CON PUNTO DE ACUERDO POR EL QUE SE EXHORTA A LA SECRETARÍA DE EDUCACIÓN PÚBLICA A EMITIR ACCIONES COORDINADAS CON EL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES Y CON LA SECRETARÍA DE SEGURIDAD Y PROTECCIÓN CIUDADANA, A FIN DE PREVENIR Y MITIGAR AMENAZAS DE SEGURIDAD INFORMÁTICA A ESTUDIANTES QUE REALIZAN ACTIVIDADES ESCOLARES MEDIANTE PLATAFORMAS EN LÍNEA, A CARGO DE LA DIPUTADA JULIETA MACÍAS RÁBAGO DEL GRUPO PARLAMENTARIO DE MOVIMIENTO CIUDADANO.

Quien suscribe, Diputada Julieta Macías Rábago, integrante del Grupo Parlamentario de Movimiento Ciudadano en la LXIV Legislatura de la Cámara de Diputados del Congreso de la Unión, con fundamento en los artículos 6, numeral 1, fracción I, y 79, numeral 1, fracción II, del Reglamento de la Cámara de Diputados del honorable Congreso de la Unión, somete a consideración de esta soberanía, proposición con punto de acuerdo mediante el cual se exhorta respetuosamente a la Secretaría de Educación Pública a emitir acciones coordinadas con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y con la Secretaría de Seguridad y Protección Ciudadana, a fin de prevenir y mitigar amenazas de seguridad informática a estudiantes que realizan actividades escolares mediante plataformas en línea, conforme a la siguiente:

Exposición de motivos

La incidencia de actividades delictivas en línea, como el robo de información personal y la suplantación de la identidad se han vuelto cada vez más recurrentes a pesar de los mecanismos de seguridad que ofrecen muchas de las plataformas y sitios web.

“En la mayoría de los casos, se roban datos para venderlos en el mercado negro y que son comprados por empresas de dudosa reputación para prospección comercial o envío de publicidad. Pero en otros, el robo de información puede generar daños considerables a una persona. En estos últimos casos, la información personal podría ser valiosa al utilizarla para suplantar una identidad y hacer transacciones o cometer fraudes.”[1]

La información personal que es robada puede ser utilizada por el delincuente para distintos fines, tales como el fraude cibernético o robo de identidad, la persuasión comercial o política,

[1] Consultado el 17 de abril de 2020. Ver más en: https://www.bbva.com/es/robo-informacion-personal-puedo-protegerme/

y la discriminación a partir de datos sensibles (como lo pueden ser los contenidos en un expediente clínico).

El Reporte Global de Riesgos 2019, publicado por el Foro Económico Mundial, colocaba al fraude o robo de datos como cuarto lugar de riesgo global con mayor probabilidad de ocurrencia y a los ataques cibernéticos en quinto lugar, solo después de los relacionados con el medio ambiente y los desastres naturales.

Top 10 de riesgos en términos de Probabilidad de Ocurrencia[2]

1. *Eventos climáticos extremos*
2. *Fracaso de la mitigación y adaptación al cambio climático*
3. *Desastres naturales*
4. *Fraude o robo de datos*
5. *Ataques cibernéticos*
6. *Desastres ambientales causados por el hombre*
7. *Migración involuntaria a gran escala*
8. *Pérdida de biodiversidad y colapso del ecosistema*
9. *Crisis de agua*
10. *Burbujas de activos en una economía mayor*

Esta clasificación nos ayuda a dimensionar el tamaño del problema que puede llegar a ser el robo de datos. Por ejemplo, "la cifra de usuarios en el mundo afectados por hackers que usan malware para robar su información se ubicó en 940,000 durante el primer semestre de 2019 respecto a casi 600,000 del mismo periodo en 2018."[3]

En el caso de nuestro país, la situación no es muy distinta. En 2018, Daniel Medina, director general y fundador de Finccom[4] (Firma especializada en temas de Gobierno Corporativo, Gestión de Riesgos y Cumplimiento), declaró que México es el segundo país donde se producen más robos de datos personales, sólo por detrás de Brasil.

[2] Consultado el 17 de abril de 2020. Ver más en: https://www.forbes.com.mx/fraude-cibernetico-y-robo-de-datos-riesgo-global/

[3] Consultado el 17 de abril de 2020. Ver más en: https://www.eleconomista.com.mx/finanzaspersonales/Aumentan-60-usuarios-afectados-por-robo-de-informacion-a-traves-de-malware-20190728-0055.html

[4] Consultado el 17 de abril de 2020. Ver más en: https://www.eleconomista.com.mx/empresas/Mexico-es-el-segundo-pais-con-mayor-robo-de-datos-personales-Finccom-20181129-0069.html

En ese mismo año, “de acuerdo con cifras de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) hasta septiembre de 2018, se registraron 49,843 reclamaciones por este ilícito. Solamente 54% de los casos tuvo una resolución favorable.”[5]

Recientemente, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) alertó sobre los riesgos al hacer compras por internet durante la contingencia por COVID-19 debido al alza de ciberdelitos[6]. Y es que la pandemia no solo ha generado problemas sanitarios y económicos en el país, también ha expuesto las deficiencias y debilidades que tenemos respecto a la protección de datos personales y la seguridad cibernética.

