
eset
ENJOY SAFER TECHNOLOGY™
PARA EMPRESAS
GUÍA DE
Teletrabajo

Introducción

El trabajo remoto o teletrabajo, es una modalidad en la cual el empleado puede realizar su actividad profesional fuera de la oficina. Si bien generalmente está asociado con el home office, no está limitado únicamente al hogar; puede ser también en oficinas compartidas o cualquier espacio diferente al de la empresa. Asimismo, en la mayoría de casos no hay horarios definidos, sino tareas u objetivos a cumplir.

Sin lugar a duda, esta metodología ha tomado gran fuerza debido al crecimiento y las posibilidades que brinda Internet, especialmente en cuanto al desarrollo de nuevas tecnologías de la comunicación integradas en sistemas alojados en la nube.

Además, el teletrabajo entre algunas de sus ventajas, reduce los costos operativos. Esto se debe a que la portabilidad tecnológica permite que los empleados sean igualmente productivos dentro o fuera de la oficina.

Esta modalidad obliga a que las empresas contemplen diversos panoramas, como la manipulación de información laboral en dispositivos que pueden no estar protegidos adecuadamente o el acceso remoto a información sensible. Estos casos, entre muchos otros, hacen que las organizaciones se planteen formas diferentes de gestionar la seguridad para minimizar los riesgos asociados con un ataque a la información más crítica.

Índice

Cambios de paradigma en la gestión

Sin lugar a dudas, esta modalidad de trabajo no solo implica un cambio para el trabajador; también lo hace para los empleadores, quienes deben considerar cuestiones que van desde dónde accede el empleado a la información, hasta la forma en la que ingresa a los sistemas.

Por esta razón, todo lo que está relacionado con los equipos de trabajo, la responsabilidad y los costos deben estar definidos claramente antes de implementar un formato de teletrabajo.

Lo más habitual es que el empleador proporcione y mantenga los equipos necesarios para el teletrabajo regular, sin embargo, también puede darse el caso en donde el empleado utilice su propio equipo.

Independiente del modelo elegido, la empresa debe considerar proporcionarle al empleado un soporte técnico adecuado para que pueda desarrollar su trabajo sin problemas.

En este sentido, la empresa deberá prestar mucha más atención a la forma en la que sus empleados se conectan a las redes corporativas y públicas para manipular la información, en detrimento de la preocupación que antes se tenía por la infraestructura física. La adopción de metodologías de teletrabajo, implica un cambio en la forma de gestionar la seguridad de la información en una amplia variedad de dispositivos, aplicaciones y sistemas operativos.

Esta modalidad de trabajo no solo implica un cambio para el trabajador; también lo hace para los empleadores, quienes deben considerar desde dónde accede el empleado a la información, y la forma en la que ingresa a los sistemas.

Retos y oportunidades

Sin lugar a dudas, el teletrabajo plantea oportunidades para aumentar la productividad debido a la implantación del trabajo por objetivos con menos costos al disminuir la infraestructura necesaria, y utilizando nuevas tecnologías que agilicen las labores de los empleados.

Pero esta metodología también conlleva retos y riesgos que se deben contemplar para implementar las medidas de control adecuadas, ya que de no tenerlos, se podría estar abriendo la puerta a fugas de información, infecciones con códigos maliciosos o accesos no autorizados a información privilegiada.

Más allá de pensar en los beneficios económicos y operativos, las compañías deben contemplar los comportamientos y equipos de todo el staff de colaboradores para tomar las medidas de control adecuadas y, así, asegura que la información permanezca protegida.

Más allá del perímetro

Al permitir que los empleados accedan y manipulen información por fuera del entorno corporativo, se amplía la frontera de implicancias en seguridad. Por lo tanto, para gestionarla se debe ir más allá del perímetro tradicional, que solía extenderse hasta los firewall en la empresa.

