La transición hacia el TELETRABAJO

A partir de la situación por todos padecida, las actividades diarias de las distintas empresas han sido redirigidas inesperadamente al teletrabajo como respuesta a una emergencia no planificada. Fue desordenado, confuso, y diría: "caótico". Con muchos cambios ocurriendo a la vez, la *seguridad* del teletrabajo ha sido una ocurrencia tardía o completamente pasada por alto.

Asimismo, teniendo en cuenta lo que significa técnicamente implementar el teletrabajo, tener comunicaciones eficientes, personal preparado, equipamiento y aplicaciones adicionales, se suma el aspecto legal el cual debe ser considerado, ante todo. En nuestro país hace muchos años se ha definido cierta normativa la cual se encuentra vigente como indica la página www.argentina.gov.ar

"*no contamos con un instrumento jurídico específicamente redactado para el teletrabajo sino con un conjunto de leyes que engloban la actividad: la Ley de Contrato de Trabajo (LCT Ley 20.744 del año 1976) es la principal normativa y junto con la Ley N°25.800, que ratifica el Convenio N°177 sobre trabajo a domicilio de la OIT, la cual promueve la igualdad de condición de este tipo de trabajadores con respecto a los presenciales.* Ambas reglamentaciones cubren la actividad correspondiente a los trabajadores contratados en relación de dependencia, englobando al teletrabajo, sin mencionarlo taxativamente, sin definirlo, ni reglamentarlo puntualmente.

(Cabe aclarar que, durante la generación de este documento, el Congreso Nacional está presentando proyectos específicos para legislar el teletrabajo)

Las resoluciones publicadas hasta la fecha son las siguientes:
Resolución 1552/2012 de la Superintendencia de Riesgos del trabajo
Medidas a aplicar para el Teletrabajo
http://servicios.infoleg.gob.ar/infolegInternet/anexos/200000-204999/204726/norma.htm
Resolución 595/2013 del Ministerio de Trabajo, empleo y seguridad social.
Programa de Promoción del Empleo en Teletrabajo
http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/217070/norma.htm
Resolución 21/2020 del Ministerio de Trabajo, empleo y seguridad social y Superintendencia de Riesgos del trabajo.
Informar a la ART la nómina de trabajadores que efectúan teletrabajo, para considerar el domicilio como ámbito laboral
http://servicios.infoleg.gob.ar/infolegInternet/anexos/335000-339999/335553/norma.htm

Ventajas y desventajas:

A partir de esta coyuntura forzada, se han observado algunas ventajas como también desventajas, las cuales intentamos enumerar.
Las ventajas y desventajas están divididas a su vez entre el empleado y el empleador.
Dentro de las ventajas para el empleador, hay ventajas directas y ventajas indirectas.

EMPLEADOR

Para la empresa, se han verificado algunas **ventajas** *directas* como, por ejemplo: que ha bajado el consumo de electricidad, consumo de agua (independientemente de lo que facturan las empresas distribuidoras de energía que *estiman* el consumo y no leen los medidores respectivos, por ahora), ahorro en la limpieza de los locales, y una baja en el consumo de llamadas telefónicas.
Y como **ventajas** *indirectas*, la reducción de personal de seguridad en algunos locales internos, el riesgo de traslado de personal, como así también la reducción de materiales de librería.
¿Porque aseveramos estas ventajas directas e indirectas?, es que ha cambiado la manera de trabajar, de modo que se han agilizado algunas actividades como las comunicaciones que se efectúan por WhatsApp, o Skype o Zoom, por medios virtuales, por correos. La documentación se gestiona digitalmente.

En cuanto a las **desventajas**

Respecto de la **información procesada:** si no se aplican medidas de seguridad y estándares de resguardo de la información, queda a disposición de la habilidad del empleado gestionarla en forma segura, de acuerdo a su criterio o a las indicaciones que reciba de su empleador.

Para el **equipamiento utilizado**, si no es provisto y limitado desde el punto de vista de seguridad al empleado, en general es utilizado para las tareas de la empresa como así también para uso familiar. Esto genera un riesgo alto en lo que se refiere a la seguridad.

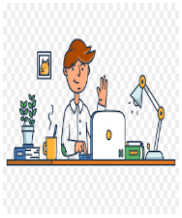
Considerando el **conocimiento por aproximación**, es intangible en cuanto a las empresas debido a que el empleado estando en su lugar de trabajo, comparte las actividades que realizan en conjunto y al generarse nuevas actividades, éstas se difunden en su ambiente laboral. Con el sólo hecho de informarlo grupalmente en forma presencial, se transfiere el conocimiento, consulta y las dudas, se pueden resolver rápidamente. Estando trabajando remotamente esta función intangible no se puede realizar.

