ENJOY SAFER TECHNOLOGY™

PARA COLABORADORES

GUÍA DE Teletrabajo

Introducción

Con el crecimiento de las tecnologías de la información y la comunicación, cada vez más colaboradores tienen la posibilidad de conectarse a los servicios de la empresa desde cualquier lugar e incluso desde cualquier lugar o dispositivo; o incluso a trabajar de forma remota para compañías que no tienen sede en su país de residencia.

Las ventajas de esta nueva tendencia están a la vista; los empleados ahorran tiempo y dinero en viajes, pueden trabajar más distendidos y administrar mejor su trabajo; para la empresa esto significa un aumento en la productividad y una reducción en los costos de infraestructura.

Sin embargo, esta modalidad laboral trae aparejados una serie de retos a la hora de asegurar la confidencialidad, integridad y disponibilidad de la información. Las medidas habituales de seguridad que se aplican dentro del dominio de la empresa no alcanzan para proteger los datos que son manipulados fuera del mismo, por lo que, el control al acceso y uso de la información se torna cada vez más complicado. Esto hace que la responsabilidad de cuidar la información sea cada vez más un compromiso del trabajador.

El objetivo de este documento es brindar información a los colaboradores respecto a cómo proteger la información, especialmente cuando se encuentran trabajando remotamente.

Índice

¿Qué es el teletrabajo? 03

Riesgos y amenazas 04

Política corporativa 05

Herramientas de teletrabajo para el Empleado 06

- Dispositivos móviles 06
- - Contraseña de acceso al equipo 06
- - Protección Antirrobo 06
- Dispositivos de almacenamiento 07
- - Cifrado 07
- - Backup 07
- Conectividad 08
- - Redes Públicas/Redes Privadas 08
- - VPN 09
- - Doble factor de Autenticación 09

Antivirus y soluciones de seguridad 10

Soporte: ¿a quién llamar si algo falla? 11

Buenas prácticas de seguridad 12

Conclusión 13

¿Qué es teletrabajo?

El teletrabajo es una modalidad de trabajo a distancia que **consiste en realizar las tareas habituales desde un lugar diferente al domicilio de la empresa utilizando como soporte diferentes tecnologías de comunicación.**

Existen muchas actividades que no necesariamente deben ser ejecutadas en una oficina ni requieren la presencia del trabajador en su puesto del trabajo, por lo que pueden realizase en un lugar distinto. Hoy en día, la incorporación de nuevas formas de comunicación permite facilitar las tareas y ejecutar el trabajo satisfactoriamente independientemente de dónde se realice.

Hacer "Home Office" no significa trabajar necesariamente desde las comodidades del hogar, sino que se refiere a toda forma de trabajo remoto, siempre y cuando se cuente con las herramientas necesarias para realizarlo. Es decir que trabajar desde la casa de un amigo, un bar, una biblioteca hasta incluso el hotel o el aeropuerto durante un viaje de negocios son también formas de teletrabajo.

Esta metodología tampoco se limita a los empleados en relación de dependencia, por el contrario, son muchos los trabajadores autónomos e independientes que trabajan conectándose remotamente a diferentes clientes, aprovechando las ventajas de las telecomunicaciones.

Por lo tanto, cada vez que un empleado, ya sea en relación de dependencia o autónomo, realice sus tareas habituales fuera del domicilio del empleador (o del cliente) utilizando tecnologías de comunicación, se lo considera teletrabajo.

Riesgos y amenazas

Más allá de los beneficios del teletrabajo, esta metodología también implica la consideración de ciertos riesgos, los cuales habitualmente son mitigados dentro del domicilio del empleador, pero quedan fuera de alcance cuando la información es accedida remotamente.

Estos riesgos pueden materializarse debido a situaciones intencionales o accidentales y comprometer la seguridad de la información, tanto del trabajador como de la empresa.

Podemos clasificarlos a través de la manera en que comprometen la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad

Riesgos que pueden provocar que un tercero no autorizado, sea un individuo o un proceso, acceda a información privada. Algunos ejemplos son:

- Conectarse a una red Wi-Fi desconocida o insegura puede provocar que un tercero, conectado a la misma red, pueda interceptar la información recibida o enviada desde el equipo.
- Si un equipo es robado, también lo es la información dentro del mismo y puede quedar expuesta a un delincuente.

