

Workplace



El teletrabajo, el internet y la protección de datos



Comité **Laboral y de
Recursos Humanos**
AmCham

Editorial



Waleska Sterkel | Directora Ejecutiva

Estimado lector,

Reciba una cordial bienvenida a la primera edición de nuestra revista Workplace este 2021. Sabemos que el año que recién termina nos ha dejado muchas lecciones aprendidas y es momento de continuar, ahora adaptados a una manera de vivir más virtual.

Es por eso que hemos dedicado esta primera edición de Workplace al teletrabajo, el internet y la protección de datos. Ahora que las interacciones las realizamos de manera digital, es importante tomar en consideración la información que se transmite por estas vías y saber cuál es la mejor manera de protegerla.

Agradecemos la participación de las siete plumas invitadas en esta edición, quienes abordan el tema central de la revista desde aristas como las brechas que nos deja el covid-19 en materia laboral, la continuidad de la transformación digital y la protección de datos.

¡Bienvenidos a la primera edición del año de Workplace, la revista legal-laboral de AmCham Guatemala!

Índice

Colaboradores

Licda. Mirla Tubac Montesdeoca

Manager, EY LAW, S.A | Co-presidente del Comité Laboral y SIYSO de AmCham

M.A. Oscar A. Pineda Chavarría

Socio, Molina Mencos, Pineda & Asociados
Co-presidente del Comité Laboral y SIYSO de AmCham

AmCham's President

Juan Pablo Carrasco de Groote

AmCham's Executive Director

Waleska Sterkel

Job Search Coordinator

Lucrecia Castañeda

Communications Coordinator

Brigitte Salazar

Layout & Design

Erwin Acajabón

Pág. Tema

4	El trabajo, el internet y la protección de datos
5	“Ley del teletrabajo” y las brechas que nos deja el covid-19 en materia laboral
6	La continuidad de la transformación digital y la protección de datos, dos prioridades para el 2021
7	Trabajo, internet y protección de datos: la combinación del futuro digital
10	Trabajo eficiente, productivo y seguro desde casa
11	La seguridad como norma en la nueva normalidad
13	Un año nuevo: ¿haremos cosas nuevas o cosas viejas?

Plumas invitadas

Evelyn Rebuli

Socia, especialista y encargada del área laboral

Giovanni Francisco Soto Santos

M.A. en Derecho de Trabajo y de la Seguridad Social y Magistrado Titular Vocal segundo de la sala quinta de Corte de Apelaciones del tribunal de lo contencioso Administrativo

Francisco Mancilla

Chief Tigo Business Officer

Roberto Marroquín

Gerente de país Microsoft Guatemala

Enrique Aguirre

Director general de 3M para Centroamérica y el Caribe

Lissette Barrios

ENERGUATE

Francisco Corzo

Director de SMART

Leadership Circle 2021





*DEJA EL HUMO ATRÁS.
MUY ATRÁS.*

IQOS es una mejor alternativa que calienta en lugar de quemar sin fuego, sin humo y sin cenizas.

Descubre más en [IQOS.com](https://www.iqos.com)



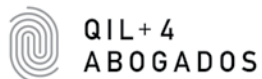
JUNTOS HACIA ADELANTE.

IQOS

Este producto es solo para fumadores adultos o usuarios adultos de IQOS. Este producto no es libre de riesgo y es adictivo.



El trabajo, el internet y la protección de datos



Por Evelyn Rebuli | Socia, especialista y encargada del área laboral

El internet y las redes sociales han venido a revolucionar la forma tradicional de trabajar. Con su implementación los empleadores y empleados se enfrentan a diario a nuevos retos y riesgos que es importante anticipar y evitar.

El uso de aparatos tecnológicos personales o como herramientas de trabajo traen nuevos riesgos que van a depender del uso que el empleado les dé. Uno de ellos es que se puede aumentar el riesgo de que la información confidencial pueda llegar a terceros.

En Guatemala existe poca regulación sobre estos temas. El patrono debe compensar tal ausencia con políticas y regulaciones claras, que tiendan a proteger su información y disminuyan los riesgos.

Hay muchas preguntas que nos podemos hacer, tales como ¿cómo puede una empresa proteger su información y que puede hacer para salvaguardarla? ¿Qué responsabilidad tiene un empleador en el manejo de la información personal de sus empleados? ¿El correo como herramienta de trabajo es propiedad del patrono o del trabajador?

