Fuerza Aérea de Chile
Centro de Estudios Estratégicos y Aeroespaciales
Estrategia, Aeronáutica, Espacio, Tecnología & Innovación

BOLETÍN INFORMATIVO Y DE ANÁLISIS N° 07-2020 Santiago, 21 de abril de 2020

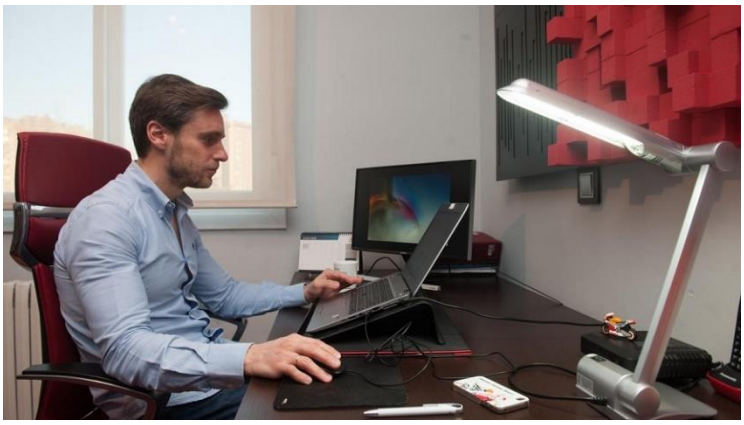
COVID-19, Home Office y Seguridad Informática

Enfrentado el mundo a una pandemia de proporciones como el COVID-19, que ya se asume nos afectará durante años, la necesidad de mantener en ejecución determinadas tareas y continuar con el funcionamiento de nuestras organizaciones (estatales o privadas, civiles o militares) ha debido conciliarse con el imperativo de adoptar medidas de distanciamiento físico que ayuden a controlar el *ratio* de contagio y, en consecuencia, permitir que los sistemas de salud enfrenten en forma exitosa este tremendo desafío.

En ese contexto, las decisiones de la gran mayoría de las organizaciones incluyen la prudente medida de disponer que el máximo posible de las tareas puedan ser ejecutadas con su personal trabajando desde sus hogares. Ello, en el caso de nuestro país y muchos otros, obedece además a la observación de disposiciones emitidas por las autoridades de salud respectivas.

Sin embargo, el trabajo en casa supone diversos desafíos que deben ser reconocidos para poder ser enfrentados en forma exitosa. Muchos de esos desafíos se enmarcan en áreas como la sociología y la psicología, así como en la necesidad de cuidar la salud y la forma física en una condición de confinamiento, pero no son parte del análisis de este boletín. El punto de atención de este reporte es otro y se refiere a la necesidad de preservar la seguridad de la información relevante que cada uno maneja, como asimismo de las redes institucionales y la información y sistemas de otros usuarios que se conectan a dichas redes.

El término “seguridad de la información” se refiere a múltiples aspectos que deben ser considerados. Nuestras conversaciones profesionales vía teléfono celular versan sobre aspectos relevantes (aunque se asume que no hablamos sobre materias clasificadas por ese medio), que son escuchados al menos por los demás integrantes de nuestro grupo familiar, a diferencia de los periodos de normalidad en que estamos entrenados para no violar la privacidad institucional en nuestros hogares, debido a que involuntariamente ello podría generar una indeseada e inocente cadena de filtraciones que funciona más o menos igual que un contagio de un virus. Apuntes, documentos que no necesariamente son clasificados están a la vista de otras personas y generan una vulnerabilidad que por sumatoria de datos puede llegar a ser importante. A pesar de la importancia de estos aspectos de la seguridad de la información, en estas líneas nos centraremos en un área que cobra cada vez más relevancia en esta materia y que se concentra en la necesidad de proteger la integridad de la información y sistemas en el ámbito informático.