Pensar en amenazas informáticas en este nuevo contexto, lleva a contemplar otro tipo de riesgos que en un entorno por fuera del corporativo tienen una probabilidad más alta de ocurrencia. Por ende, se deben identificar las vulnerabilidades que se generan y las amenazas que pueden aprovecharlas.

Veamos algunas de las que deberían considerarse:

VULNERABILIDADES	AMENAZAS
Contraseñas débiles	Pérdida de dispositivos
Ausencia de soluciones de seguridad	Infección con códigos maliciosos
Conexión desde redes inseguras	Ejecución de exploits
Dispositivos con la información sin cifrar	Daño de los equipos
Falta de respaldos de la información	Engaños basados en ingeniería social
Falta de actualización de sistemas y dispositivos	

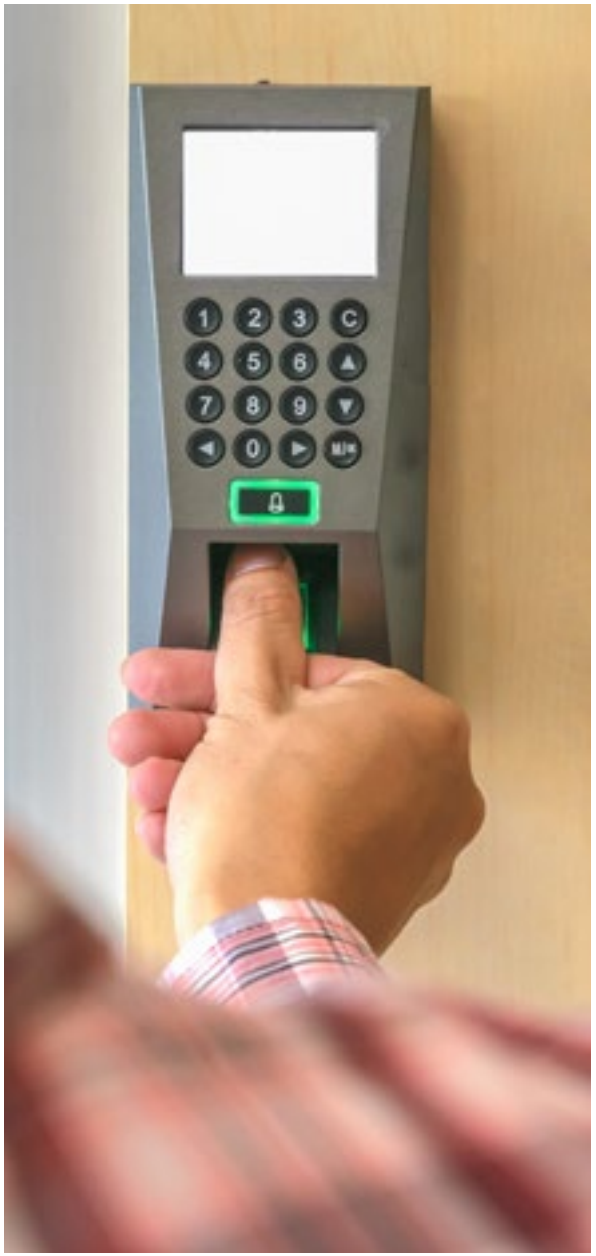
Gestionar los riesgos

La gestión de riesgos debe enfocarse en implementar los controles adecuados para corregir las vulnerabilidades o evitar la ocurrencia de un incidente.

El primer paso que debe dar una empresa antes de implementar una política de este tipo es la clasificación de la información con el objetivo de establecer, por ejemplo, cuáles son los datos sensibles que requieren mayores niveles de protección; a qué información se puede acceder desde dispositivos personales; a cuál por fuera de la red de la empresa; y a cuál debe restringirse el acceso total.

Si la empresa tiene claro este punto de partida puede determinar cuáles son los riesgos que tengan una mayor probabilidad de ocurrencia o que pueden tener más impacto, y a partir de esto determinar las medidas de control más adecuadas para garantizar la seguridad de la información, ya sean de tipo tecnológico como de gestión.

