

Conferencia Magistral. Vida digital sana y protección de datos personales de menores en la era digital
https://youtu.be/p7PYdirqlmM?list=PLZaXWcGPIGDZKdmlwg2JDz58py_DDqjp5

CONFERENCIA MAGISTRAL “VIDA DIGITAL SANA Y PROTECCIÓN DE DATOS PERSONALES DE MENORES EN LA ERA DIGITAL”.

Mtra. Elsa Bibiana Peralta Hernández: Buenos días, daremos inicio a nuestro panel siguiente. Muchas gracias.

Es un gusto tener aquí en esta Conferencia Magistral en una modalidad, digamos, un tanto novedosa, una modalidad compartida porque queremos escuchar los dos puntos de vista de dos grandes especialistas que tenemos la fortuna de conocer, no sólo porque en el plano personal hemos tenido oportunidad de intercambiar algunos escenarios, sino también porque también en esos mismos escenarios los hemos escuchado, hemos escuchado su expertise en la parte docente, en la parte conferencista, como compañeros de aula y también como conferencistas.

Y la verdad que les aseguro que lo que vamos a escuchar aquí será muy, muy provechoso para el inicio e iniciamos de verdad con invitados muy, muy especiales estos trabajos de estos tres días para conmemorar el Día Internacional de la Protección de Datos Personales.

Les agradecemos mucho que estén aquí y que no dejen de acompañarnos el día de mañana en las actividades también conjuntas con el INAI y el próximo viernes también en la Escuela de Medicina, que es un recinto que ya se ha constituido como una tradición para celebrar los seminarios internacionales por parte del InfoDF y de los organismos que nos permiten colaborar.

Muchas gracias al Archivo General de la Nación por permitirnos estar aquí en sus instalaciones y con quien hemos realizado una serie de trabajos conjuntos para trabajar los temas que nos atañen relacionados con archivos, protección de datos y transparencia.

Muchas gracias a todos ustedes por su participación, por su permanencia y bueno, les decía, es una Conferencia Magistral con dos expertos, tenemos un horario, manejaré ahorita la dinámica, si me lo permiten, tenemos un horario de hora y media, aunque ya nos retrasamos un poco, por atención a nuestros ponentes, vamos a tomarnos el horario que nos corresponde y de esta hora y media me parece que tenemos, ¿45 minutos cada quien? 45 minutos, está bien y de esos 45 minutos vayan ustedes preparando sus preguntas, por ahí les van a pasar algunas papeletas para que nos hagan llegar sus preguntas, haremos brevemente un paréntesis para las preguntas al final.

Yo no quisiera robarles mucho tiempo de eso, pero sí quisiera hacerles una breve síntesis curricular de nuestros participantes, dándoles la bienvenida por acompañarnos.

Muchas gracias, Daniel, muchas gracias Lina.

Daniel Korn es Director de Asuntos Corporativos de Microsoft Latinoamérica, donde dirige asuntos gubernamentales de Microsoft en los 46 países de la región.

Daniel llega a Microsoft Latinoamérica desde la sede de Microsoft de Redmond, Washington, donde estaba en el equipo de política y estrategia global IP conducción, participación de Microsoft en cuestiones de propiedad intelectual en los mercados emergentes, con un enfoque especial en China y Brasil.

Daniel recibió su licenciatura en música de la Juilliard School, un precedente muy interesante, y es coautor de Facilitando la Nube. Reglamento de protección de datos como motor de la competitividad nacional en América Latina, publicado por la Universidad Inter-American Law Review de la Facultad de Derecho de Miami.

Más recientemente su artículo en primer lugar para la adopción de las normas de seguridad internacional de la Nube, ISO 27018. Fue publicado por Trinidad & Tobago de Guarniar y La tecnología al servicio de la comunidad 2015, que fue publicado por la revista Uno.

La verdad es que la currícula de Daniel es muy, muy extensa, quisimos destacar solamente los trabajos más recientes y ustedes lo van a escuchar, es todo un deleite.

Daniel, te damos por equidad de género, primero, el uso de la palabra.

Gracias.

Daniel Korn: Muchas gracias. Buenos días a todos, muchas gracias por esta honrosa invitación.

Es siempre un placer regresar a México y más aun teniendo la oportunidad de saludar a la Comisionada Presidenta del INAI, Ximena Puente de la Mora; al Comisionado Presidente del InfoDF, Mucio Israel Hernández Guerrero; a la Comisionada ciudadana del InfoDF, Elsa Bibiana Peralta Hernández; al Coordinador de Protección de Datos Personales del INAI, Luis Gustavo Parra Noriega; a la Directora de Datos Personales del InfoDF, Ana María Cervantes Jasso; a mi colega de Google, Lina Ornelas Núñez, con quien comparto el espacio y a todos ustedes.

Aprovecho para congratular al INAI y al InfoDF su organización de este importante evento en ocasión del Día Internacional de Protección de Datos Personales, especialmente en esta histórica sede del Archivo General de la Nación, encabezado por su Directora General, Mercedes de Vega.

El cómputo en la nube es una de las más importantes transformaciones de nuestro tiempo. Es cierto que cuando uno piensa en el cómputo en la nube, uno suele pensar en los contenidos, juegos y redes sociales que accedemos desde nuestros dispositivos; y hoy vamos a hablar de una serie de buenos hábitos que desde Microsoft impulsamos para tener una vida digital sana.

Es importante reconocer a la vez que el cómputo en la nube contribuye a un nuevo modelo de desarrollo para América Latina, tiene la capacidad de proporcionarle a la comunidad un nivel de computación que anteriormente sólo estaba disponible para las compañías más grandes y las economías más desarrolladas, constituye la próxima etapa en la democratización de la

computización, eliminando la barrera entre aquellos que podían hacer la gran inversión de capital para adquirir y mantener las últimas tecnologías y aquellos que no podían hacer tal inversión.

Promueve la equidad mejorando los estándares de vida de nuestras comunidades al crear nuevos empleos, reducir costos, dar mayor agilidad, promover la inclusión social y facilitar la seguridad de los datos en un mundo cada vez más digitalizado.

Los nuevos empleos se generan gracias a que el cómputo en la nube libera el presupuesto de la organización previamente atado a inversiones en tecnología y su mantenimiento para invertirlo en nuevos mercados y productos.

Un reciente estudio del Boston Consulting Group, revela que las Pymes que utilizan el cómputo en la nube generan dos veces más puestos de trabajo que sus padres que no lo utilizan.

En este sentido la iniciativa Yo Puedo Programar de Microsoft, busca que más de un millón de jóvenes latinoamericanos mayores de 12 años aprendan un lenguaje de programación por medio de cursos que se ofrecen online de manera gratuita.

Usando la imaginación y las nuevas tecnologías los jóvenes desarrolladores de juegos webs pueden generar puestos de trabajo comenzando su propio negocio.

El ahorro en costos surge porque no se necesitan mayores inversiones de capital en servidores y otros equipos físicos.

Al consolidarse la demanda, se logran economías de escala, permitiendo menores costos por servidor en conceptos tales como electricidad, operación y mantenimiento y espacios físicos.