Genera dudas respecto de la **Validación de gastos registrados**, requiere controles muy fuertes en los sistemas que gestiona la empresa y además confianza en sus empleados.

Es difícil verificar que el equipamiento y aplicaciones instaladas sean utilizadas como **recursos de terceros**, es decir, la utilización de dichos recursos para otras empresas, siendo que esto es difícil de disimular o esconder cuando se encuentra el empleado trabajando en la instalación de la empresa.

Las ventajas enumeradas son en general económicas, no obstante, las desventajas están asociadas a riesgos que generalmente nunca fueron evaluados. Las desventajas deben ser necesariamente analizadas, y en todo caso asumir el riesgo en función de la operatividad y continuidad de la empresa. No obstante, es posible y conveniente desarrollar controles que permitan minimizar dichos riesgos.

EMPLEADOS



En el caso del empleado podemos enumerar ventajas y desventajas, las cuales son muy diferentes a las de la empresa. Se debe tener en cuenta que es muy dependiente de la relación laboral, el tipo de función, la necesidad de compartir información entre la empresa y el empleado.
La diferencia sustancial consiste en la manera en que las tareas que realiza el empleado, podrían clasificarse de la siguiente manera:

- Cumplimiento de objetivos
- Tareas de recopilación/gestión de información (administrativa)
- Atención clientes

Ventajas 

Dependiendo de la relación laboral una de las ventajas que podremos considerar es el **Horario Flexible**. Esto es posible en el caso de recopilación de información o trabajo por objetivos, donde el horario no es necesario que sea el mismo para todos los empleados, sino que debe cumplirse con la tarea asignada para una fecha acordada.

Ahorro importante en lo que se refiere a **traslados y desplazamiento**. El empleado al trabajar desde su casa, ahorra en viajes y gastos adicionales en el itinerario.

Ahorro en **gastos adicionales**, comidas, compras adicionales en barrios más caros. En general, se realizan compras en horarios de almuerzo de algunos ítems que al llegar al hogar ya no pueden hacerlo.

Desventajas 

Se ha detectado durante este período especial que el empleado ha encontrado algunas desventajas del trabajo desde su domicilio

No ha logrado mantener un equilibrio en la **cantidad de horas trabajadas**. En general, al no ser disciplinando en torno a sus horarios laborales, en definitiva, siente que trabaja más de lo previsto. En particular, no aplica pausas que son necesarias para un trabajo eficiente.

No encuentra un **lugar adecuado en su hogar** que le resulte confortable, o que no tenga interrupciones del tipo familiar. Es necesario habilitar espacios de trabajo y le es imposible

Se **dispersa más frecuente** en redes sociales, noticias, llamadas y no puede **concentrarse** y abstraerse en el trabajo asignado.

Se siente más controlado, más **exigido por parte de su jefe**, el cual lo llama más frecuentemente y consulta en más ocasiones que cuando trabaja en su oficina.

No puede lograr que sus **familiares utilicen su equipamiento**, dado que probablemente sea más actualizado y moderno que el que se utilizaba en el hogar antes de trabajar remotamente.

Pareciera ser que en muchos casos los empleados encuentran muchas desventajas al trabajar desde su domicilio. El reto entre su vida laboral versus su vida personal parece estar en conflicto. No obstante, esta situación es posible remediarla acordando con los empleados cada una de las problemáticas relacionadas al confort laboral.

¿Y la Seguridad en la implementación de teletrabajo?:

Su empresa podría exponerse a un mayor riesgo considerando que los atacantes, que muchas veces parecían lejanos, ahora se perciben *muy cerca*.
Estos personajes siempre están buscando oportunidades para aprovechar la interrupción en general y las prácticas de seguridad débiles y vulnerables específicamente, que son frecuentes en cualquier instalación que, en general nunca habían estado tan expuestas a amenazas. Ellos se ven muy confiados en que su táctica puede ser muy efectiva y especialmente disimulada en la situación actual.
Pero la pregunta es ¿Cuál es el problema? Y su respuesta es: En las casas de los empleados hay un gran déficit de seguridad como probablemente también exista en su empresa. En general, se protege el acceso físico a una oficina o domicilio, mucho más que el acceso a la red de internet. En una oficina o domicilio, colocamos llaves de protección, puertas blindadas y hasta una persona de custodia. En cambio, cuando accedemos a internet no conocemos si las páginas son seguras o son las que corresponden a mi búsqueda. Los atacantes buscan parónimos en los nombres de páginas de modo de confundir al usuario cuando accede por ejemplo a la página de un banco cambiando una letra de su nombre lo cual se hace imperceptible, siendo que la página se copia de la original, es allí donde toman los datos de identificación del usuario para realizar un fraude. El empleado en muchos casos comparte los dispositivos con los integrantes de la familia, con lo cual no tenemos certezas de cómo se comportan, cómo los utilizan, cuan atentos están a los archivos que descargan o las páginas que visitan. Esto supone un riesgo en el manejo de información valiosa del ámbito laboral a través de la plataforma del hogar, ya que facilita la tarea del cibercriminal. En muchos casos no hay ningún software de protección de malware o análisis de accesos.