Es indispensable entonces, que cada empresa se haga estos planteamientos y desarrollen políticas y lineamientos internos que sean ampliamente

comunicados a nivel interno en la empresa:

- Brindar o no equipo de cómputo al personal. Esto conlleva la necesidad de regular su uso, incluir limitaciones, comprobantes de entrega, valor del equipo, responsabilidad ante accidentes y daños, cuidados necesarios, instalación de programas, licencias, entre otros.
- Permitir el uso de equipo de cómputo personal para el trabajo o de dispositivos móviles personales para acceder al correo electrónico de la empresa. En ese caso es necesario regular el uso de claves para acceso al dispositivo. La propiedad de la información y el cuidado que debe tener el trabajador para evitar que llegue a terceros. El monitoreo del correo electrónico y la información contenida en el mismo. Uso personal e intransferible de claves y accesos. Responsabilidad por pérdidas del equipo y que la información pueda ser vista o usada por otros.
- Uso del nombre de la empresa, su marca o demás distintivos en redes sociales por parte de los trabajadores. Regulando los procesos o requisitos necesarios para ello.
- El manejo de la información de los

trabajadores para efectos del trabajo en forma interna o la contratación de terceros para la administración de planillas y files de personal. Si la información será administrada localmente o fuera del país. La autorización del personal para el uso de su información. Convenios de confidencialidad para uso de la información exclusivamente para efectos del trabajo.

- El uso de software ajeno al trabajo en los equipos.
- Uso del correo electrónico como herramienta de trabajo. Regular su uso, monitoreo de la información, limitaciones y responsabilidades.

El peor enemigo de una empresa en estos temas es hacer las cosas sobre la marcha, sin regulación y sin documentar la entrega del equipo, pues se abre la puerta a riesgos económicos, legales y de posibles conflictos con los trabajadores, clientes y terceros.

Entonces hay que prepararse, anticiparse y regular todo aquello para evitar riesgos innecesarios.



QIL+4
ABOGADOS

Diagonal 6. 10-01 Zona 10
Oficina 302 A. Torre II
Centro Genrecial Las Margaritas.
Guatemala, C.A.
(502) 2327-4646
(502) 205-9000
www.qil4.com



“Ley del teletrabajo” y las brechas que nos deja el covid-19 en materia laboral

Por Giovanni Francisco Soto Santos | M.A. en Derecho de Trabajo y de la Seguridad Social y Magistrado Titular Vocal segundo de la sala quinta de Corte de Apelaciones del tribunal de lo contencioso Administrativo

Intrínsecamente, el ser humano lleva consigo la responsabilidad de realizar alguna actividad para cubrir sus necesidades. En la actualidad, cuenta con herramientas tecnológicas que le facilitan la labor, pero con la llegada de estas herramientas, también ha surgido la necesidad de regular las formas de trabajo que a través de ellas se realiza. La manera de vivir como la conocíamos ha variado a nivel mundial como consecuencia de la pandemia y el trabajo no ha sido la excepción; hoy quiero compartirles mi opinión desde un enfoque judicial.

El Organismo Judicial, es el encargado de garantizar la certeza jurídica, el estado de derecho, el debido proceso y una justicia rápida y cumplida, además de ser el encargado de proteger, entre otras cosas, los derechos tanto de los empleadores como de los trabajadores.

Actualmente, es importante disponer no solo de la Constitución Política de la República, que contempla derechos laborales, sino de los convenios internacionales ratificados por Guatemala ante la OIT y de otras leyes específicas que permitan que todos los actores del quehacer laboral, puedan desarrollar sus actividades dentro del marco de la ley, buscando la mejora continua para la partes involucradas, modernizar la organización del trabajo, con el objetivo de mejorar la productividad y la competitividad de las empresas y lograr el equilibrio necesario entre flexibilidad y seguridad de los datos sin importar si el trabajo se realiza de manera presencial, virtual, dentro o

fuera de su sede laboral, siempre y cuando el esfuerzo institucional esté orientado al cumplimiento de las responsabilidades encomendadas.