El Instituto Mexicano para la Competitividad (IMCO), estima que el sector público en México pudiera ahorrar un 1.7 por ciento de su gasto anual migrando a la nube.

Con respecto al consumo eléctrico, los ahorros en energía pueden traducirse en una reducción de emisiones de carbono, lo cual es otro resultado positivo para la comunidad.

En este sentido también el IMCO estima que la migración al cómputo en la nube por el sector de medianas y grandes empresas de México, significaría una reducción en tales emisiones equivalente a sacar 90 mil autos de circulación.

Al facilitar el acceso a recursos de computación, según la demanda, en cualquier momento y desde cualquier dispositivo conectado a internet, el cómputo en la nube brinda mayor agilidad a sus usuarios; por ejemplo, permite a los gobiernos y empresas responder a inesperados picos de demanda que un escenario de servidores internos, muchas veces no podría alcanzar.

Cuando el terremoto de 2012 en Costa Rica tornó inoperables las comunicaciones tradicionales, la capacidad del cómputo en la nube permitió responder a repentino aumento en tráfico y fue clave para que la estación de televisión nacional (Teletica), pudiera atender las necesidades de la comunidad en la provisión de actualización de información esencial, es igualmente importante el enorme potencial que tiene esta tecnología para aumentar la inclusión social.

Por ejemplo, la decisión de los arhuacos, el pueblo indígena que vive en la Sierra Nevada de Santa Marta de Colombia, de mantener sus registros catastrales en la nube democratiza la información entre 65 asentamientos con más de 46 mil habitantes, permitiendo el mapeo de sus lugares sagrados, el registro de sus conocimientos y la preservación de su idioma e identidad para el beneficio de la humanidad.

El cómputo en la nube también tiene el potencial de mejorar la seguridad de los datos, muchas pequeñas y medianas empresas no están en condiciones de tener adecuados niveles de seguridad en sus sistemas.

De hecho, según su estudio de 70 mil vulneraciones de seguridad en mil 600 empresas, Alert Logic encontró que los sistemas en servidores

propios, son más susceptibles a accesos no autorizados que las aplicaciones en la nube.

Estos grandes beneficios se podrán alcanzar siempre que haya confianza en la tecnología, para lograrla es necesario garantizar el respeto a la privacidad y seguridad de los datos personales y contar con reglas claras para el manejo de los mismos.

En el caso de Microsoft asumimos el compromiso contractualmente de custodiar los datos personales y estamos a la vanguardia de la implementación de estándares internacionales, somos los primeros en adoptar el nuevo estándar internacional ISO 27018 para la privacidad en la nube y es maravilloso ver otros en la industria siguiendo nuestro ejemplo y adoptando el ISO 27018 también.

Todos nos beneficiamos cuando estándares le otorgan a los clientes y a los reguladores transparencia y confianza en el cumplimiento por parte de los proveedores de servicios de nube con sus compromisos de privacidad.

El hecho que ISO 27018 es auditado por un tercero independiente lo hace una herramienta invaluable, inspira confianza cuando el tercero independiente verifica nuestras afirmaciones respecto de cómo manejamos la privacidad de los datos de los usuarios.

Como componentes relevantes noto que la ISO 27018 requiere que los proveedores servicios de nube se comuniquen con los clientes y reguladores en caso de un acceso no autorizado a los datos y que los proveedores de servicios de nube no utilicen los datos de los clientes a fines comerciales, sin previamente obtener su consentimiento expreso.

Noto que la autoridad de protección de datos personales del Uruguay, cuya directora está agendada para presentar mañana en esta misma serie de conferencias, ha notado públicamente, ¿qué se lograría con la adopción de este estándar? Mayor confianza en los proveedores de servicios en la nube que lo implementen y que todas las organizaciones que prevean seleccionar un proveedor para contratar servicios en la nube podrán tomar esta norma como referencia al momento de un mejor tratamiento de los datos personales.

La transparencia es esencial, tenemos que ser claros con el mundo acerca de qué tipo de datos se están colectando y cómo se están utilizando para ayudarle a la gente sacarle más valor a estas herramientas que estamos creando.

Asimismo, tenemos que asegurar que la gente pueda apagar las cosas y aunque sea cierto que algunas cosas no se pueden apagar porque son fundamentales a la operación del software o del dispositivo, la mayoría de las cosas deberían ser configurables de una manera que sea fácil para la gente descubrir, ajustar o cambiar; dándole a la gente transparencia y control les permite apoyar nuestro trabajo para avanzar la tecnología para el beneficio de todos.

La nube está transformando la manera en que jugamos, aprendemos, comunicamos, colaboramos y trabajamos, nuestra visión en Microsoft es que para mejor aprovechar los beneficios de todo lo que la tecnología tiene para ofrecernos, debemos adoptar unos buenos hábitos para llevar una vida digital sana y plena.

Para mejor protegernos cuando estamos en línea, necesitamos entender primero algunos de los potenciales viejos a nuestra seguridad, la privacidad de nuestra información y la seguridad de nuestros dispositivos.

Una vez que repasemos nuestros riesgos, compartiré nuestros hábitos recomendados para una vida digital sana.

Microsoft agrupa en cuatro áreas los riesgos a nuestra seguridad personal en línea: contenido, contacto, conducta y comercio.

El primero es contenido, bien se conoce el dicho que simplemente porque está en las noticias no quiere decir que sea verdad, ése mismo dicho se aplica en línea porque cualquiera conectado a internet puede ser un periodista ciudadano por medio de redes sociales o blogs, hay que tener presente que esta realidad a veces conlleva a contenidos incorrectos, cuestionables, inapropiados o extremistas.

El segundo es contacto, estos son los riesgos a los cuales nos exponemos por nuestras interacciones en línea, tales como ciberbullying, este es un mensaje dañino o un repetido acoso en línea

a través de cualquier tipo de dispositivo. Este contacto no deseado puede suceder a cualquier persona, pero más típicamente ocurre entre chicos.

Se denomina cyberstalking o cyber-harassment si se llevan a cabo con la participación de un adulto; depredadores y pederastas también pueden iniciar contacto no deseado con chicos, aunque no hay duda que éste es el peor tipo de contacto es también la forma más infrecuente de contacto en línea.

El tercero es conducta, los riesgos de conducta tienen que ver con lo que nosotros hacemos y decimos en línea, así como lo que otros escriben sobre nosotros. Nuestra reputación es producto de nuestras acciones, interacciones y lo que publicamos en las redes sociales, juegos y mundos virtuales o en los teléfonos móviles.

La información que ponemos en internet sobre nosotros mismos puede tener efectos no deseados, por ejemplo, cuando entrevistamos para un puesto de trabajo.

Y el cuarto es comercio electrónico, los riesgos del comercio electrónico surgen del hecho que nuestros datos personales son un producto muy valioso para las personas y las empresas, sean confiables o no, así que los riesgos del comercio electrónico, tienen que ver con una invasión de la privacidad o robo de identidad, cuando la gente mala obtiene acceso sin autorización a nuestra información sensible, tales como cuentas bancarias o números de tarjeta de crédito.

Así que cuáles son los hábitos que recomendamos para una vida digital sana.