Integridad

Situaciones en donde un tercero no autorizado, sea un proceso o un individuo, podría alterar la información.

- Un código malicioso que infecta un equipo puede modificar tanto la información alojada en el mismo, como aquella a la que el equipo, o usuario infectado, tenga acceso.
- En una conexión remota insegura, un individuo podría alterar los certificados y firmas digitales y suplantar una identidad.

Disponibilidad

Amenazas que podrían generar que un sistema deje de estar accesible o utilizable cuando sea requerido.

- La información alojada en un dispositivo, o incluso el dispositivo en sí, pueden ser cifrada por un código malicioso que infectó el equipo y, así, quedar inutilizada.
- El acceso remoto a información o servicios alojados en servidores de la empresa puede verse interrumpido si la conexión es inestable.

Dentro del dominio de una empresa estos riesgos suelen ser mitigados o controlados por distintos departamentos, aplicando diversas medidas de seguridad, pero **al encontrarse fuera de este entorno protegido pasa a ser una responsabilidad del trabajador mitigarlos o reducirlos.**

Política corporativa

Antes de entrar en temas técnicos, herramientas de trabajo o configuraciones, es fundamental establecer un marco normativo que estandarice las condiciones y procedimientos mediante los cuales se va a desarrollar el teletrabajo.

La empresa debe proveer a los colaboradores una política de teletrabajo clara que abarque puntos como:

- Quiénes tendrán acceso a esta modalidad y en qué circunstancias.
- Procedimiento de conexión remota.
- Equipos y herramientas que se van a utilizar para desarrollar las tareas.
- Cómo se debe manejar la información fuera de las instalaciones.
- Cuál es procedimiento o contacto en caso de necesitar asistencia técnica.
- Responsabilidades y obligaciones del teletrabajador en cuestiones de seguridad de la información.

Es crucial, tanto para el trabajador como para el empleador, que las reglas estén claras. Antes de comenzar a trabajar de manera remota, de conectarse a la red de la empresa o de utilizar diferentes dispositivos para acceder a la información, es importante que el trabajador conozca y entienda la política de trabajo. Es necesario que tenga claro cuáles son sus responsabilidades en cuanto a la seguridad, si puede o no utilizar dispositivos propios y, de ser así, qué cuidados debe tener, de qué manera puede hacer uso de los servicios de comunicación de la empresa y, sobre todo, cuáles son las medidas de seguridad establecidas y cuáles son las herramientas disponibles para cumplir con esas medidas.

Ya sea que se trate de empleados en relación de dependencia o trabajadores autónomos que manejan información de clientes, en todos los casos es imprescindible conocer la política de teletrabajo o de acceso remoto, de forma que siempre se sigan **los lineamientos de seguridad del negocio**.

Herramientas de Teletrabajo para el empleado

A la hora de trabajar de manera remota es necesario contar con herramientas que permitan tanto la portabilidad como la conectividad a los servicios y sistemas del empleador. Estas herramientas, tanto físicas como digitales, son variadas y cada vez más populares. A continuación, analizaremos las más comunes y explicaremos de qué manera protegerlas.

Dispositivos móviles

Dentro de las herramientas que hacen posible el teletrabajo, las más comunes son los dispositivos móviles. Ya sean notebooks, tablets o celulares, estos equipos facilitan la movilidad y permiten realizar diferentes tareas desde la comodidad del hogar, un medio de transporte, durante un viaje o cualquier otro sitio remoto.

A través de estos dispositivos se accede a información sensible y se la almacena, por lo que es importante tener en cuenta los riesgos asociados a su uso y, sobre todo, a la pérdida o robo de los mismos.

Contraseña de acceso al equipo

Si se trabaja desde un lugar público o una oficina compartida con otras personas desconocidas, es importante **nunca dejar el equipo desatendido**. Además, en caso de no utilizarlo por un período de tiempo siempre se debe **bloquear con una contraseña**, incluso es importante que el mismo se bloquee automáticamente por inactividad. De esta forma se evita que en un momento de descuido un tercero pueda acceder fácilmente a la información del equipo.