Desde el punto de vista judicial, son necesarios cambios y/o reformas a las leyes, para que tanto jueces como magistrados puedan resolver de acuerdo con la realidad actual. Tal es el caso de las iniciativas de ley presentadas ante el Congreso de la República, 5764 y 5781 “Ley del Teletrabajo”, las cuales ya se encuentran con dictamen favorable y tienen como objetivo, promover y regular el teletrabajo como una modalidad laboral que estimule la generación de empleo y la modernización de las relaciones empleador-trabajador, a través de la utilización de las tecnologías de la información y comunicación que sean aplicables tanto en el sector público como en el sector privado, contando con una normativa legal que garantice la protección de los datos utilizados y procesados por el teletrabajador para fines profesionales.

La pandemia ha causado grandes daños a la industria y al comercio en general, lo que ha obligado a realizar adaptaciones en los antiguos modelos de trabajo. Es importante, resaltar que los procesos judiciales con relación al teletrabajo o trabajo en casa que han surgido en estos últimos meses, no ha variado la forma en que se llevan a cabo; los casos más comunes presentados ante las autoridades correspondientes son por despidos, reducción de salarios y por supuesto, por modificaciones en las

modalidades y condiciones de trabajo con cuales los trabajadores no han estado de acuerdo y esto ha provocado la saturación de los juzgados laborales y como consecuencia, la de las Salas Laborales de la Corte de Apelaciones.

De acuerdo con mi experiencia, considero que la brecha más relevante que ha causado toda esta transformación es que ha obligado en la administración del trabajo al (MINTRAB) y a las otras instituciones encargadas de regular el tema laboral, a contar con mecanismos que van surgiendo de acuerdo con las necesidades que se van presentando en cada uno de los casos por conflictos entre empleador y trabajador; el reto de adaptarse hay que enfrentarlo diariamente y poder continuar garantizando los derechos de ambas partes.





La continuidad de la transformación digital y la protección de datos, dos prioridades para el 2021



Por Francisco Mancilla | Chief
Tigo Business Officer

Conforme la pandemia covid-19 avanza, las organizaciones de todos los tamaños continúan adaptándose a una realidad más digital y con nuevos riesgos cibernéticos. Empresas más digitales requieren de una estrategia sólida que proteja sus datos.

La transformación digital se convirtió en un pilar fundamental para hacer frente a la crisis actual, lo cual ha llevado a repensar los modelos de negocio de cientos de empresas. En una encuesta realizada por Fortune 500 a los CEOs de las empresas más grandes de Estados Unidos, muestra que el 75% tuvo que acelerar la transformación digital en su empresa.

Esta es una tendencia que permanecerá en el futuro, no por moda, pero sí por una cuestión de sobrevivencia empresarial. Los tres elementos clave a considerar en esta transformación y adaptación a una nueva realidad son las personas -clientes, colaboradores, proveedores-; la evaluación de los procesos de la cadena de valor desde la perspectiva del nuevo consumidor y sus nuevos hábitos; y las

herramientas tecnológicas.

Es así, como un entorno cada vez más virtual trae consigo desafíos ahora y a futuro, entre ellos, la agilización de los procesos internos, la mejora de la experiencia del cliente, la administración de la seguridad de los trabajadores remotos y la gestión de la productividad a distancia. Para superarlos, es crucial trabajar en un cambio de cultura organizacional y de pensamiento, y centrar las estrategias de negocio en el análisis y comprensión del cliente.

Sin duda, todo esto debe estar acompañado de una estrategia de ciberseguridad integral y holística que resguarde los datos, los sistemas y los equipos. De acuerdo con el informe de la plataforma Threat Intelligence Insider Latin America de Fortinet, Guatemala fue objetivo de 25 millones de intentos de ciberataque entre enero y junio del 2020.

Ante este escenario, la ciberseguridad ya no puede ser un tema solo de informática, sino que debe tener un rol más estratégico liderado por la alta gerencia. Como líderes debemos estar atentos a los cambios y adaptarnos rápidamente para no quedarnos atrás.