Primero, piensa antes de hacer clic, este hábito es esencial y tiene dos componentes, el primero es piensa antes de hacer clic en links provenientes de alguien que no conoces o abrir fotografías, canciones u otros archivos adjuntos que provengan de un correo electrónico desconocido, esto para evitar descargar un software malicioso conocido como malware, que causa daño intencionalmente para robarte tus datos o tu contraseña, por ejemplo.

También hay que ser cauteloso con los archivos extraños que vengan de personas que sí conoces, a menos que estés esperando algo específico, ya que la computadora de tu amigo pudiera estar infectada con un virus que envía correo electrónico no deseado automáticamente.

El segundo es piensa antes de hacer clic y publicar algo en línea, mejor leer todos los mensajes antes de enviarlos para asegurarnos que el texto transmite el mensaje que queremos enviar y que no será mal interpretado.

Mejor no responder a mensajes amenazantes, insultantes o agresivos, en lugar de ello eliminarlos y de ser posible bloquear al usuario que emitió esos mensajes.

Mejor no enviar mensajes o correos cuando estamos molestos, pues en esos momentos podríamos no controlar nuestras palabras y lastimar a nuestros amigos.

Todo lo que escribas en la red puede permanecer al alcance de otros de manera permanente, aun cuando lo borres, datos, información, opiniones, ideas y fotografías, esto es fundamental, en el momento en que subes una foto, video o comentario a internet, hay que tener presente que el mismo es replicado de manera automática por los servidores y a través de las redes, a fin de mantener nuestros contenidos siempre disponibles.

Sin embargo, en el caso de muchas redes sociales también puede ser visible para amigos y hasta para terceros que a su vez pueden replicar nuestros contenidos en sus propias cuentas, como si ese contenido suyo fuera de ellos.

Fíjense como un tuit popular se replica de cuenta en cuenta y el autor en segundos pierde control sobre su difusión; asimismo, vemos como una foto de mal gusto caída en ciertas manos, es descargada en otras computadoras y reenviada miles de veces.

Mantén en secreto tu contraseña, no se la digas a nadie, inventa una contraseña que sea difícil de adivinar, pero fácil de recordar. Como yo le digo a mi hija de 14 años, si yo lograra adivinar tu contraseña,

¿cuánto invadiría tu privacidad? No utilices tu nombre ni tu fecha de nacimiento.

En las preguntas de seguridad de tus cuentas evita utilizar información que pueda ser deducida de tus publicaciones en redes sociales, como por ejemplo el nombre de tu mascota, de tu maestra de primaria o de tus gustos y preferencias conocidas.

Asimismo, para fortalecer la contraseña hay que mezclar letras mayúsculas y minúsculas, números y caracteres especiales utilizando contraseñas más largas que las cortas.

Tampoco se debería utilizar la misma contraseña para distintos servicios, si se roba su única contraseña todas sus cuentas protegidas por la misma contraseña quedarían expuestas.

Cuida tu imagen y la de los demás, no subas fotos tuyas o de otros de las que después te puedas arrepentir, una vez en internet su difusión es incontrolable, mientras su publicación puede dañar a alguien; además de saber que la información en internet puede ser replicada por múltiples razones, uno de los principales intereses de cada uno, tiene que ser cuidar y mantener una imagen respetable en línea.

Es bien conocido que los sitios de pornografía buscan fotos de perfiles públicos en las redes sociales para colocarlas en anuncios de sitios de pornografía.

Asimismo, nuestros comentarios y fotos en redes sociales pueden llegar a estropear oportunidades laborales y de educación superior.

En cuanto a la imagen de los demás, existen muchos casos de amigos que suben a canales de video secuencias graciosas de alguna persona, luego causándoles serios problemas de imagen e incluso dañando su salud emocional, cuando la audiencia cambia o se amplía.

Verifica qué saben de ti, busca tu nombre en internet y verifica qué información aparece de ti, siempre es importante buscar tu nombre, dirección, teléfono, cuentas de correo y usuarios de redes sociales dentro de los motores de búsqueda, como Bing, Yahoo o Google para

saber qué información sobre ti circula en internet y cuál es tu grado de anonimato en la red.

Cierra tu sesión, si te conectas en una computadora que no sea la tuya siempre cierra tu cuenta para que otros no tengan acceso a tu información o se hagan pasar por ti, esta recomendación aplica a las sesiones de computadoras o de cualquier otro dispositivo, como una tableta o teléfono móvil, incluyendo todo tipo de aplicaciones.

Si tienes la necesidad de acceder a tus cuentas a través de dispositivos ajenos, borra el historial de navegación de páginas, cookies y contraseñas almacenadas en el equipo una vez terminado su uso.

Por la misma razón es aconsejable no aceptar el almacenamiento automático de contraseñas ofrecido por los navegadores y aplicaciones.

Respetar a los demás, el ciberbullying es una tendencia creciente debido a la sensación de anonimato de los agresores; asimismo, un solo agresor puede hacer mucho daño a su víctima por la facilidad con la que se difunde la información.

La mejor manera de contribuir es no uniéndote a estas campañas nocivas y siempre estar pendiente de la naturaleza de los amigos que se tienen en línea y en la vida real.

Tú eres responsable de lo que publicas, cuida las palabras que pones en los foros y redes sociales, no hagas lo que no quieras que te hagan.

Usa un apodo o un alias, así te proteges y sólo tus amigos y familiares sabrán que eres tú, si por alguna razón necesitas ser identificable de manera más formal, a través de un correo o perfil de red social utiliza sólo un nombre y un apellido, así serás identificable para las personas indicadas, pero serás más difícil de ubicar a través de los motores de búsqueda, pero el uso de apodos o alias también implica responsabilidad de parte nuestra, hay que usar el anonimato como una herramienta para protegernos y no como una máscara para encubrir actos maliciosos.

No digas todo de ti, da la mínima información posible, no te expongas ni expongas a los tuyos, en las redes sociales, minimiza las opciones de terceros para buscarte, por ejemplo, controlar el nombre de tu secundaria, tu ciudad o tu empleador.

La mayoría de las personas mal intencionadas no están detrás de una persona en particular, siempre es más fácil y rápido estar monitoreando la red hasta encontrar a los grupos o personas más vulnerables.

Es claro que las personas cuya información es difícil de acceder son menos atractivos para los mal intencionados.

Asegura y cuida tus cuentas, decide cuál información es conveniente publicar y compartir en las redes sociales, así como quienes pueden acceder a ellas, no compartas detalles que pudieran utilizarse para identificarte a ti o tu ubicación.

No publiques algo que sólo le dirías a una íntima amiga, no aceptes invitaciones de personas que no conoces, ya que los amigos pueden cambiar con el tiempo, reevalúa periódicamente quién tiene acceso a tu cuenta y como tus preferencias cambian con el tiempo, comprueba las configuraciones y modifícalas, según sea necesario, revisa lo que tus amigos escriben sobre ti, asegúrate de que no compartan tu información confidencial. Está okey, pedirle a un amigo que remueva cualquier cosa que no quieras que se publique.