La empresa primero debe clasificar la información para establecer qué datos deben ser de fácil acceso y cuáles deben tener mayores niveles de protección.



Por dónde empezar a identificar riesgos

Accesos a información sensible desde entornos no confiables

Es necesario considerar el panorama en el cual el empleado acceda a los sistemas corporativos desde redes Wi-Fi públicas o desde equipos que no estén protegidos adecuadamente.

Permisos de los usuarios en el sistema

Si el empleado trabaja desde su propia computadora, puede hacerlo desde un perfil como administrador. Por lo tanto, no es posible controlar qué se instala o qué usos adicionales se le dan al dispositivo.

Equipo corporativo para uso personal

Cuando la empresa asigna un equipo al empleado para hacer teletrabajo, lo puede utilizar, además, para realizar actividades personales, por lo tanto hay que considerar este tipo de uso y los inconvenientes que podría tener para la información corporativa del equipo y su respectivo acceso a las redes de la empresa.

Respaldo de información

Las actividades de backup de información importante puede complicarse si no se contempla que muchos de los datos usados por el empleado pueden estar alojados localmente, es decir, por fuera de las tareas de respaldo. Esto es especialmente problemático si el equipo no se encuentra conectado a las redes correspondientes en el periodo programado.

Sistemas de autenticación débiles

Dejar únicamente la autenticación a sistemas de la empresa con una contraseña es la opción menos recomendada. Es importante pensar en otros medios de autenticación adicionales que agreguen más capas de protección.

Falta de políticas de seguridad

Tanto el empleado como la empresa deben saber claramente qué pueden hacer y cómo deben hacerlo. Si esto no está claro, se convierte en un eslabón débil de la cadena de seguridad.

Control de datos corporativos y virtualización

Una de las mejores alternativas que tienen las empresas para aplicar un esquema de teletrabajo es la virtualización de sus entornos. Con este enfoque se obtiene un mayor control de los datos más sensibles de cada organización y se eliminan los riesgos asociados al uso de un dispositivo propio del empleado al manejar la información de la empresa.

Al virtualizar el entorno de trabajo, se logra que el usuario pueda hacer sus actividades desde una ubicación remota en un ambiente al que se le pueden agregar más medidas de control. De esta manera, tanto las aplicaciones, como la información que se maneja a través de estas, están bajo el control de la empresa. Incluso los archivos permanecen dentro de los servidores corporativos y en ningún momento pasan al dispositivo desde el que accede el usuario.

No es un método infalible, pero sí se logra agregar un nivel adicional de protección al limitar que la información se procese directamente en el dispositivo del empleado. Obviamente esto debe estar acompañado de los controles apropiados para evitar una posible fuga de datos.

Continuidad del negocio

Cuando todos los empleados se encuentran en una misma oficina, la empresa suele tener un plan para recuperar las operaciones en caso de un incidente. Del mismo modo, se debe contar con este plan cuando se implementa el teletrabajo y los empleados están fuera de la compañía.

No obstante, al contar con un esquema de trabajo remoto, es decir, con equipos por fuera de la infraestructura comprometida, el proceso de restauración se torna más eficaz para garantizar la continuidad del negocio; esto se debe a que solo hay que focalizar los esfuerzos en la infraestructura más crítica.

En el mismo contexto, es ideal contar con los sistemas virtualizados, ya que permitiría descentralizarlos en diferentes proveedores y, así, reducir el impacto de un posible incidente. De esta manera, si ocurriera un incidente que afectara la continuidad de las operaciones -como una falla eléctrica en las oficinas o un ataque que comprometiera el acceso a Internet-, aquellos que estén conectados por fuera no van a verse perjudicados y podrán seguir con sus actividades. En el caso de que el incidente afectara el dispositivo físico de un empleado, este podrá utilizar otro para acceder al entorno virtualizado y continuar con sus actividades.