Supongamos que la empresa posee medidas de seguridad para proteger su información, para lo cual informamos algunas cosas simples que puede hacer para mejorar la seguridad de su empleado. Los siguientes consejos se aplican a casi todas las situaciones, y son relevantes ya sea que esté utilizando la computadora portátil o el teléfono inteligente que proporciona su empresa, o la propia computadora de escritorio o tableta del personal.

- Dispositivo dedicado: si es posible otorgar al empleado un dispositivo en el cual no tenga privilegios de administrador (de modo que no pueda instalar software adicional) y que pueda ser reparados sus inconvenientes en modo remoto.
- Generar una VPN (Red Privada Virtual) para que se conecte a la empresa con todas las medidas de seguridad que esto implica, es decir que no pueda acceder a privilegios que no necesite en sus tareas
- Preparar el dispositivo para que mantenga actualizado los parches que los softwares solicitan. En lo posible que actualice automáticamente.

- Proteger las comunicaciones asegurándose que la red este configurada adecuadamente y sobre todo que las contraseñas del dispositivo de Wifi sea una contraseña fuerte de modo que no pueda ser intrusada por un vecino o por atacantes. Si el dispositivo de comunicaciones es de terceros, colaborar con el empleado para comunicarse con el proveedor del servicio y comprobar los puntos anteriores
- Capacitar al empleado en cuanto a las prevenciones que debe aplicar y que en el anexo de este documento se sugieren enviar. Hacer actualizaciones permanentes sobre las alertas existentes como por ejemplo la aparición de un phishing que intente engañar al usuario invitándolo a acceder a una página porque su cuenta esta inhabilitada. Indicándole al empleado que si observa una actividad inusual o sospechosa en su dispositivo inmediatamente se ponga en contacto con la empresa

La ingeniería social es habitual para lograr el ingreso a la red de la empresa por medio del empleado obteniendo datos que les permita acceder. Intentan engañar para que haga algo o brinde información personal. Los estafadores y los delincuentes utilizan todos los eventos importantes para crear nuevos esquemas. Los atacantes tratarán de aprovechar este entorno cambiante. En general el engaño ingresa por medio de correos electrónicos de cuentas desconocidas con archivos adjuntos extraños, y en algunos casos dicen ser personal técnico y le piden sus contraseñas o le dicen que vaya a un sitio web para 'escanear' su computadora, si recibe solicitudes de reuniones web inusuales. Los atacantes siempre están buscando oportunidades para aprovechar las débiles prácticas de seguridad, también tratan de obtener información para acceder ofreciendo un regalo a cambio de datos.
Estamos aseverando que la mayoría de los ataques ingresan por ingeniería social.
SI, definitivamente la mayoría de los ataques comienzan en el ingreso de un atacante luego de que obtuvo información interna de la empresa.
En definitiva, si cualquier dispositivo que utiliza para el teletrabajo se ve comprometido, cualquier otra cosa conectada a la red doméstica de sus empleados también podría estar en riesgo y esto se podría trasladar a la empresa, por lo cual es un riesgo que traslada al manejo de información valiosa del ámbito laboral.

Esto riesgos pueden ser:

- La información puede ser usada para extorsionar a la empresa, al usuario o para vendérsela a la competencia
- pueden destruir o alterar datos valiosos, “secuestrarlos” (encriptarlos) y pedir recompensa o hacer caer remotamente el sistema
- pueden valerse de los datos para cometer otros delitos contra otras personas de la empresa
- pueden realizar fraudes y la utilización de credenciales, que son sin dudas las maniobras predilectas

Una de las recomendaciones más importantes y que son gratuitas es la capacitación de sus empleados y especialmente que reconozcan y comprendan el funcionamiento de un phishing

Para lo cual informe a su empleado que:

- Verifique la autenticidad del remitente, la dirección de correo no miente.
- Esté atento a que el saludo en el correo electrónico no sea genérico.
- Si el correo tuviera un enlace a una web, desplácese SIN HACER CLIC sobre él, ello permite corroborar si lo lleva al lugar donde promete.
- La mala gramática y el diseño son buenos indicios de la ilegitimidad del correo.