Crea varios emails, puedes tener una cuenta de correo electrónico para los amigos, otra para juegos y redes sociales, otra para maestros y empleadores, etcétera.

La seguridad en internet se mueve en círculos de confianza, así como en la vida real existe un espacio que sólo nos interesa a nosotros, uno que se comparte con la familia, otro con los amigos cercanos, otro con los contactos laborales, etcétera.

Tener definidas estas áreas en cuentas de correo, redes sociales y agendas telefónicas es muy importante para ayudar a proteger tu privacidad, protege a tus hijos.

Todos los hábitos que mencioné se fortalecen cuando se practican con la participación de los padres, específicamente con respecto a ciberbullying, se recomienda a los padres de familia platicar con sus hijos sobre cualquier problema de ciberbullying, preguntándoles qué saben del problema, si lo han visto o si lo han experimentado y se recomienda a los padres de familia estar muy pendientes de qué hacen sus hijos en internet, de tal forma que si detectan que son víctimas de ciberbullying o que son ellos mismos los ciberbullying puedan platicar y aplicar las medidas que consideren pertinentes.

Y para prevenir que el internet se convierta en una adicción de los niños, se recomienda a los padres de familia establecer horarios de uso de la computadora, platicar en familia sobre lo que el niño visita en internet, procurando que su uso sea principalmente para actividades académicas y culturales.

Seguir consultando otras fuentes de información, fuera de internet, como periódicos, libros, revistas, y seguir llevando a cabo actividades que no involucren el uso de internet o de la computadora, tales como correr, salir con los amigos, etcétera.

Toda esta información y más forma parte de Navega Protegido en Internet. Una iniciativa sin fines de lucro, impulsada por Microsoft México que surge hace más de 10 años para contribuir a la formación de ciudadanía digital y una vida digital sana.

Navega Protegido en Internet promueve el uso seguro y responsable de la tecnología, su objetivo es desarrollar prácticas que le ayudan a las personas a protegerse de los distintos riesgos asociados al uso de internet.

Navega Protegido en Internet lleva a cabo conferencias, cursos, talleres y asesorías sobre estrategias de seguridad informática, privacidad y ética en la red.

A fin de disminuir la ocurrencia de incidentes de seguridad informática en las empresas, así como para garantizar el cumplimiento con normas nacionales e internacionales, se ofrecen servicios de consultoría que permitan el diseño e implementación de campañas de

concientización dirigidas a los empleados en temas de privacidad y seguridad informática.

En esta iniciativa hemos colaborado con aliados estratégicos, tales como el INAI, la Asociación Mexicana de Internet, la Comisión Nacional de los Derechos Humanos y otros aliados públicos y privados para desarrollar prácticas que le permitan a las personas protegerse de los distintos riesgos asociados al uso de internet.

Como parte de este proyecto se han desarrollado cursos, talleres y conferencias que permiten dar a conocer los riesgos existentes dentro de internet, pero también las medidas de protección dirigidas a usuarios finales de tecnología.

Hasta la fecha Navega Protegido en Internet ha capacitado a más de 10 mil formadores y se han impartido conferencias sobre seguridad en línea, redes sociales, privacidad, gestión de datos personales, creatividad y propiedad intelectual y ciudadanía digital para más de 150 mil personas en todo el país; por ello, la Asociación Mexicana de Internet otorgó el reconocimiento AMIPCI 2009 y 2011 como la mejor iniciativa en arte cultura y educación.

Asimismo, en 2009 Navega Protegido en Internet tuvo la oportunidad de incorporar temas de privacidad y seguridad en el uso de la tecnología dentro de la currícula de tronco común en el sistema Conalep.

Así que los invito a descargar el App de Navega Protegido en Internet la próxima vez que visiten en Microsoft App Store, es gratis.

En resumen la vida digital sana surge de nuestra concientización de la necesidad de proteger nuestra privacidad y resguardar nuestra información.

La privacidad representa la capacidad del usuario de controlar el acceso a sus datos y actividades personales. Tiene que ver con la libertad individual para escoger qué queremos compartir y con quién.

La protección a la privacidad se traduce en la posibilidad de tomar decisiones informadas sobre cómo se comparte nuestra información digital y nuestras actividades en línea.

La gente y las compañías deben buscar servicios que cumplan sus necesidades de privacidad y seguridad, porque esa es una responsabilidad compartida entre los usuarios y los proveedores.

Asimismo, para resguardar la información, los usuarios se beneficiarán adoptando mejores prácticas, tales como contar con contraseñas seguras y los buenos hábitos que hemos repasado, para evitar caer en fraudes, *Malware* y robos de identidad.

Los delincuentes cibernéticos son una amenaza real, de ahí la importancia de saber de quién se obtiene información y a quién se le proporciona nuestra información antes de hacer clic.

Así que en esta celebración del Día Internacional de Protección de Datos Personales, dediquémonos a una vida digital sana para disfrutar de los avances en la tecnología, mientras protegemos los valores fundamentales de nuestra comunidad.

A eso se dedica Microsoft y somos optimistas, que entre todos lo podremos lograr.

Muchas gracias a todos.

Mtra. Elsa Bibiana Peralta Hernández: Muchas gracias a Daniel Cohn, les dije que iba a ser muy interesante escucharlo, nos deja muchas reglas muy claras, que no solo aplican, creo yo, en el ámbito privado, también en el ámbito público en todos los portales en todas las páginas y en todas las aplicaciones que tienen que ver con nuestro quehacer cotidiano en el ámbito público también.

Muchas gracias, Daniel, ha sido un gusto tenerte aquí y nos vas a acompañar ahora a escuchar atentamente a Lina Ornelas, que para muchos de nosotros ya es muy conocida ella, nos ha dado, les decía, pláticas, cursos y conferencias; es una amiga del Instituto desde hace muchísimos años y la consideramos parte de casa.

Muchas gracias, Lina, por estar aquí.

Y rápidamente les platico que Lina es egresada de la Facultad de Derecho de la Universidad de Guadalajara y maestra en cooperación legal internacional por la Universidad Libre de Bruselas; es experta en clasificación de información, transparencia, archivos, protección de datos y privacidad y ha publicado diversos libros y numerosos artículos; se desempeñó, durante 12 años, en el sector público en México y Europa, de los cuales nueve trabajó en el Instituto Nacional de Acceso a la Información Pública y Protección de Datos (INAI) como Directora General de clasificación y datos personales y, posteriormente como Directora General de autorregulación en materia de protección de datos personales.

Anteriormente, trabajó para la Comisión Europea y las secretarías de Economía y Gobernación, es miembro del *Apizori Board* del México Institute de la *Fundación Goodrow Wilson* en Washington, D. C.; del *Future of Price* –perdón por mi inglés, disculpen ustedes, *Forum*.

Juntos con expertos en privacidad en Internet y de la Asociación Internacional de Profesionales de Privacidad; es Vicepresidenta de Relaciones con Gobierno de la Asociación Mexicana de Internet y, me comunica que ha sido designada, recientemente, Presidenta de la Comisión de Economía Digital de la Cámara Internacional de Comercio en México; fue profesora e investigadora asociada del CIDE donde investigó diversos temas relacionados con lo que ahora nos ocupa.