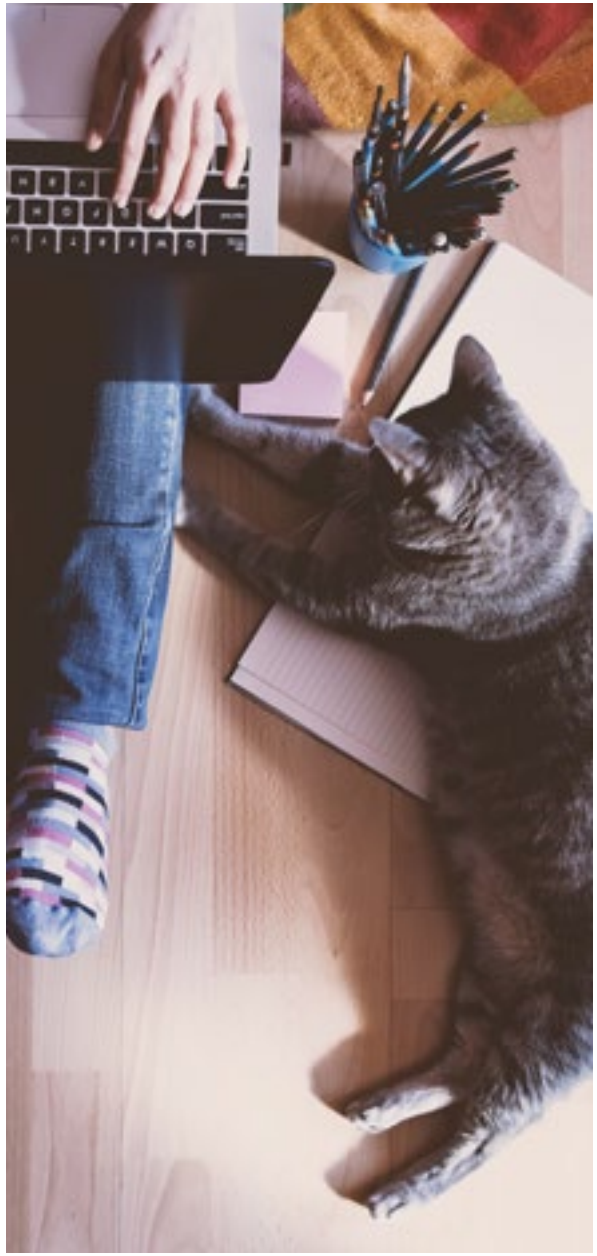
Mas allá del contrato laboral

Si el empleado manipula información de la empresa en su dispositivo personal, debe estar claro qué pasará con ella una vez terminada la relación contractual, ya que es difícil saber a ciencia cierta que la información será eliminada.

Si bien la empresa puede proveer los equipos para que el empleado realice su trabajo, y de esta manera recuperarlo al final de la relación contractual, el riesgo de fuga de información sigue siendo bastante amplio. Contar con los datos en repositorios administrados por la empresa y cuidar los permisos de acceso y modificación reducen la posibilidad de una fuga.

Asimismo, otras acciones de control pueden apoyarse en aspectos contractuales, como la firma de acuerdos de confidencialidad o medidas más estrictas en relación al tipo de información que se pueda descargar y almacenar en dichos equipos.

Se debe hablar previamente con el empleado sobre la manipulación de la información de la empresa, ya sea que trabaje con su dispositivo personal, como con uno provisto por la empresa.



7 pilares de seguridad

1 GESTIONAR ROLES

Es vital cerciorarse de que el acceso a la información esté permitido únicamente para aquellos roles que realmente estén habilitados para ello.

Para esto en la empresa se deben establecer las responsabilidades de acuerdo a los objetivos planteados tanto para los empleados como para aquellos involucrados en la gestión. Aspectos como el control de las tecnologías, la realización de copias de seguridad, contar con procesos de recuperación, entre otros, son algunas de las tareas que deben tener un ejecutor y momento definido.