Protección Antirrobo

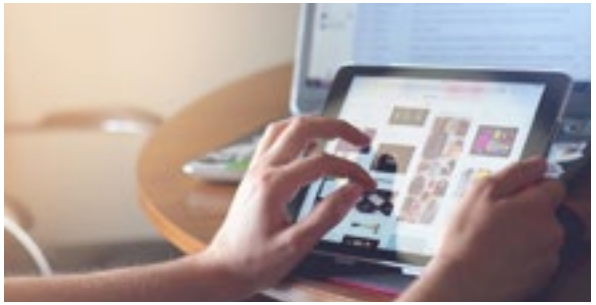
En el caso de que un equipo se pierda o alguien lo robe, existen herramientas que previenen que la información o los accesos almacenados sean accedidos por terceros, así como también pueden ayudar a localizarlo y recuperarlo.

La función de la protección antirrobo permite rastrear el dispositivo mediante la función GPS del mismo para intentar recuperarlo, así como también enviar mensajes al mismo que pueden ser leídos por la persona que lo haya encontrado.

Además, es posible **monitorear la actividad** del mismo, detectar acciones extrañas e incluso ver fotografías capturadas con la cámara o desde la misma pantalla. Todo esto, protegiendo las cuentas e información del usuario para que no puedan ser accedidas por quien tenga el equipo.

Por último, esta funcionalidad permite realizar ciertas **acciones de prevención** en el equipo de manera remota, habitualmente mediante el envío de un SMS, como por ejemplo **bloquear** el mismo, **apagarlo** o hasta **eliminar todos los datos** almacenados y restaurar la configuración de fábrica.

Es muy recomendable activar este tipo de protección, tanto en equipos móviles personales como corporativos.



Dispositivos de Almacenamiento

Dentro de los equipos móviles suele viajar mucha información, tanto archivos como certificados personales e información de sesión de las diferentes cuentas. Esta información se almacena en los discos y memorias de diferentes dispositivos, como el disco de una laptop, la memoria de un celular o incluso un pendrive.

En el caso de extraviar cualquier dispositivo, también lo hará la información dentro de él, por lo que es importante tener en cuenta las siguientes tecnologías y medidas de seguridad:

Cifrado

El cifrado es una medida de seguridad muy utilizada para proteger los datos alojados en un dispositivo. Consiste en alterar la información de acuerdo a un patrón establecido por una clave (o llave), de tal forma que solamente puedan ser entendidos por quienes conocen esa clave.

Al cifrar la información la volvemos ilegible a la vista, por lo que, si el equipo es robado, cae en manos de terceros o, incluso, es infectado por un código malicioso que intenta robar los archivos, lo único que verán o se llevarán serán caracteres sin sentido.

A pesar de lo que comúnmente se cree, utilizar herramientas de cifrado es realmente práctico y fácil de hacer para cualquier usuario. Basta con saber qué información queremos proteger y configurar la herramienta de cifrado que utilicemos con una clave fuerte y segura. **Para más información recomendamos revisar la Guía de Cifrado.**

Backup

Nos hemos referido en esta guía a cómo proteger la información para que no sea accedida ni modificada por terceros no autorizados, incluso si se extravía un dispositivo. Sin embargo, es importante pensar también de qué manera recuperar la información perdida para poder continuar con las tareas habituales.

En este sentido, se deben respaldar todos aquellos archivos que no puedan volver a obtenerse con facilidad. Por ejemplo, documentos de autoría propia, informes, investigaciones, planillas y presentaciones; incluso fotografías y documentos personales.

Los tipos de respaldo que se pueden utilizar son diversos y se debe evaluar cuál se adapta a las necesidades de cada usuario. **Para más información recomendamos leer la Guía de Backup.**

Conectividad

Hoy en día la conectividad se ha vuelto un servicio básico para el desarrollo de la vida cotidiana y es posible acceder a Internet desde diversos sitios y conexiones, incluso, de manera gratuita.

Así como esta tecnología hace posible el desarrollo del teletrabajo, también puede ser la puerta de entrada para algunas amenazas si no está bien configurada o algún intruso se encuentra conectado a la misma. Es por esto que siempre es preferible utilizar redes inalámbricas seguras para evitar riesgos.

Redes Públicas/Redes Privadas

La mayoría de las empresas cuentan con redes Wi-Fi privadas que protegen los datos que viajan por la red y garantizan a los usuarios una navegación segura. Sin embargo, cuando la conexión es remota es necesario un punto de acceso a Internet, que no suele tener los mismos controles ni medidas que la red interna de la empresa.

¿Cuáles son las redes inalámbricas seguras?