Actualmente se desempeña como Jefa de Políticas Públicas y Relaciones con Gobierno para México, Centro América y El Caribe de Google.

Escucharemos la voz de otro representante importante, en lo que llega les concluyo, muy muy importante en los temas que estamos tratando.

Muchas gracias, Lina, te cedo el uso.

Mtra. Lina Ornelas Núñez: Al contrario.

Muchísimas gracias, de verdad que estoy muy honrada en que el InfoDF me invite a los eventos que organiza en materia de protección de datos personales, en particular quiero agradecer al Comisionado Presidente Mucio Hernández, también a David Mondragón, por supuesto a la Comisionada Ciudadana Elsa Peralta, a Luis Fernando Sánchez y Alejandro Torres con quien tengo incluso una amistad personal. Les agradezco muchísimo que nos inviten.

Y directamente creo que voy a endosar todo lo que dijo antes Daniel, realmente tienen ustedes que saber que la industria de Internet está comprometida con estos temas, y así tiene que ser porque debe existir una responsabilidad social.

Como ustedes saben, tanto Google, como Microsoft, como FaceBook, etcétera son compañías que tienen tantos millones de usuarios, miles de millones de usuarios, que realmente tenemos esta responsabilidad de crear ambientes seguros, de trabajar de la mano para que haya productos que haga que los usuarios en línea y los internautas naveguen seguros y protegidos.

Entonces en el marco de este evento tan importante que es el Día Mundial de la Protección de Datos, que se celebra mañana, tienen que saber ustedes por qué el 28 de enero se celebra esto en todo el mundo y hay eventos organizados por las autoridades de protección de datos, y esto es así porque se firmó, en los '80 un convenio, el Convenio 108 para la protección, fíjense, de las personas en relación al tratamiento de sus datos personales, tiene un nombre precioso, el Convenio 108, no es la protección del dato *per se*, sino la protección de la persona en relación al tratamiento de sus datos.

Y eso fue en los '80 y a partir de ahí, si bien México no es miembros de pleno derecho al Consejo de Europa, porque es solo para países en ese continente, tiene un carácter de observador y fue, la verdad, un modelo para nuestra Ley de Protección de Datos, tanto en el ámbito público, como privado, porque los datos personales están tanto en manos del gobierno, como de las empresas. Esto como marco referencial.

Y volverlos a felicitar por esta celebración.

Ya entrando en materia, en cuanto a la protección de los menores en la era digital, ustedes saben que realmente Internet es un espacio lleno de oportunidades para todos y realmente, sobre todo para los nativos digitales, ellos nacen en Internet, mientras que nosotros los migrantes digitales tuvimos que aprender a usar el correo electrónico, a navegar, pero realmente no hacemos todas las cosas que ellos ya hacen ahora.

Yo tengo tres hijos de todas las edades. El de cinco años, por ejemplo, ya hace búsquedas por voz, no necesita escribir para buscar; antes teníamos que esperar a poder poner algo, pero ahora con voz él, dice: "Polinesios, casas de navidad de jengibre". Y le sale lo que busca en YouTube.

Entonces, realmente el reto es mayúsculo, porque podría decir cualquier cosa y le aparecería cualquier cosa.

Entonces tenemos que contar con mecanismos de seguridad, educar a los padres, educar a todo el mundo y tener un enfoque holístico.

Pero hay que ver que en cuanto a cifras, el tema de los que se están integrando cada día Internet, es vertiginoso; simplemente en México hay 53.9 millones de usuarios en Internet, el 46 por ciento de esos tiene entre 13 y 24 años, para que nos demos una idea del universo y cada usuario se conecta a Internet, en promedio, estas son cifras de la Asociación Mexicana de Internet, entre seis horas y seis y 11 minutos, diariamente, este es el promedio.

Habrán niños que estén desafortunadamente a la mejor 10 horas porque se pierden de la vida real como decía Daniel y otros que parecen una, pero en realidad el promedio es seis horas, es altísimo.

Entonces por eso tenemos que enfocarnos muchísimo a cómo protegerlos en los distintos ambientes en los que están, porque nueve de cada 10 internautas usan redes sociales.

Ahora bien, no olvidemos que hay todo un mundo de oportunidad también, o sea Daniel enfocó mucho los riesgos, que es perfecto, porque además eso tenemos que hacer, prevenir esos riesgos y empoderar a los jóvenes para que sepan cómo protegerse.

Pero también no hay que olvidar que el Internet es el mundo abierto al conocimiento. Hoy en día uno puede estudiar, por ejemplo, teoría de juegos en Stanford y es gratis.

Realmente incluso el papel de las universidades va a modificarse, porque aquél que quiera tener una certificación de la universidad hará los exámenes, pero en el futuro podemos aprender lo que sea prácticamente ya en Internet; existen sitios como *Kanaka de Mite* que tienen contenidos para aprender todo lo que querramos y YouTube, por ejemplo, tiene un canal que ya lo pueden acceder en México, que es YouTube para Educación, en donde los jóvenes pueden estudiar desde matemáticas, cómo tocar guitarra, geografía, biología. Y todos esos vídeos están curados por profesores.

Entonces también tenemos que orientara a los niños y a los jóvenes a esos sitios con contenido que les puede interesar muchísimo y que los va a mantener con cuestiones más creativas, etcétera.

También hay recursos que la industria ha desarrollado. Por ejemplo hace poco FaceBook lanzó una plataforma contra bullying en México, son cosas muy importantes que hace la industria para que entre todos nos demos la mano y busquemos soluciones.

En el caso, por ejemplo de YouTube, tenemos un sitio que se llama...que en español también tiene su versión, para que los jóvenes que han sido objeto de bullying puedan ver vídeos de otros chicos que tuvieron esas experiencias y cómo resolvieron esa situación y cómo se sienten mejor ahora, la situación siempre puede mejorar y no por el contrario que se suman en una depresión que los pueda llevar a temas terribles, como ocurrió en Canadá o en otros países que llegan al suicidio.

Creo que es importante también decir que las plataformas, las redes sociales, etcétera lo que permiten es que haya mucha más libertad de expresión también.

Por un lado tenemos que transmitir un mensaje importante en cuanto a cuidar sus datos personales, como bien decía Daniel, pero que sí

puedan manifestar también lo que piensan y sus ideas y sus sentimientos.

Cada vez más vemos unos niños muy proactivos defendiendo sus derechos, pero también en plataformas por ejemplo de organismos internacionales como la UNESCO.

En Argentina existe un sitio que se llama “Yo Digo”, en donde los jóvenes empiezan a decir qué opinan de tener relaciones sexuales a temprana edad y cómo saber cuidarse, etcétera. Son temas que tienen que abordarse también y es la forma en la que se están comunicando.

Desafortunadamente las ciudades cada vez son más agrestes por temas de seguridad y distancia y los niños a veces ya no pueden salir a jugar a la calle como lo hacíamos en otras generaciones; su medio de comunicación es el Internet, y también tenemos que enseñarles a que pueden tener ideas increíbles que compartir, etcétera.

