.

Si bien este tipo de ataque puede afectar a cualquier empleado, el hecho de trabajar a distancia hace que sea posible que el usuario no conozca físicamente a sus compañeros, o que el comunicarse siempre por teléfono le haga ser más confiado ante una llamada maliciosa.

Para evitar este tipo de ataques se debe de formar al usuario para que sepa en todo momento la información que puede dar por teléfono y la que no, como por ejemplo configuraciones de red, contraseñas o ficheros con información sensible.

Por otro lado se debería de establecer un protocolo para identificar al interlocutor en las llamadas telefónicas que vayan a requerir intercambiar información sensible, especialmente si los usuarios no se conocen. Puede ser algo tan sencillo como disponer de un listado de numero de teléfonos autorizados, intercambiar verbalmente contraseñas pre-pactadas mediante métodos seguros, o sencillamente ser el propio usuario que haga la llamada hacia la sede de la organización y que sea la centralita quien redirija las conversaciones.

Cabe destacar que este tipo de ataques pueden llegar a ser muy elaborados pudiendo desde crearse perfiles falsos en redes sociales profesionales como Linkedin y hacerse pasar por alguien de la empresa, hasta llegar a entablar una relación amistosa en redes más generalistas para, con el tiempo, obtener información sensible.

7 Al finalizar el trabajo…

En un entorno de trabajo presencial generalmente se utiliza un PC por usuario, lo cual hace posible ser relativamente laxos a la hora de apagar el equipo para seguir trabajando al día siguiente, pero en un entorno de teletrabajo donde es posible que el equipo se pierda, cuando se utiliza el equipo de casa para trabajar al cual tienen acceso otros miembros de la familia, o donde se utiliza un equipo que no es del propio usuario (jamás se debería trabajar desde un cibercafé u ordenador de un hotel/aeropuerto, pero sabemos que sucede), se recomienda seguir los siguientes consejos para proteger adecuadamente la información y las comunicaciones. Aunque algunos puedan parecer excesivos, se deberán aplicar según la criticidad del equipo y su acceso por parte de otros usuarios:

- Cerrar todas las conexiones con servidores y páginas web utilizando cuando sea posible la opción "desconectar" o "cerrar sesión".
- Eliminar información temporal prestando especial atención a la carpeta de descargas, papelera de reciclaje, o posibles carpetas perdidas que se dejen en "Mis documentos".
- Utilizar herramientas de borrado seguro para eliminar los ficheros en caso de información sensible o especialmente confidencial.
- Si se han utilizado certificados digitales, estos deben ser borrados de forma segura.
- Asegurarse de retirar cualquier memoria USB, CD o DVD que se haya utilizado en el equipo.
- Borrar el histórico de navegación, así como las cookies, y otros datos del navegador web, prestando especial atención a las contraseñas recordadas.