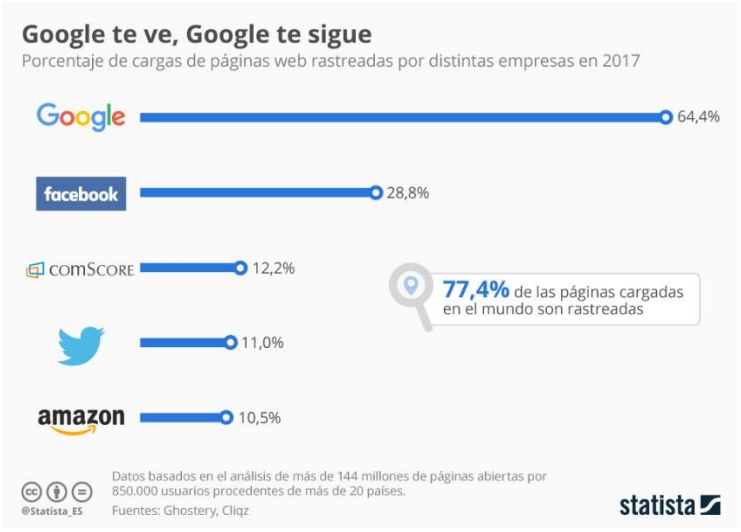


Las noticias diarias, nos alertan y alarman respecto de la profusión de amenazas que nos rodean en el ambiente informático. Engaños que conllevan el robo de datos, emails falsos que por medio de links malignos nos introducen malware, seguimiento de nuestras actividades y de nuestra ubicación física son ahora parte del escenario, por lo que debemos aprender a convivir con ese ambiente y salir airosos. La buena noticia, es que no es imprescindible ser un experto en seguridad informática para adoptar costumbres y formas de trabajo más seguras.

Una primera medida y no exenta de problemas y limitaciones, consiste en evitar el manejo de temas profesionales-institucionales en nuestros computadores personales. Para ello, entonces, es recomendable en la medida de lo posible, llevar los computadores institucionales al domicilio. En ocasiones esto no es posible, debido a las características físicas de los sistemas que empleamos en nuestro trabajo. En otros casos nuestros PC son parte de redes institucionales que no pueden ser llevadas al domicilio. En todos los casos, ello requiere dispensar del cumplimiento de restricciones institucionales para llevar elementos fiscales fuera de las dependencias institucionales.

Ahora bien: ¿cómo nos comportamos al usar internet?
Cada vez que navegamos en la red estamos activando una dirección que nos identifica ante esa red. Esa es la muy conocida IP, que al conectarnos a un sitio le entregan a ese servidor nuestra información sobre detalles de contacto, posición, nombre y mucho más que puede ser extraído por un experto en la materia. Actualmente el uso de Inteligencia Artificial (IA) hace que los sistemas buscadores “aprendan” sobre cada usuario, con lo que tienen un perfil cada vez más preciso sobre nosotros. Es por ello que nos envían información espontánea justamente sobre aquellas materias por las que hemos mostrado interés. Es el caso de las aplicaciones de e-commerce como Amazon, Alibaba, Wish y muchas más.

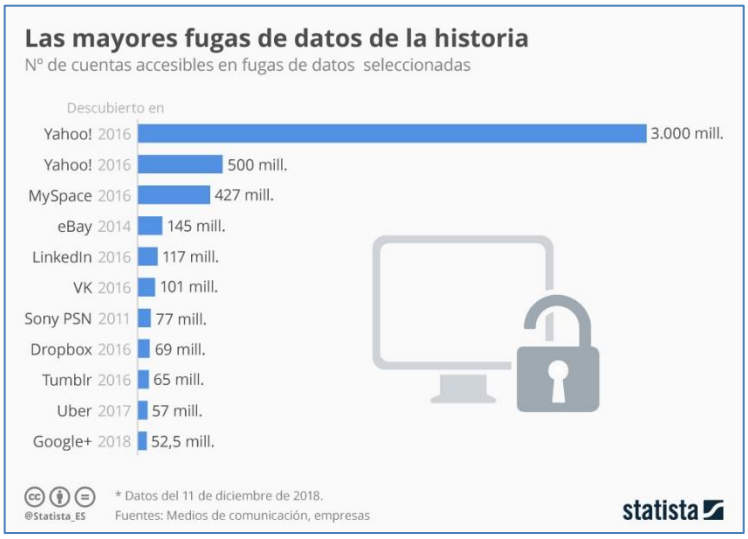
Un tendencia muy típica, es ingresar a un sitio, encontrar lo que buscábamos pero además enfrentarnos al ofrecimiento de múltiples “temas relacionados” que nos tientan a hacer click en sucesivos enlaces que nos hacen separarnos completamente de la búsqueda inicial y entrar inadvertidamente en el dominio de servidores que no son el inicialmente elegido y probablemente no son tan seguros.
Pregunta al respecto: ¿Usa usted Google? ¿Es usuario de Chrome?



Seguramente los utiliza en su PC personal y también en la oficina. Bueno: en ambos casos el usuario es el mismo, independientemente

de qué "máquina" esté usando, por lo que muchos datos sobre su persona pueden ser extraídos o deducidos por la IA de ese buscador desde ambos PC.
Cuando un usuario navega por internet, todo puede ser potencialmente rastreado, como por ejemplo:

- las búsquedas del usuario en los motores de búsqueda
- las páginas que el usuario visita
- la frecuencia con la que el usuario visita una página
- en qué sitios hace click el usuario
- la velocidad con la que el usuario mueve el cursor
- cuánto tiempo se queda el usuario en una página
- dónde el usuario se detiene para leer más profundamente
- los movimientos del *mouse* en la página web
- los comentarios y las reacciones que el usuario pueda añadir en una web o en las redes sociales, etc.
- etc. etc



¿Cómo Navegar en forma más segura, entonces?
Lo primero, es acceder solamente a sitios "seguros", que se identifican porque su URL comienza en https donde la "s" significa "seguro". Desde luego, cuando nos veamos obligados a caer en la tentación de pasar de un sitio a otro en secuencia, verifiquemos que el nuevo sitio también es seguro.