Y miren, este es un ejemplo de una chica que se llama Adora, ella es buenísima, porque un día se desesperó de que no entendía a sus profesores y decía: “Es que por qué no dan las clases más fácil”. Y se puso a armar unos vídeos en Internet de cómo explicar las partes de la planta y cuestiones de biología.

Y la verdad tuvo miles, cientos de miles de visitas y ahora ya es una conferencista Tec Toc porque es increíble. Entonces también hay que decirles a los chicos todas las oportunidades que hay ahí.

Entrando ya en materia de desafíos, como sabemos hay una prevalencia de los medios digitales a Internet en la vida privada de los jóvenes.

Hay una encuesta también que se hizo, internacional, para preguntarles a los chicos que si tuvieran que escoger un solo objeto de su casa porque se mudaran de casa al día siguiente ¿qué se llevarían?

Y todos dijeron que el celular, porque obviamente la cama, los juguetes, una cobija que les guste desde que eran niños no les importa, lo que les importa es eso. Y creo que a muchos adultos

también, ya hay hasta un síndrome de mucha ansiedad cuando uno no encuentra el celular; sales de tu casa y dejas el celular y no puedes ni respirar.

Es un tema interesante analizar sociológicamente, pero también saber que hay esa prevalencia en la vida de ellos y que también dicen todo sobre ellos y los pone en riesgo.

Por eso Google tiene tres pilares que son nuestros principios desde la parte de responsabilidad social, y lo que hacemos es, junto con la sociedad civil, con organizaciones muy importantes, con gobiernos y con otros aliados promover estos tres pilares.

Por un lado es empoderar a los jóvenes a través de información, esos consejos que dio antes Microsoft son súper importantes y los compartimos totalmente. Nosotros tenemos unos muy resumidos en cinco, pero engloban lo que él dijo y no los voy a repetir por obvio de tiempo, pero básicamente es eso, empoderarlos para decirles, miren: “En México vienen nuevos millones de conectados, de esos la mayoría son jóvenes, pero que entren conectados de manera segura.

Estamos trabajando también con el INAI en un proyecto que ojalá pueda cristalizarse este año, para que lleguemos, a través de medios masivos, a poder difundir estos cinco consejos; porque lo mejor que nos podría pasar es que todo niño en México supiera esos cinco consejos.

Por ejemplo, el tema de la contraseña de no compartirla es nodal. Ustedes sabían que entre los jóvenes de secundaria la prueba de amor, hoy en día, es darse la contraseña e incluso entre muchos adultos ha habido divorcios, porque hay gente que dice: “Es que si no me das la contraseña es que no hay confianza y algo me ocultas”.

Tienen que saber que no, incluso es un delito y aún con la pareja, la contraseña es consustancial a nosotros mismos y es parte de nuestra identidad digital.

Antes se hablaba de la *habeas corpus* porque es el tema de proteger la integridad física y demás, ahora es el *habeas Data* y hay que cuidar nuestra identidad digital.

Hay gente que nunca nos va a conocer en persona, pero nos va a conocer en línea. Entonces eso es muy importante cuidarlo.

Y hay temas muy serios que luego se salen de control. Por ejemplo el asunto de lo que le llaman Raid Points o el “porno de venganza”, en donde hay parejas que cuando están muy enamoradas, a veces se hacen vídeos o se toman fotos y cuando rompen, en el 99 por ciento de los casos las más afectadas son las mujeres, porque el hombre que está sentido sube esas fotos a la red y le destroza la vida a las mujeres

Entonces ya incluso eso se considera un delito, por ejemplo en California, aquella persona que utilice material en la intimidad y bajo un tema de confianza ocurrió, puede ir a la cárcel si difunde esas fotografías.

Se fijan cómo va evolucionando hasta el marco jurídico, porque a veces es un tema complejo. Y son temas que por ejemplo dentro de Google hay una responsabilidad social y se puede bajar ese contenido.

Realmente los únicos contenidos que se bajan, porque nosotros somos plataforma, no somos los propietarios de la información que circula ahí, pero son contenidos ilícitos y, sobre todo, quiero hacer hincapié en que hay cero tolerancia al abuso sexual infantil.

Google lucha todos los días, junto con otros miembros de la industria, para que por ejemplo si hay imágenes sobre abuso sexual infantil, etcétera. Esas imágenes desaparezcan.

En el buscador, si ustedes buscan pornografía infantil o lo que sea, no van a encontrar esos contenidos, porque se lucha siempre por estarlos eliminando; es un trabajo muy complejo que es con la sociedad civil, no podemos solos, porque hay terminología que en cada país es distinta y cambia para poder encontrar esos contenidos y a veces los pederastas y los “malos” como decía Daniel, usan unas cosas que uno no se imaginaría para poder llegar a encontrar contenidos así. Entonces es una lucha constante.

Por ejemplo Microsoft desarrolló una tecnología, que es la tecnología Hash para que se pueda encontrar una fotografía que tenga partes del cuerpo de un niño y de un adulto para poder encontrar esas imágenes terribles de abuso sexual y que se eliminen de manera automática; porque antes eso se hacía de manera manual, eso significaba que tenía que haber ingenieros.

Por ejemplo en Google viendo vídeos o buscando en *Search*, en el buscador, haber si había un contenido de ese tipo para bajarlo. Estos ingenieros tenía incluso problemas psicológicos, no podían trabajar más de cuatro horas seguidas, porque era terrible lo que veían.

Gracias a esta tecnología conjunta y luego Google desarrolló también otra para vídeo, la industria trabajó de la mano y junto con ONG's muy importantes para que eso se lograra.

También está el pilar de educación y el pilar de protección, que es ahí donde entran más las compañías.

Les voy a explicar un poco cómo funcionan.

Por ejemplo, en empoderar tenemos, a lo mejor no lo alcanzan a ver, pero en el buscador existe una forma ya muy sencilla y eso es importante tener aliados, terceros que nos ayuden a difundir esto, que los padres pueden poner un control parental para poder controlar de una manera que los niños no puedan llegar a contenidos de violencia o sexo explícito, etcétera a través de los buscadores.

Que digo, es difícil, como les digo, porque se está bajando eso, pero no es imposible que pase y tiene perfiles para la sesión de los niños y estar uno tranquilo de que cuando entra el niño en su sesión va a estar controlado lo que busque y lo que quiera encontrar.

Por ejemplo, yo con mi hijo Daniel hago eso, el entra por su sesión y yo sé que las cosas que le diga por voz al buscador no lo van a llevar a sitios que lo puedan perturbar, porque además está comprobado que los chicos, como no hay una buena comunicación entre los padres y los educadores, los adultos en general y los nativos digitales, ellos no le dicen a sus papás si vieron algo que los perturba, por miedo a que les quieten el Internet.

Porque lo que nos está pasando es que estamos entrando como en un tema de pánico que es terrible, y no debemos de entrar por ahí, que decimos, a los tres o cuatro años les damos una tableta para que en el restaurante nos dejen estar platicando a gusto y cuando ya tienen nueve ó 10 ya nos empezamos a preocupar por qué andarán haciendo y por qué están conectados todo el día.