Son aquellas en las que se han aplicado diversas medidas de seguridad para prevenir que terceros no autorizados se conecten. Dentro de estas medidas de seguridad hay una fundamental que es posible identificar fácilmente: **la contraseña**. Una red sin contraseña o con una contraseña débil puede ser fácilmente accedida por ajenos. De esta forma, una persona con los conocimientos adecuados podría fácilmente obtener una contraseña con cifrado WEP mucho más fácilmente que una **cifrada en WPA o WPA2**, siendo esta última la más segura y recomendada.

En el caso de las redes hogareñas, también es importante que el **router Wi-Fi no pueda ser accedido desde el exterior** y cuente con una clave de administrador fuerte y difícil de adivinar. Por último, es recomendable mantener actualizado el firmware del router y monitorear los equipos conectados a la red.

Por otro lado, existen también las redes públicas, que resultan muy útiles al momento de trabajar desde un bar, un aeropuerto o cualquier otro lugar público. Se trata, normalmente, de redes abiertas que son ofrecidas como un servicio adicional al cliente. Estas conexiones no poseen medidas de seguridad restrictivas y cualquier persona conectada a la misma puede interceptar e incluso manipular el tráfico de otros equipos en la red. En el caso de conectarse de esta forma, es necesario aplicar las configuraciones más restrictivas de seguridad, especialmente en lo que respecta a archivos compartidos y acceso al sistema. Si no se tienen en cuenta los controles de seguridad pertinentes, es recomendable **evitar el uso de servicios que requieran información sensible en conexiones inalámbricas públicas.**

Es frecuente utilizar redes que no son ni del propio hogar ni públicas, sino redes de terceros, ya sea la de un hotel, la casa de un amigo, etc. A pesar de ser privadas, el usuario no conoce a las otras personas conectadas a la misma red, ni sus intenciones. Por lo tanto, se deben tomar los recaudos como si fueran públicas, aun cuando se conozca y se tenga confianza sobre el administrador de la misma.

VPN

Las VPNs (Red Privada Virtual) son conexiones cifradas que se utilizan **para conectarse de manera segura a una red privada conocida**, por ejemplo, la red interna de una empresa.

Si bien existen diferentes protocolos para conectarse vía VPN, todos ellos utilizan comunicaciones cifradas, es decir que los datos transmitidos son ilegibles hasta que llegan a destino. De esta forma, por más que sean interceptados por un tercero no podrá leerlos ni utilizarlos.

La mayoría de las empresas brindan a sus usuarios conexiones VPN para poder acceder a los servicios de la red interna de manera remota.

Dado que estas conexiones son cifradas, es recomendable utilizarlas siempre que se esté conectado a una red pública o insegura, ya que evitarán que la información sea interceptada (o de serlo, que sea inútil).

Doble Factor de Autenticación

La doble autenticación es un sistema que complementa la autenticación tradicional en los servicios. Es decir, además de requerir un usuario y una contraseña para acceder a un sistema o servicio, también requiere un tercer dato, como puede ser un código de seguridad, una huella digital o cualquier otra información adicional que posea el usuario. Habitualmente, se utiliza un código generado de manera aleatoria en un dispositivo, como puede ser un token o una aplicación en el teléfono celular.

El objetivo del doble factor de autenticación es proteger el acceso a cuentas y servicios del usuario si la contraseña del mismo es comprometida, ya sea por un código malicioso, por una filtración de información o un engaño. Sea cual fuera el caso por el cual las credenciales de una cuenta puedan haber sido obtenidas por un tercero, tener habilitado un doble factor de autenticación evitará que pueda acceder a la misma si no posee el código correspondiente.

Cuando se trabaja de manera remota aumentan los riesgos de que las credenciales puedan ser obtenidas por un atacante, especialmente al conectarse a redes no seguras o compartidas. Si se requiere un tercer dato para iniciar sesión, el atacante no podrá ingresar a la cuenta por más que obtenga el usuario y la contraseña.

Antivirus y soluciones de seguridad

Por más que el trabajador tome todas las medidas indicadas en esta guía, siempre puede existir una posibilidad de infectarse con un código malicioso, entrar a una página fraudulenta o comprometer información en la red sin darse cuenta. La razón: ningún equipo está libre de riesgos.