Fuente: Murray, A. (2020). Fortune 500 CEO survey: How are America's biggest companies dealing with the coronavirus pandemic? Fortune. <https://fortune.com/2020/05/14/fortune-500-ceo-survey-coronavirus-pandemic-predictions/>
Fortinet. (2020). Threat Intelligence Insider Latin America. <https://www.fortinetthreatinsiderlat.com/es/current/landing>



Trabajo, internet y protección de datos: la combinación del futuro digital



Por Roberto Marroquín, gerente de país Microsoft Guatemala

A medida que las organizaciones se enfrentan a los distintos escenarios impuestos por el COVID-19, se hace más claro que la tecnología continúa siendo uno de los elementos clave en el camino hacia la recuperación.

El mundo camina velozmente hacia un modelo híbrido que no tiene marcha atrás y, según como lo demuestra el estudio, “El camino digital hacia la resiliencia empresarial”, preparado por Boston Consulting Group, la madurez digital es la que distinguirá a los ganadores durante la pandemia¹.

Esto significa que de cara a este 2021 los líderes empresariales enfrentarán el reto de adoptar un cambio en la cultura de trabajo, que conlleva impulsar la productividad a la distancia al mismo tiempo que proteger los datos y llevar la innovación minimizando los riesgos de internet.

Solo durante el mes de abril, Microsoft detectó más 60 mil mensajes diarios con archivos o enlaces maliciosos relacionados con el covid-19 y bloqueó 1,6 millones de URLs que tenían el propósito de realizar ataques de phishing.

Entonces, ¿cómo hacemos del trabajo remoto algo conveniente y seguro para los empleados durante este tiempo de disrupción constante? La respuesta es el paradigma ‘Cero Confianza’².

La autenticación multi factor (MFA) al 100% de los usuarios todo el tiempo, es de lo más importante que pueden hacer las organizaciones para asegurar su información, así como las soluciones que limitan o bloquean el acceso a dispositivos desconocidos o que no cumplen con sus directivas de seguridad y un agente de seguridad de aplicaciones en la nube para evaluar el perfil de riesgo y decidir permitir el acceso, bloquearlo o incorporarla a su entorno de nube.

Contar con una infraestructura y servicios tecnológicos que cumplan los más estrictos requerimientos de seguridad y privacidad de la data es, ahora más que nunca, la clave para proteger los más importantes activos de las corporaciones. En Microsoft, hemos visto que una arquitectura de seguridad de “Cero Confianza” ayuda a proteger a las personas, los dispositivos, las aplicaciones y los datos de manera integral. La pandemia sin duda pasará, pero el uso intensivo de las tecnologías digitales seguirá en aumento, y proteger nuestro espacio digital continuará siendo fundamental.

Fuente:

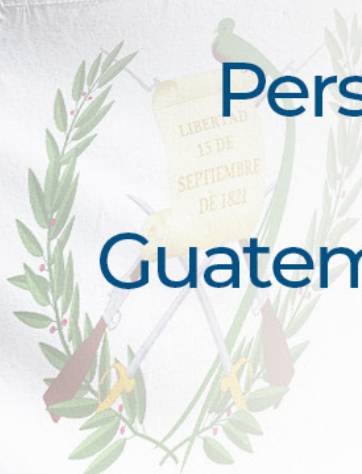
¹ “The Digital Path to Business Resilience” (El camino digital hacia la resiliencia empresarial). Boston Consulting Group. 2020. <https://www.bcg.com/publications/2020/digital-path-to-business-resilience>

² Implementing a Zero Trust security model at Microsoft. Microsoft. <https://www.microsoft.com/en-us/itshowcase/implementing-a-zero-trust-security-model-at-microsoft>



Visión empresarial 2021

Perspectivas económicas
y de inversión entre
Guatemala y Estados Unidos



ENE.26

02:30 p. m. CST

Regístrese acá:

<http://bit.ly/perspectivas-21>

Inversión:

Socios AmCham Q200

Miembros de Comités AmCham Q180

Público en general Q325

Información: Débora Aragón | 3096-1297
daragon@amchamguatemala.com



Conferencistas



José Alfredo Blanco Valdés

Vicepresidente
Banco de Guatemala



Neil Herrington

Vicepresidente Senior
Departamento de América
Cámara de Comercio de EE.UU.