- No abra los archivos adjuntos incluidos en los correos electrónicos hasta que confirme que es legítimo.
- Nunca proporcione información personal o financiera requerida a través de un e-mail o un enlace de phishing contenido en él.

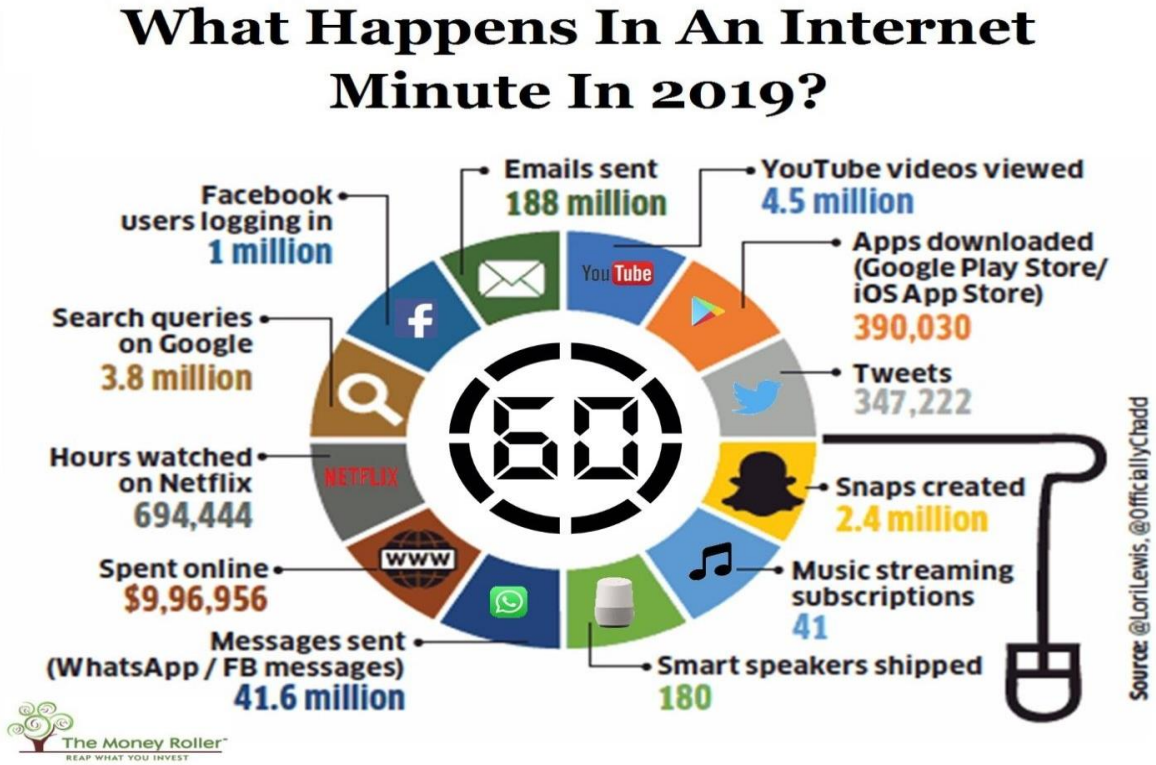
Cuando realice conferencias con sus empleados, tome los siguientes recaudos

- Elija aplicaciones con cifrado extremo a extremo (WhatsApp, Facetime, Google Meets, Skype, Microsoft Teams, Cisco Webex y Zoom -en su última versión- son algunos ejemplos).
- Sea cual sea la aplicación que utilice, descárguela del *sitio web oficial* o del *appstore*, **nunca de un enlace incluido en un mail o un banner de publicidad.**
- Cree sesiones privadas y no publique la invitación en redes sociales o donde puedan verlas personas ajenas.

Conclusión

La tecnología es el cambio que estamos viviendo y que ha modificado nuestros hábitos tanto personales como laborales. Muchos perciben que ser más seguro tiene costo, seguramente es así, pero es la realidad que estamos viviendo y si nos subimos a esta realidad no será posible participar el futuro.

A modo de resumen de lo que pasa en el mundo digital, la siguiente figura nos refleja lo que sucede en el mundo digital cada 60 segundos en el mundo.



Nora Susana Alzúa CISM – CRISC

CCI, Industrial Cybersecurity Center | www.cci-es.org | @info_CCI