Asimismo, aquellos empleados que estén directamente involucrados en las actividades de teletrabajo, deben estar al tanto de las políticas y, además, tener asignados los permisos necesarios para llevar a cabo sus tareas, puesto que dejar perfiles por defecto, sin control o sin políticas de acceso pueden generar problemas de seguridad.

2 CONTROL DE DISPOSITIVOS

Teniendo en cuenta la amplia variedad de dispositivos en el mercado, es importante restringir el acceso solamente a aquellos en los cuales se aplicar las herramientas de seguridad adecuadas.

En este sentido, no es lo mismo que un empleado acceda desde su computadora personal con un sistema operativo actualizado y con una solución de seguridad instalada, a que lo haga desde una tablet desactualizada, sin protección y que utiliza el hijo de esta persona para jugar y descargar aplicaciones.

Por lo tanto, se debe contemplar desde qué tipo de dispositivos y con qué características se va a permitir acceder a la información de la empresa.

3 PROTEGER CONTRA CÓDIGOS MALICIOSOS

Para garantizar que ningún código malicioso afecte los datos, todos los dispositivos utilizados por el empleado deben contar con soluciones de seguridad que detecten proactivamente este tipo de amenazas.

Si el dispositivo desde el cual accede el empleado no es propiedad de la empresa y, además, no se utilizan entornos virtualizados, los riesgos de sufrir una infección con códigos maliciosos son más altos. La misma condición aplica para dispositivos móviles.

Además de una solución de seguridad, es necesario que la computadora o dispositivo móvil tenga todas las aplicaciones actualizadas. Por lo tanto, la política de actualización debe ser clara para no dar lugar a brechas de seguridad.

4 MONITOREAR EL TRÁFICO DE RED

Dado que hay dispositivos que están ingresando a la red por fuera del perímetro físico de la oficina, es necesario hacer un seguimiento de qué tipo de tráfico generan. Por ejemplo, dónde tratan de acceder, si hay intentos recurrentes y fallidos de ingreso a servidores o si, incluso, generan algún tipo de tráfico inapropiado, como la descarga de archivos desconocidos.

Otro aspecto importante, es la posibilidad de hacer bitácoras de tráfico que permitan verificar el comportamiento de la red cuando se hace algún cambio, ya sea la inclusión de una nueva tecnología o algún servicio, logrando determinar el uso que hacen los usuarios que están por fuera de la red.

5 CONEXIONES SEGURAS

Una VPN (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

Al momento de implementarla, la empresa tiene una mayor certeza de que cuando sus empleados quieran acceder a recursos corporativos desde sus casas, un hotel o un restaurante lo puedan hacer de forma segura.

Para estos casos de teletrabajo, la implementación de conexiones VPN basadas en el cliente es lo más conveniente, ya que este tipo de redes permiten tener conectado un usuario a una red remota, a través de una aplicación que se encarga de entablar la comunicación y levantar la VPN.

Para acceder a la conexión segura, el usuario debe ejecutar la aplicación y autenticarse con un nombre de usuario y contraseña, e incluso agregando un segundo factor de autenticación. De esta manera se crea el canal cifrado entre el equipo y la red remota, para un intercambio seguro de datos.

6 REDACTAR UNA POLÍTICA DE SEGURIDAD

En la política de seguridad se deben declarar las intenciones respecto a la seguridad de los recursos informáticos, y a partir de ella sentar las bases para determinar las obligaciones y responsabilidades de los usuarios respecto al uso de las tecnologías que tienen a su disposición.

Por lo tanto, esta política debe definir el tipo de acciones que se pueden hacer y quién está habilitado a ejecutarlas. No es lo mismo tratar de modificar una base de datos por parte de un usuario que está por fuera de empresa, a que pueda hacer consultas e informes.

Cada política es propia de la realidad de la organización y del alcance establecido para los empleados que hacen parte del teletrabajo. No obstante, se debe partir de un reconocimiento de los activos de información, ya que no se puede controlar aquello de lo cual no se conoce su estado.