David Lewis

Vicepresidente
Manchester Trade

Invitado especial



William Popp

Embajador de Estados
Unidos en Guatemala

Panel



Moderador
Juan Pablo Carrasco
Presidente AmCham Guatemala



Carlos Melo
BID



Pedro Brolo
MINEX



**Jorge Rolando
Paiz Klanderud**
PRONACOM



Clara Contreras
PEPSICO

Con el patrocinio de:



Con el apoyo de:





Trabajo eficiente, productivo y seguro desde casa



Por Enrique Aguirre, Director General de 3M para Centroamérica y el Caribe

"...es importante recordar que, aunque no estemos trabajando en una oficina, los equipos de cómputo con los que lo hacemos son para su uso laboral exclusivo."

Con la llegada de la pandemia de COVID-19, millones de personas alrededor del mundo tuvieron trabajar desde casa, buscando cumplir con las recomendaciones y requerimientos de las autoridades sanitarias, así como lineamientos proactivos de algunas empresas. En pocos meses, un importante porcentaje de la fuerza laboral mundial se encontraba trabajando desde sus estudios, cocinas, comedores o habitaciones.

El trabajo remoto ha demostrado ser una alternativa funcional, y aunque cada uno ha podido tener su propia experiencia positiva o negativa, para muchos pudiese representar una gran variedad de ventajas, como la eliminación de largos traslados de ida y regreso a la oficina, comer más saludable, la oportunidad de poder aumentar la productividad en un ambiente familiar y amigable, o estar cerca de seres queridos, como hijos, a lo largo de estos

meses de retos y dificultades. Sin embargo, hay ciertas precauciones que valen la pena revisar y tomar en cuenta para tener un Home Office óptimo.

Un tema trascendental es el de la ciberseguridad y el cuidado de los datos que se manejan en el trabajo, muchos de ellos son confidenciales. Un primer paso es saber que las conexiones privadas son más seguras que las públicas: trabajar desde el Wifi de un restaurante o una cafetería implica un alto riesgo, por lo que es recomendable conectarnos desde la conexión privada de nuestras casas, debidamente resguardada por una contraseña de acceso.

De igual forma, es importante recordar que, aunque no estemos trabajando en una oficina, los equipos de cómputo con los que lo hacemos son para su uso laboral exclusivo. Utilizar el equipo de una forma más personal, descargando aplicaciones ajenas al trabajo, o como punto de entrada para redes sociales o de navegador para diferentes páginas web, puede vulnerar el equipo a través de virus y otro tipo de peligros cibernéticos.

De acuerdo con Deloitte, "los efectos en forma de robo y extorsión, fraude y

daños irreparables se harán evidentes progresivamente, ya que el tiempo medio en el que una empresa descubre que es víctima de un intruso cibernético puede llegar a 170 días". Este dato es revelador y da la necesidad de estar preparados y alertas

Un punto que también me gustaría señalar es sobre los servicios de nube gratuitos. Aunque pueden ser vistosos, justamente por tratarse de servicios de almacenamiento de costo cero, existe un riesgo al utilizarlos, ya que son frecuentemente el target de robos de información. Es mejor utilizar las plataformas cloud corporativas que ya tenga contratada la empresa, generalmente de las marcas Google o Microsoft, o utilizar un servicio de membresía, que generalmente tiene estándares más altos de seguridad.

Finalmente, el feedback y el acompañamiento de las áreas de IT con todos los colaboradores. En 3M, hemos procurado que, desde las primeras semanas de Home Office, los colaboradores comprendieran las mejores prácticas para trabajar desde casa, tuvieran el equipo necesario, y una comunicación eficiente y directa con el equipo de IT. Después de varios meses de trabajo remoto, el resultado ha sido exitoso y satisfactorio.



La seguridad como norma en la nueva normalidad



Por Lissette Barrios

Con la transformación de las actividades laborales, se incrementan los riesgos y controles en el uso desde la casa de los colaboradores del internet y de las aplicaciones empresariales, destinadas a mantener la dinámica y gestión empresarial.

La conclusión de 2020 nos deja como lección la necesidad de innovar y buscar alternativas a las prácticas tradicionales de conservación de la información, de las reuniones presenciales y la concentración de personal en oficinas e instalaciones laborales.

Consecuencia de la pandemia, se evidenció la importancia del trabajo desde casa, para reducir las posibilidades de contagio por covid-19, además de las restricciones gubernamentales, para continuar con la dinámica empresarial y la prestación de los servicios esenciales para la población.