Tenemos que ser congruentes, lo que decía Daniel es súper importante, no abandonar nuestro rol como padres y educadores, y los mismos consejos que les damos para decir cuando vayas al parque no te vayas a ir con un extraño, son los mismos en Internet, o sea realmente no cambia, el mensaje es el mismo.

Decirles, miren en una sesión de chat en una red social puede haber la foto de un niño de tu edad, pero en realidad puede ser un adulto; no te hagas amigos así nada más, tienes que saber si son de la escuela, etcétera.

Esos mismos consejos ya los hemos abandonado, porque como es una niñera muy barata el Internet, los dejamos ahí conectados todo el día y eso es terrible, tenemos que iniciar conversaciones.

Por eso Google creó el Centro de Seguridad de Familias, hay una página que se llama “es bueno saberlo” y en esa página hay una guía para que los padres también sepan cómo iniciar esas pláticas con sus hijos, dependiendo de la edad.

Porque miren, cuando uno le habla a un nativo digital, por ejemplo de FaceBook y no tiene una cuenta de FaceBook que digo ya no es el caso, porque muchos adultos ya están súper metidos en eso también, pero cuando empezaba el asunto, si no saben lo que es el muro o lo que es un Hashtag, los chavos ya no te quieren escuchar, te descalifican completamente.

En esta página hay maneras de iniciar conversaciones y demás, pero tenemos que, entre todo como les decía, buscar esa forma de llegar.

Y también en todos nuestros productos hay maneras de tener el modo de seguridad, poder poner filtros especiales y que la comunidad, entre

todos nos ayudemos a que si vemos un vídeo terrible hagamos lo que se llama el *flag*, es decir, levantar una bandera roja en YouTube y decir: “Este contenido es inapropiado para que nuestro equipo de remociones pueda bajar ese contenido”.

Obviamente hay todos unos criterios, porque es muy delicado el balance entre la libertad de expresión y bajarle el contenido a alguien que lo suba, pero si es algo ilícito y entra dentro de esas políticas del servicio o va en contra de las leyes, pues obviamente se bajará.

También quería contarles de otros recursos, por ejemplo este canal que les digo de familias seguras, todo está en español. Les pido una disculpa porque no traje la presentación traducida, pero hemos lanzado muchos retos para que los propios niños hagan los contenidos, porque justamente hablando de la comunicación es mucho mejor que un chavo haga el vídeo y le diga a otros cómo cuidarse, que nosotros desde nuestro mundo a lo mejor con un lenguaje que los pueda asustar más, etcétera.

Y hay ahí algunos buenísimos que los pueden ver, sobre por ejemplo un niño que se está bañando ahí en la bañera en un parque y, dice: “¿Tú harías eso?” Pues claro que no, nadie se va a ahí.

Lo mismo es con tu cámara Web que tienes ahí, está tal cual de exponencial si tú te desnudas ante esa cámara y pierdes el control de esa información.

Hago un comercial nada más muy rápido, porque ustedes no saben, a lo mejor muchos de los que son servidores públicos aquí, pero entre el público hay gente súper valiosa que está empujando estas iniciativas en todo el mundo y sí quería comentar aquí que tenemos a Jorge, de “pantallas amigas”, que es una ONG española que hace unos vídeos increíbles para que los chavos entiendan estos riesgos y son compañías contra el Sextin, contra el Bullying; porque ahora por ejemplo, sobre todo niñas y demás se toman fotos con poca ropa, etcétera y esa información, como ya dijimos, es muy difícil después controlarla una vez que se sube, por más que tú pidas que se elimine o tú la bajes, pudo haber mucha gente que ya copió esa imagen y que te va a perseguir y te va a causar muchísimos problemas en la vida.

También está Katitza Rodríguez, de la Electronic Frontier Foundation, es una Fundación increíble que ve los derechos y libertades de los usuarios en Internet.

Katitza, durante años también ha peleado por la seguridad de los niños en línea.

Lo menciono porque el trabajo que hacemos desde nuestras áreas, un aplauso para ella, porque la verdad es increíble.

La industria, siempre trabajamos con esas asociaciones y con el trabajo tan arduo que tienen, porque a veces es culturalmente la idea es la misma, pero hay que adecuarla, es muy interesante lo que se está trabajando.

Ya para ir terminando, a manera de corolario les cuento qué estamos haciendo en México ahorita.

Lanzamos un proyecto piloto el año pasado, que se llama “generación digital”.

¿Y por qué le llama generación digital? Va en la línea lo que decía Daniel, o sea en el futuro lo que vamos a buscar es ciudadanos digitales que respeten los derechos de los demás, que podamos ejercer derechos y libertades en línea, porque hacia allá vamos. En un futuro vamos a votar por Internet, vamos a hacer prácticamente nuestra vida por Internet y en la nube, como decía Daniel.

Es muy importante iniciar conversaciones, iniciar una campaña para empezar a mandar todos esos mensajes.

Y lo que hicimos con este piloto fue contribuir con mensajes al uso seguro y responsable de todas las oportunidades que Internet nos da, pero va dirigido a adolescentes de 13 y 14 años, de escuelas secundarias públicas y privadas también, nos acercamos a ellos a través de la Secretaría de Educación Pública.

Y también invitamos a la Policía Cibernética, porque tienen que saber que en México la Policía Cibernética da muchísimos cursos de capacitación a profesores en escuelas para mandar todos estos

mensajes, porque ellos ahorita están llenos de trabajo buscando a lo mejor pederastas o a la mejor un niño que no apareció y están viendo de qué manera pueden saber si a lo mejor se fue a una fiesta o dónde estaba la IP desde donde mandó el último mensaje. Es un trabajo muy técnico, muy complejo, muy delicado también.

Y lo que hicimos fue un proyecto piloto para que varias escuelas concursaran, les dimos un curso de capacitación con los cinco consejos para navegar seguro, que tiene Google, que son muy similares a los que mencionó Daniel: “El de no compartir tu contraseña, el que navegues buena onda”. Todo esto.

Y les pedimos que hicieran vídeos, y yo les quiero pasar, duran tres minutos estos vídeos ganadores, los primeros lugares. Uno es de una secundaria privada y otro es de una secundaria pública.

Lo interesante es que a ellos solos se les ocurrió cómo es el mensaje que tenían que transmitir.

Le vamos a poner el micrófono porque no había sonido, pero mientras vemos los vídeos y resolvemos eso, me voy rapidísimo al pilar de protección.

Proyección de Vídeo

Les mostraron fotos gracias de compañeros y las tenían que calificar.

Esto va en la línea de pensar antes de dar clic, que decía Daniel. Luego les mostramos una foto graciosa de su persona, primero de amigos, que es más fácil reenviar, pero esta fue la reacción cuando ellos estaban en la foto.

Se fijan que distinto.

Ocho de cada 10 alumnos enviarían la foto de alguien más, siete de cada 10 no enviarían su foto; son unos chavos muy listos del Colegio Jefferson, de secundaria. Esta fue una escuela privada.

Ahora vamos a ver el vídeo de la escuela pública, que también es súper interesante.