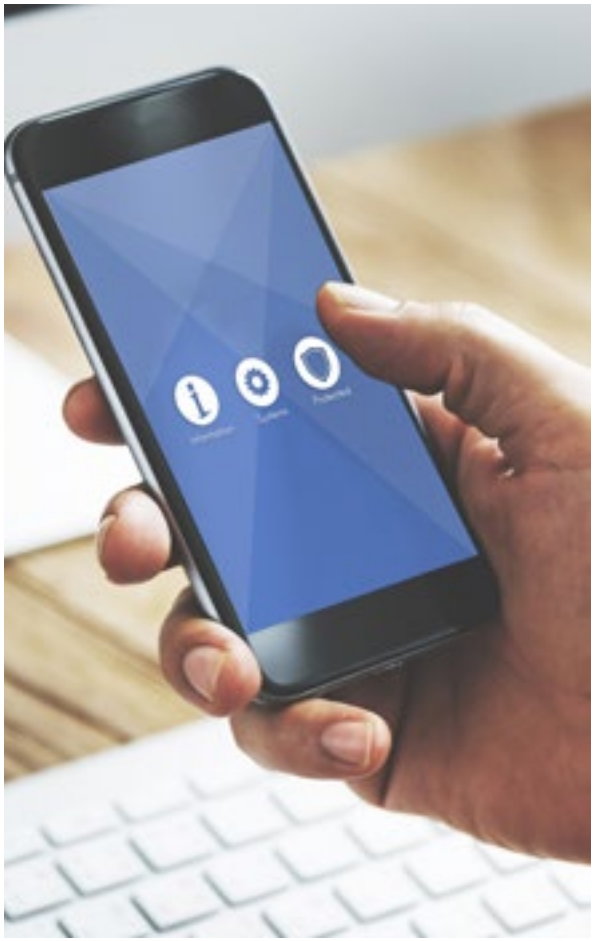
Esto hace que sea sumamente importante complementar todas las precauciones con un sistema de **detección proactivo de amenazas**, lo cual se consigue **instalando una solución integral de seguridad** en los dispositivos.

Hablamos de solución integral y no meramente de antivirus, ya que hoy en día no basta con detectar únicamente códigos maliciosos. Estas soluciones cuentan con diferentes módulos que detectan también otros tipos de amenazas, como por ejemplo, conexiones inseguras, sitios engañosos, paquetes malformados y otras señales que pueden indicar un posible riesgo.

Cuando el trabajo remoto se da en empresas donde el usuario utiliza equipos corporativos para conectarse y manipular información, los mismos suelen estar protegidos por una solución de seguridad proveída y administrada por la misma empresa.

Sin embargo, **en los casos donde el trabajador utiliza sus propios dispositivos, esta medida de seguridad resulta indispensable**. No solo se debe contar con una solución de seguridad en cada equipo, ya sean de escritorio o móviles, en los que se manipule información sensible, sino que también **es necesario mantener la misma actualizada** para prevenir nuevas amenazas.

En el caso de los equipos hogareños, sobre todo aquellos que son utilizados por diferentes miembros del hogar, se elevan los riesgos de ser víctimas de una amenaza, ya que resulta difícil controlar el uso del equipo, las descargas que se realicen o los sitios a los que se accede. Contar con un producto respaldado por una empresa de seguridad confiable y con trayectoria en el mercado soluciona estos problemas muy rápidamente, brindando una capa de seguridad a todos los usuarios.



Soporte: ¿a quién llamar si algo falla?

Tal como hemos mencionado a lo largo de esta guía, hay diversas cuestiones que deben tenerse particularmente en cuenta a la hora de trabajar remotamente; temas que suelen ser habituales o estar resueltos en el ámbito de la oficina. Una de estas cuestiones es el tema del soporte o asistencia a la hora de solucionar un problema técnico.

A diferencia del soporte en sitio, donde suele ser más ágil y sencillo resolver un problema ya que se tiene acceso directo al equipo, el soporte remoto suele traer algunas dificultades y riesgos que el trabajador debe tener en cuenta.