En ENERGUATE, el teletrabajo fue una de las primeras opciones para seguir con las actividades del negocio. Uno de los retos más importantes fue hacer las coordinaciones para el uso de equipo, plataformas y aplicaciones desde los lugares donde desarrolla sus tareas el personal.

En ese sentido, se recurrió constantemente a las reuniones desde Zoom y Teams, cuyas prestaciones permiten reunir a una gran cantidad de personas desde puntos remotos, mantener la comunicación, hacer coordinaciones y mantener unidos y

enfocados en los objetivos a los equipos de trabajo.

De esa cuenta, el internet se volvió una herramienta imprescindible en la gestión de las actividades y el mantenimiento del liderazgo. Prácticamente la dinámica ha girado en torno a las expectativas de una buena conectividad, que garantice el cumplimiento de las atribuciones en tiempo y forma.

Las acciones colaterales

Al utilizar y almacenar información sensible desde distintos lugares del país, cobró mayor relevancia la protección de los datos, y con ello también se evidenció la capacidad de la distribuidora para garantizar este tipo de seguridad y capacitar a su personal sobre detección de amenazas cibernéticas.

ENERGUATE utiliza plataformas web para la formación de los colaboradores respecto formas seguras del uso de internet, creación de contraseñas, detección de virus y cualquier otra amenaza que pudiera poner en riesgo los datos de la empresa.

Además, se cuenta con un equipo de Soporte Técnico que está capacitado y disponible para atender las dudas y resolver inconvenientes sobre ciberseguridad y mantener en funcionamiento óptimo las aplicaciones usadas desde el trabajo en casa, con constantes revisiones y pruebas.





Un año nuevo: ¿haremos cosas nuevas o cosas viejas?



Por Francisco Corzo, Director de SMART

El 2020 quedó atrás. 2021 es un nuevo año, una nueva oportunidad para brillar, para reinventarnos.

El aprendizaje organizacional es vital para el crecimiento y la sostenibilidad. En este ámbito, el “año de la pandemia” nos deja resultados negativos, pero también muy positivos. Si bien en algunas áreas (como los servicios de transporte, turismo, hotelería, etc.)¹ podemos haber retrocedido 5-10 años, en los sistemas de trabajo podemos haber avanzado un tanto similar.

El trabajo remoto no es un tema sencillo; menos cuando hemos tenido que improvisar. Es más que tecnología, o enviar una silla a casa, o hacer grupos A y B para turnarnos en la oficina. Es un proceso donde debemos analizar la esencia y la razón de ser de cada puesto en la empresa y lo que eso conlleva. Y también debemos analizar el entorno de cada persona, y las condiciones con que cuenta para trabajar en casa (que no es la única modalidad, pero ha sido la más usada

este año para procurar el aislamiento)

El remote working cada día será mayor. Centroamérica es hoy la segunda región de más rápida urbanización en el mundo² y, con ello, los problemas de tráfico. No habrá proyecto vial o de transporte que solucione ese problema, con suerte podrá compensar parte del deterioro vial. La solución es adoptar modelos de vida donde reduzcamos la movilidad y los traslados³. Además, Guatemala tiene una población joven (edad promedio 26.5 años)⁴; jóvenes que nacieron con la tecnología digital, y que tienen otras expectativas de vida y trabajo. ¿Está preparada su empresa para atraer y retener ese talento?

En SMART estamos apoyando a nuestros clientes a desarrollar un plan de retorno a sus oficinas, de manera segura y priorizando las necesidades del negocio y el bienestar y salud emocional de sus colaboradores; pero con una visión de largo plazo. ¡Año nuevo, cosas nuevas!



Fuente: Murray, A. (2020). Fortune 500 CEO survey: How are America's biggest companies dealing with the coronavirus pandemic? Fortune. <https://fortune.com/2020/05/14/fortune-500-ceo-survey-coronavirus-pandemic-predictions/>
Fortinet. (2020). Threat Intelligence Insider Latin America. <https://www.fortinetthreatinsiderlat.com/es/current/landing>

EXPO EMPLEO NACIONAL

**17 al 19 de
febrero**

Tendrá la oportunidad
de reclutar personal de
forma virtual.



AMCHAM
GUATEMALA

AMERICAN CHAMBER OF COMMERCE