7 CONCIENTIZAR A LOS EMPLEADOS

La educación debe ser un pilar importante para que todos los usuarios sean conscientes de los riesgos a los cuales pueden verse expuestos y cuáles son los cuidados que deben tener al ingresar dispositivos ajenos a la compañía.

Si el usuario no conoce los riesgos a los cuales expone la información de la empresa, e incluso la propia, puede ser víctima con más facilidad de muchas amenazas. El empleado debe entender que así esté por fuera de la oficina, el dispositivo desde el cual trabaja es una puerta a toda la organización y como tal debe garantizar un uso adecuado.

Evaluación y mejora continua

La mejora continua es un concepto que viene de los sistemas de gestión, y que para el caso de implementaciones importantes, como la del teletrabajo, es crucial no perder de vista. Por lo tanto, se debe evaluar y medir la forma en que se van desarrollando las actividades de quienes trabajan remotamente contra la política y los objetivos de seguridad, e informar los resultados.

Es a partir de esta información que se pueden implementar los cambios requeridos para la mejora de los procesos. Para que estas actividades sean exitosas es necesario hacer un monitoreo del uso de los activos de información para detectar cambios en los posibles riesgos que pudieran materializarse.

Por ejemplo, cada vez que se hace un cambio en la infraestructura más crítica o cuando se cambia alguna política de seguridad, es importante verificar que todos realicen sus actividades acorde a dichos cambios. La aparición de una nueva vulnerabilidad o la desactualización de alguna de las herramientas utilizadas para conectarse de forma remota pueden ser utilizadas por atacantes para llegar a información sensible.

No basta con implementar un programa de teletrabajo de forma exitosa, la clave para que realmente se pueda aprovechar y genere los beneficios esperados es que se haga un seguimiento de cómo ha sido implementada.

Conclusión

La adopción de una metodología de teletrabajo puede traer grandes beneficios relacionados con la disminución de gastos en infraestructura, la comodidad de los empleados para el manejo de la información y, por tanto, el incremento de la productividad; no obstante, la empresa enfrenta nuevas amenazas que deben ser gestionadas. Principalmente, se trata de las fugas de información y los accesos no autorizados a la misma. Para enfrentar estos retos, las organizaciones deben realizar una combinación entre políticas claras para el manejo de la información y el uso de herramientas adecuadas que permitan la gestión de la seguridad de la misma. Asimismo, no hay que dejar de lado la educación de los empleados para que conozcan los riesgos y sepan cómo enfrentarlos.

El acceso a información corporativa por parte de personas ajenas a la empresa y la consecuente fuga de la misma, muchas veces, deja secuelas económicas para recuperar o reparar los daños causados. En este sentido, barreras de prevención como programas de cifrado, contraseñas y cortafuegos contra ataques desde la red pueden evitar más de un dolor de cabeza.

El teletrabajo no es una opción viable para todas las empresas, e incluso si una decide adoptarlo quizá no pueda hacerlo para todas sus áreas. Para cambiar la forma de trabajar en la compañía, es importante realizar una buena planificación y que la implantación sea progresiva, evaluando los resultados obtenidos.

La mejora continua del proceso, la implementación de controles de seguridad y la concientización a los empleados va a ser fundamental para que se pueda tener un ambiente seguro de trabajo. De esta manera, la organización podrá contar con un entorno lo suficientemente robusto conociendo el tipo de dispositivos que se pueden conectar, y con métodos de acceso seguros y definidos, independientemente del enfoque (físico o virtual) por el que haya optado.

Después de todo, para poder estar alineado con el avance de la tecnología es necesario concentrarse en la gestión de la seguridad de la información, más que en la seguridad de la infraestructura, y el teletrabajo es un gran ejemplo de estas prácticas.

www.eset.com/latam

esetla esetla ESET Latinoamérica