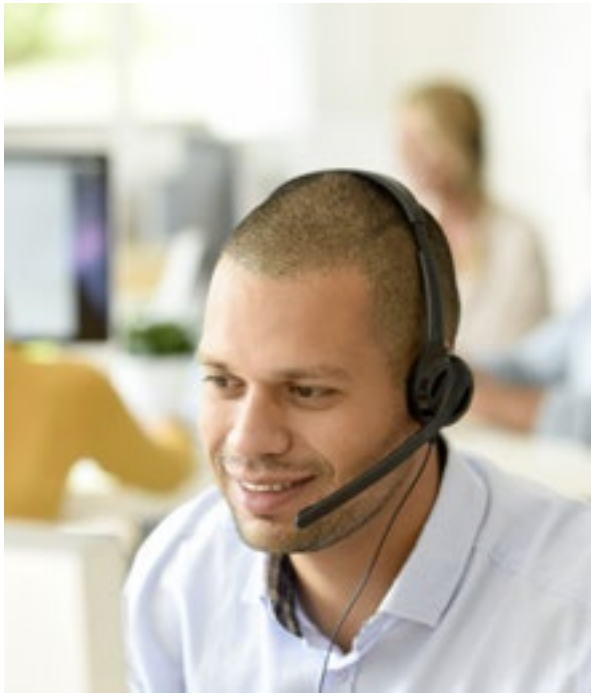
Por un lado, **contar con los contactos a donde recurrir al momento de reportar un problema** o solicitar asistencia. Es importante que estos siempre estén a mano y disponibles desde diversos dispositivos, de forma tal que, si uno de ellos no puede ser accedido, la información de contacto este igualmente disponible.

Esto aplica también para los contactos donde reportar un incidente de seguridad, como el robo o pérdida de un equipo, donde **es de suma importancia dar aviso lo antes posible** al empleador para que puedan ejecutarse los protocolos de seguridad correspondientes y evitar que la información sea comprometida.

Muchas empresas utilizan conexiones de control remoto de escritorios para que el técnico tenga acceso al equipo. Muchas de estas soluciones son públicas y gratuitas, por lo que pueden ser utilizadas por cualquier persona. También existen diferentes engaños que intentan hacer creer al usuario que tiene un problema en el equipo y requiere soporte, cuando no es verdad.

En todos los casos es importante **contactarse siempre con el soporte técnico autorizado del empleador** y asegurarse que es realmente él quien está accediendo al equipo y **evitar darle acceso a personas desconocidas o de dudosa reputación**. También es recomendable prestar atención a las acciones que el encargado de soporte ejecuta en el equipo, ya sea que se tengan o no conocimientos técnicos, debemos asegurarnos que no acceda en el proceso a información confidencial.

Dado que el soporte remoto puede no ser tan ágil o tenga algunas limitaciones, también es recomendable solicitarle a la empresa una guía de solución de problemas para los inconvenientes más comunes, de forma tal que podamos resolverlos proactivamente.



Buenas prácticas de seguridad

A la hora de trabajar de manera remota, la seguridad de la información queda, en gran medida, en manos del usuario. Para poder mitigar, entonces, los riesgos que esto implica y proteger la información, se deben seguir algunas buenas prácticas de seguridad.

- Cifrar la información alojada en los dispositivos móviles.
- Utilizar una solución de seguridad y mantenerla actualizada.
- Mantener todos los dispositivos actualizados, tanto el sistema operativo como las aplicaciones.
- Utilizar, en lo posible, redes Wi-Fi seguras y configurar de manera segura la red inalámbrica hogareña.
- Si se conecta a una red pública o compartida, utilizar siempre una VPN o evitar enviar información sensible.
- Realizar respaldos periódicos de la información.
- No dejar nunca el equipo desatendido y protegerlo con una contraseña.
- Contar con una protección antirrobo.
- Utilizar doble factor de autenticación para acceder a cuentas críticas.
- Tener siempre a mano los contactos de soporte y, si ocurre un incidente de seguridad, denunciarlo lo antes posible.
- Estar atento e informado acerca de nuevos engaños y amenazas.

