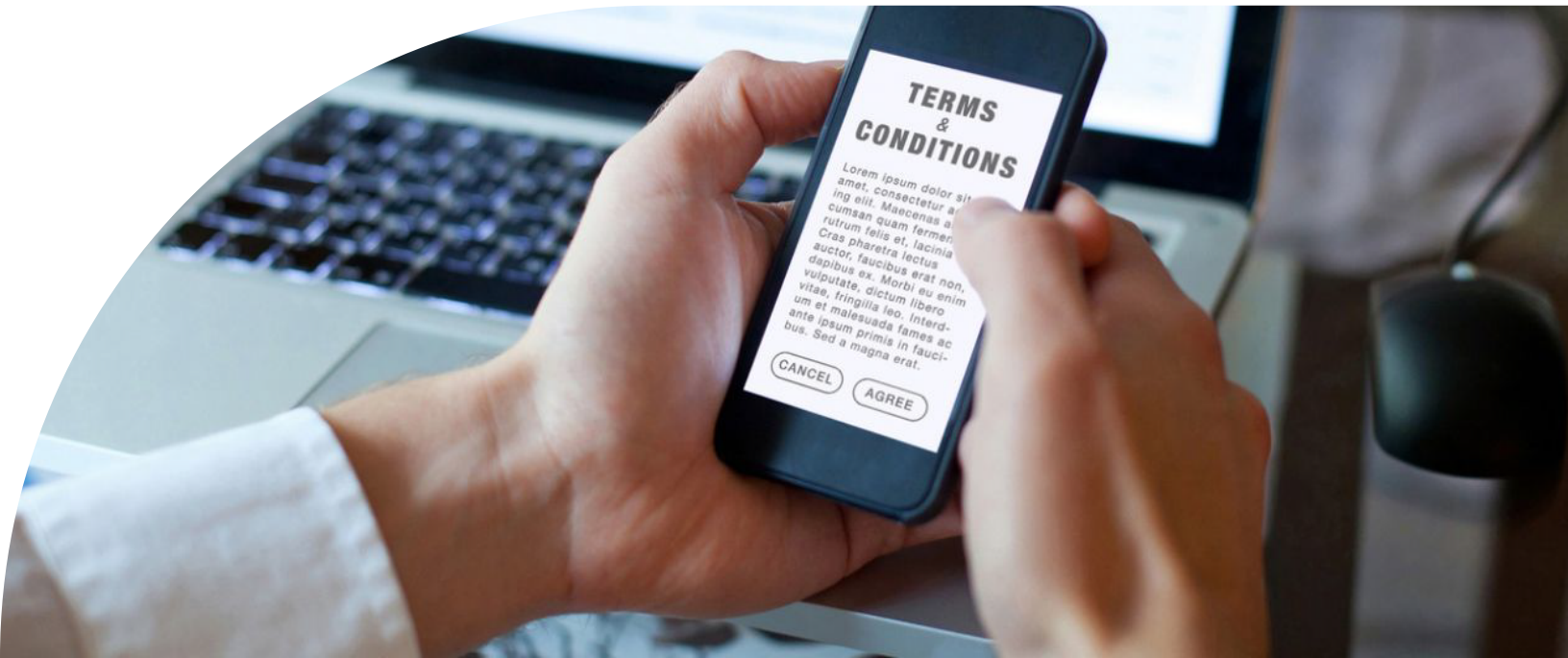
“LA GRAN TECNOLOGÍA SIGUE A TU EMPRESA; RECUPERAR EL CONTROL ES COMPLIANCE”

Grandes empresas de tecnología están siguiendo a miembros de tu organización. Incluso, pudieran estar comercializando sus datos al mejor postor, sin que las organizaciones tengamos conocimiento de ello.

Cuando navegamos por Internet nuestros datos se comparten con miles de empresas. Las famosas “cookies” se encargan de ello, distribuyendo nuestro perfil de consumidor para personalizar los anuncios que vemos a lo largo y ancho de Internet.



LA GRAN TECNOLOGÍA SIGUE A TU EMPRESA; RECUPERAR EL CONTROL ES COMPLIANCE

Los distintos tipos de cookies realizan un seguimiento y trazabilidad de las diversas actividades que las personas realizan. Por ejemplo, las "cookies de sesión" se utilizan solo cuando una persona está navegando activamente por un sitio Web. Una vez que abandona el sitio la cookie de sesión desaparece: Las cookies de seguimiento se pueden utilizar para crear registros a largo plazo de múltiples visitas al mismo sitio. Por su parte, las "cookies de autenticación" rastrean si un usuario ha iniciado sesión y, si es así, con qué nombre. En otras palabras, las cookies sirven para obtener información de los usuarios.

Te has preguntado: *¿cuántas empresas en Internet tienen tus datos?* Según Cambridge Analytica del año 2018, el usuario medio puede esperar que al menos 350 empresas tengan acceso a su información como puede ser su nombre, su cargo, el correo electrónico (profesional o no), información financiera, sus datos en las redes sociales, entre otros.

Sam Jones, fundador de Gener8, extensión de navegador de Internet que te permite navegar en línea en modo privado, en una entrevista publicada en la revista Forbes señaló: " *Hacemos clic sin pensar en aceptar en la ventana emergente de cookies que se interpone en el camino del artículo que estamos tratando de leer, pero la realidad es que, esa fracción de segundos está abriendo la mayoría de las veces*

una puerta de entrada para que cientos, tal vez incluso miles, de empresas comiencen potencialmente a rastrear, compartir y beneficiarse de su actividad en línea. Pero esa información, son nuestros datos y, según la legislación de la materia, son nuestra propiedad".

Así las cosas. Una vez que los miembros de una organización dan clic sin pensar detalladamente ni reflexionar con el fin de aceptar las "cookies", surge un cierto descontrol de la seguridad y privacidad de su información. Fenómeno que está fuera del alcance de la organización.

En circunstancias normales las cookies no pueden transferir virus ni malware a su ordenador. Debido a que los datos de una cookie no cambian cuando viajan de un lado a otro, no tienen forma de afectar el funcionamiento del equipo. Sin embargo, algunos virus y malware pueden disfrazarse de cookies o, por ejemplo, las cookies de seguimiento de terceros también pueden causar vulnerabilidad o problemas de seguridad, ya que facilitan que terceros que no pueden ser identificados con facilidad vean a dónde va el usuario y qué está haciendo en línea.

LA GRAN TECNOLOGÍA SIGUE A TU EMPRESA; RECUPERAR EL CONTROL ES COMPLIANCE

En la actualidad empresarial los miembros de las organizaciones no suelen estar conscientes ni concientizados en el uso y alcance de las cookies y esto genera riesgos evidentes que comprometen a las compañías y las hacen vulnerables. La mayoría de los hackeos y cibercrímenes que se cometen se deben a la desinformación y falta de capacitación o formación en materia de seguridad de datos personales.

Diseñar e implementar políticas internas para la prevención de riesgos en materia de Protección de Datos, concienciar, capacitar y formar a los trabajadores en el uso correcto de las cookies, es Compliance. Elegir una correcta extensión de navegador para que los trabajadores puedan navegar en línea en modo privado, es Compliance.

En la actualidad nacional e internacional son permanentes la violación de datos o escándalos de privacidad. El control en estos temas es casi imposible, pero la prevención sí está en manos de tu empresa.