Mientras lo ponen les voy platicando, muy rápido, el pilar de protección. El de protección, como les decía, es todo eso que hace una empresa para que no salgan esos vídeos de abuso sexual infantil, etcétera. De remover el contenido que se denuncia y aplicar toda esta tecnología con expertos.

Vamos a ver éste, de la Técnica 14.

Proyección de Vídeo

Es lo que cada quien opina. Unos sí, ¡qué suba más fotos!

Y otra, ¡hay, quiere ser la más popular!

Ella ya bajó la foto, se fijan, del muro, pero ya está en todos lados.

Entonces lo que queremos hacer con “generación digital” es que en todas las secundarias del país necesitamos el apoyo de la Secretaría de Educación Pública, de las autoridades de Protección de Datos y hacer un esfuerzo conjunto para que cada escuela haga su campaña y la puedan transmitir.

Lo lindo es que cuando ellos se involucran ya son parte del mensaje y les queda mucho más claro a que si uno va y les platica.

Y ya para cerrar, unas reflexiones finales, ya no tengo el control, pero las reflexiones finales son en torno a todos los desafíos que tenemos para que esto se logre y es muy complejo, porque pasa por el marco regulatorio, por distintas autoridades, por todos los actores involucrados. El tema regulatorio es muy importante.

Por ejemplo, cuando hablamos de menores y el ámbito digital o de Internet, no tenemos en México una diferenciación de edades, porque en materia de protección de datos personales es solo con el consentimiento de los padres que se pueden tratar datos de menores, o por ejemplo que un menor podría abrir una cuenta de correo electrónico.

Ustedes se imaginan a un chavo de 17 años pidiéndole permiso a sus papás para abrir un correo electrónico o para crear un FaceBook.

En Estados Unidos existe algo que se llama “La COPA”, que es la Ley de Privacidad para Niños en Línea y que obliga a toda la industria del ocio en Internet y a todas las empresas que tienen este tipo de servicios y oferta y demás de bienes y productos, etcétera. Para que después de los 13 años ya los niños puedan navegar y ejercer su consentimiento.

Esto es importante porque tiene que haber un debate nacional acerca o en torno de ¿qué edad va a poner México para eso? Porque si no ahorita en los hechos se estaría incumpliendo, pero tampoco hay esta forma de poder obligar a que se cumpla, porque es muy difícil de poder comprobar la edad; la forma en que se comprueba la edad es cuando se despliega un combo de años en el año de nacimiento, pero la mayoría de los niños desde los nueve años están abriendo cuentas en redes sociales y lo que hacen es poner una fecha de nacimiento 10 años más de la fecha en la que nacieron y esa es la forma en la que lo hacen.

Eso incumple con las disposiciones, a nosotros como compañías que estamos radicadas en Estados Unidos nos aplican las leyes de los Estados Unidos y tenemos que cumplir con La COPA, que es esta regulación.

Es un tema que entiendo que la COMAIP que es la Comisión Nacional de Organismos de Protección de Datos y de Accesos a la Información ha puesto sobre la mesa para que se vea de qué manera podemos fijar un tema o discutir sobre la edad, porque es un tema importante.

Y también el tema de los tipos penales, que hay varias iniciativas de ley de senadores y diputados en torno al Grooming, Sexting, Bullying y es muy importante hacer tipos penales que sirvan realmente para atrapar a las personas que están cometiendo estos ilícitos y que no castiguen el medio comisivo per se, es decir, no es la culpa de Internet o del medio o de la plataforma lo que está ocurriendo, sino es una conducta humana ciento por ciento, es como el fraude. El fraude existe, pero si es en línea le llaman *Fishing*, que es hacer una página apócrifa, por ejemplo, de un banco y ustedes piensan que es Banorte

y ponen su NIP y en tres segundos les vacían la cuenta, porque no se fijaron que era un sitio seguro, pero eso es fraude, robo de identidad, etcétera.

Ya existe la pornografía infantil, existe el abuso sexual infantil, lo que falta es ver algunos otros tipos penales. Por ejemplo en el tema de Grooming, pues si es un adulto que estaba incitando o acosando a un menor para llegar a eso, a lo mejor ver si de los tipos penales existentes se puede hacer nada más en grado de tentativa, etcétera pero no castigar el medio comisivo per se, etcétera.

Y por último simplemente decir que sí es un tema de responsabilidad compartida, que estamos dispuestos a trabajar en la Asociación Mexicana de Internet entre todos.

Ya lo mencionó Daniel, ahí está Microsoft, está FaceBook también se acaba de incorporar en México y lo que tenemos es un sitio que se llama “conéctate seguro” en la página de Amipci.

Yo les pido que lo puedan consultar y que lo difundan en sus redes sociales lo más ampliamente posible, este es un tema de corresponsabilidad.

El sitio “conéctate seguro” lo que hace es que pone todos estos consejos que les dije, más los que dijo Daniel de “navega protegido” de Microsoft que es esta campaña tan importante más, lo que está creando FaceBook y todo los demás en temas de robo de identidad y de seguridad en compras en línea, etcétera están en un solo sitio, es un esfuerzo que hicimos para eso y que el Día de la Seguridad en Internet que es el 9 de febrero, lo vamos a divulgar más ampliamente ante los medios de comunicación.

Lo dejo ahí y les agradezco muchísimo. Estoy abierta para sus preguntas.

Hasta luego.

Mtra. Elsa Bibiana Peralta Hernández: Muchas gracias.

Yo creo que se merecen un aplauso ambos ponentes, mucho mayor, porque todo esto que nos han traído es bastante ilustrativo para todo lo que nos estamos enfrentando.

Les decía que también nosotros como dependencias estamos replicando aplicaciones, valga la expresión.

Entonces necesitamos también conocer todas estas reglas para aplicarlas y para normarnos.

La verdad es que el tiempo se nos ha acabado, yo preferí escucharlos a ellos. También me encantaría escucharlos a ustedes; ellos van a dejar un correo electrónico para poder enviarles sus preguntas, sus inquietudes y que más ampliamente ellos pudieran responder a todas estas inquietudes.

Les recuerdo que toda consulta causa honorarios, así es que no se extiendan en aquellas preguntas, no van a resolver problemas van a resolver nuestras inquietudes que como, estoy segura, los temas nos dejan muchísimas inquietudes, porque el tema es tan amplio, como tan amplia está siendo la cobertura de Internet en todo el mundo. ¿Verdad?

Muchísimas gracias a ustedes, los invitamos a pasar a darles otro aplauso muy fuerte porque se lo merecen, y ese mismo aplauso para ustedes porque han estado muy atentos y me parece que enseguida sigue un breve receso.

Los invitamos a pasar ahí a unos bocadillos que creo que hay o un cafecito.

No se vayan, nos falta entregar los reconocimientos.

Gracias, les agradezco.

Presentador: A continuación la Comisionada Ciudadana del InfoDF Elsa Bibiana Peralta Hernández, hará entrega del reconocimiento y un presente a la maestra Lina Ornelas Núñez.

También se hace entrega del reconocimiento y del presente a Daniel Korn.

Brindémosles un fuerte aplauso.

Invitamos a los integrantes de esta mesa a tomarse la foto.

A continuación haremos un receso.