Segundo, utilicemos en la medida de lo posible diferentes buscadores en el PC personal y en el de la oficina. Hay muchas alternativas, unas mejores que otras, pero ninguna es perfecta: Google, Windows Explorer, Ask, Yandex, Tor…

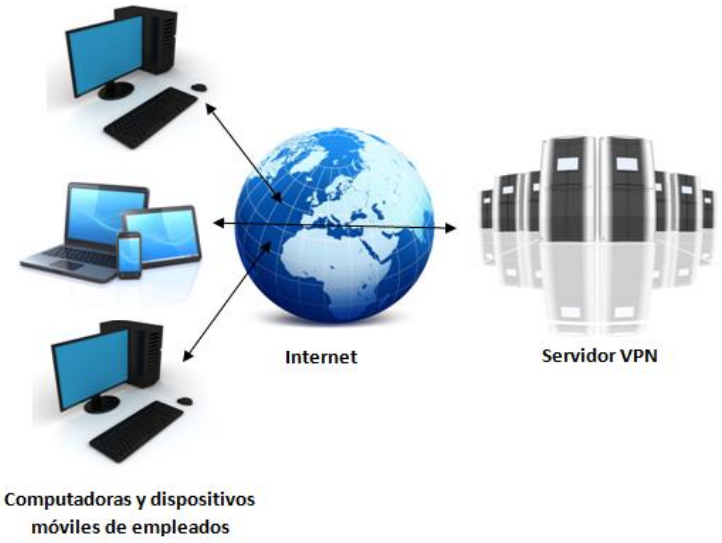
Tercero: sea que utilicemos un antivirus comercial, o el antivirus de Windows o las seguridades de IOS, verifiquemos los detalles de la configuración de seguridad. No toma mucho tiempo y se debiera hacer una sola vez, pero es importante determinar conscientemente qué permisos, restricciones y alertas estamos fijando. En el caso de los computadores fiscales, normalmente integran un antivirus específico y los *settings* son establecidos por la organización de seguridad, pero en nuestros computadores personales es nuestra responsabilidad.

Cuarto: Si nuestra organización ha establecido restricciones sobre el uso de dispositivos removibles o sencillamente ha bloqueado esos dispositivos, no intente burlar esas restricciones aunque la necesidad sea muy grande. En primer lugar, expone el sistema y eventualmente una red a múltiples amenazas y en segundo lugar, es muy posible que esa vulneración sea detectada y ello le traerá consecuencias.

Quinto: ser más restrictivo en el uso de *cookies.* Casi todos los sitios le preguntan si accede al uso de éstos y la tendencia natural es acceder en todos los casos. Al aceptar el uso de cookies, sus datos personales van a ser almacenados y procesados por ese sitio, lo que usualmente hacen las tiendas para crear un perfil suyo como comprador. Es cierto que los cookies ayudan a hacer más fácil navegación la próxima vez, ya que sus datos de ingreso "mágicamente" aparecerán de inmediato y le evitarán llenar formularios de datos como nombre de usuario y clave cada vez que acceda, pero los grandes buscadores logran obtener a través del análisis de cookies, mucha más información sobre usted y sobre lo que hace aún en otros sitios ajenos a esos buscadores.

Sexto: ¿Alguna vez se ha detenido a leer completamente los "términos y condiciones" antes de descargar una página o inscribirse en alguna comunidad u organización o empresa vía internet? Muchas veces, en esos términos y condiciones aparece la aceptación de que varios de sus datos, incluyendo el acceso a parte de sus archivos, sean accedidos por terceros.

Séptimo: Utilizar servicios VPN. VPN o Virtual Private Network consiste en la contratación de un servicio que, como dice su nombre, crea una red privada que evita que usted ingrese directamente a un sitio de internet, lo que lo protege de eventuales amenazas y evita que su IP sea detectada y seguida. Ello agrega una serie de ventajas adicionales que incrementan el nivel de seguridad de su aparato, lo cual es muy útil si accede a redes wi-fi desconocidas como los aeropuertos, pero hay que tener en cuenta que al contratar ese servicio usted está poniendo su seguridad en manos de ese proveedor. En consecuencia, ya que existen múltiples proveedores de VPN, hay que contratar a aquellos reconocidos por su calidad y confiabilidad.



Octavo y lo más importante: siga las normativas de seguridad de su institución y sea cauteloso. El sentido común y la prudencia, le darán buenas respuestas ante las dudas que le surjan trabajando desde su hogar, para beneficio de su tranquilidad y la seguridad de que la información de su institución, la suya y la de sus compañeros de trabajo, esté bien resguardada.

MLL