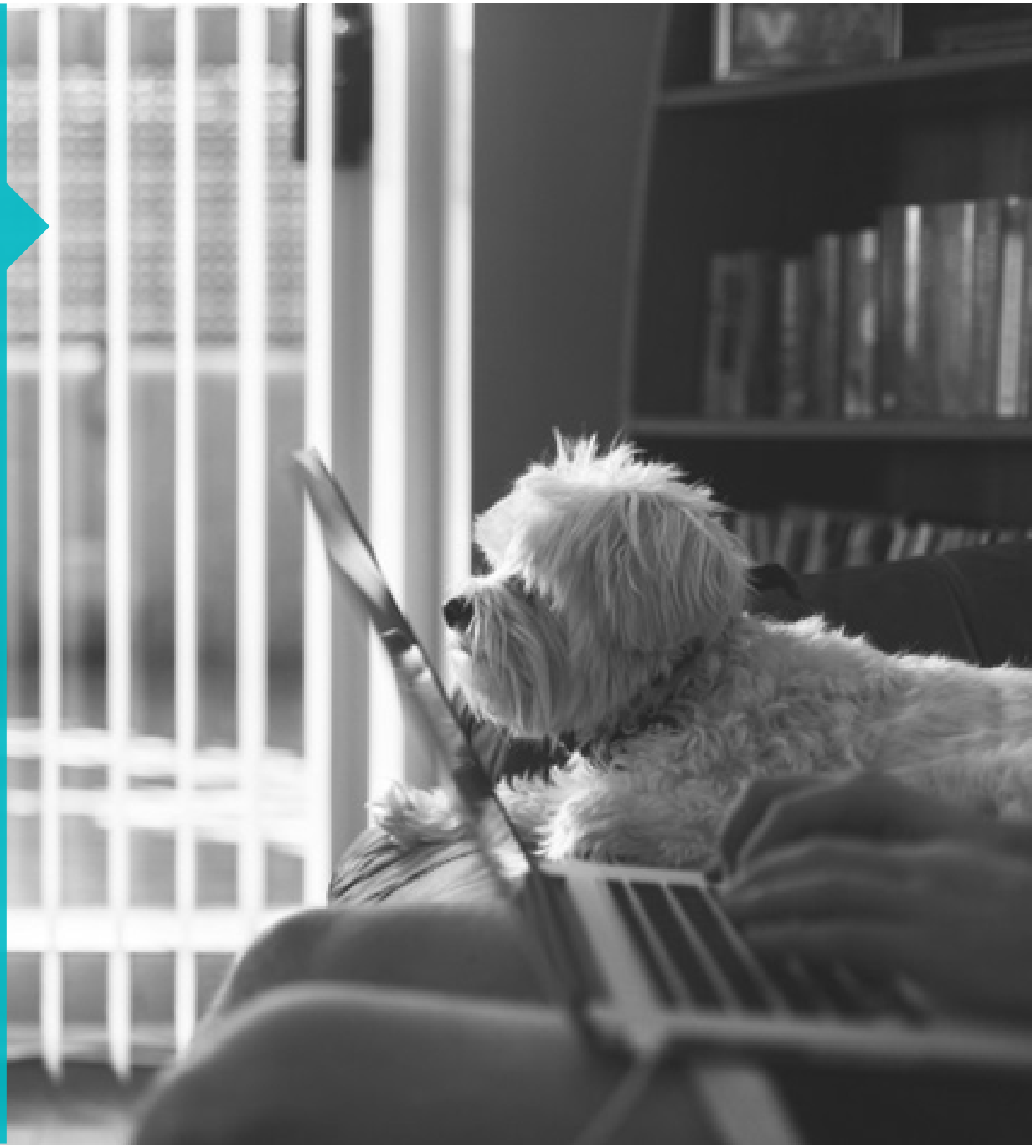
Conclusión

A lo largo de esta guía hemos repasado los riesgos que implica el trabajo remoto y cómo se debe cambiar la manera en que se gestiona la seguridad para garantizar que el acceso a la información se haga de manera segura.

Además, teniendo en cuenta nuevas tecnologías como 4G, Wi-Fi en aviones y otros avances en materia de conectividad, el teletrabajo y, en especial, el acceso remoto a la información, es sin duda una tendencia en aumento que cada vez más empresas pretenden implementar y que los empleados desean aprovechar.

En la medida en que las oportunidades y ventajas del teletrabajo se aprovechen de la mejor manera, el trabajador pasará a ser una pieza fundamental en la gestión para garantizar la seguridad de la información. Y para enfrentar los retos nuevos que pueden surgir, las organizaciones deberán contar con políticas claras para el manejo de la información y con herramientas adecuadas que les permitan a los colaboradores realizar sus actividades de manera segura.

Si bien el teletrabajo no es una opción viable para todas las empresas, e incluso en aquellas que decidan adoptarla quizá no puedan hacerlo para todas sus áreas, para cambiar la forma de trabajar en la compañía es importante que todos los involucrados se capaciten para conocer los riesgos y para saber cómo evitarlos y/o contrarrestarlos.



www.eset.com/latam

esetla esetla ESET Latinoamérica