Hace unos días, “la Policía Cibernética de la Secretaría de Seguridad Ciudadana (SSC) de la Ciudad de México, alertó sobre el robo de datos personales a través de una página de internet para acceder a tarjetas de Bienestar, en la cual los adultos mayores y personas con discapacidad recibirán apoyos extra del Gobierno Federal y un bono adicional por la contingencia del COVID-19.”[7]

El riesgo de ser víctima de algún robo de información en plataformas digitales se incrementa durante el periodo de contingencia, debido a que la mayor parte de los mexicanos se han visto obligados a modificar diversos aspectos de su vida cotidiana, con el objetivo de evitar las interacciones sociales y así, prevenir el contagio del COVID-19.

Esto se traduce en un aumento exponencial en el uso de aplicaciones y plataformas digitales para realizar actividades como trámites administrativos, reuniones de trabajo o sesiones escolares. Sin embargo, la gran mayoría de usuarios de plataformas digitales, no se encuentran al tanto de los posibles riesgos que existen al proporcionar sus datos personales a las plataformas digitales.

Recientemente, “La empresa de ciberseguridad Cyble explicó que pudo comprar unas 530,000 cuentas de Zoom por unos 0,0020 dólares cada una. Zoom se ha hecho muy popular

[5] Consultado el 17 de abril de 2020. Ver más en: https://www.eleconomista.com.mx/finanzaspersonales/Que-debe-hacer-si-fue-victima-de-robo-de-identidad-20190224-0062.html

[6] Consultado el 17 de abril de 2020. Ver más en: https://www.milenio.com/politica/comunidad/compras-linea-inai-alerta-robo-datos-personales

[7] Consultado el 17 de abril de 2020. Ver más en: https://www.publimetro.com.mx/mx/noticias/2020/03/31/aprovechan-contingencia-sanitaria-robar-datos-personales.html

en medio de la pandemia de COVID-19, y ya había sufrido intrusiones por parte de terceros en videollamadas de escuelas, reuniones laborales y otras actividades."[8]

Considerando que el INAI[9] define a los datos personales como "cualquier información relativa a una persona física, que la identifica o hace identificable. Es la información que nos describe, que nos da identidad, nos caracteriza y diferencia de otros individuos." Estamos hablando de información como nombres, domicilios, fotografías, huellas digitales, números de tarjetas de crédito o débito, RFC, CURP e inclusive trayectorias educativas, número de cédula o certificados.

Y en este tipo de robos, las victimas más vulnerables son los menores de edad, pues "Hay una tendencia creciente entre los ladrones de identidad a robar identidades de menores, incluso de niños pequeños, ya que los registros de éstos constituyen un registro "limpio" para el delincuente y a veces lleva años hasta que se descubre el robo."[10]

Estos riesgos se agravan frente a la contingencia que enfrenta el país, pues son los niños y adolescentes los que mayormente se han visto en la necesidad de utilizar plataformas digitales para efectuar sus actividades escolares, así como mantener contacto social con familiares y amigos.

Los delincuentes utilizan diversos métodos para obtener la información deseada que van desde el engaño a los usuarios, la suplantación de sitios bancarios e incluso la extorsión. A continuación se detallan algunos de ellos:

> *Además de los formularios, las formas más comunes en que los delincuentes pueden robar su información a través de plataformas digitales, son las siguientes[11]:*
>
> *Phishing. Este concepto se le denomina a los correos electrónicos no deseados enviados por ciber-delincuentes, que simulan proceder de una persona o una organización legítima con la intención de engañarle para que revele información personal. Por ejemplo, un ciber-delincuente puede enviar un correo electrónico que parece proceder de su banco, en el cual se le solicita que "confirme" la información*

[8] Consultado el 17 de abril de 2020. Ver más en: https://www.excelsior.com.mx/hacker/zoom-refuerza-seguridad-tras-sufrir-robo-de-datos-por-parte-de-hackers/1376525
[9] Consultado el 17 de abril de 2020. Ver más en: https://www.cinvestav.mx/Portals/0/sitedocs/tyr/GuiaTitulares-01_PDF.pdf
[10] Consultado el 17 de abril de 2020. Ver más en: https://www.lja.mx/2017/09/robo-identidad-proteges-tus-datos-personales-arcana-imperii/
[11] Consultado el 17 de abril de 2020. Ver más en: https://www.lja.mx/2017/09/robo-identidad-proteges-tus-datos-personales-arcana-imperii/

de su cuenta haciendo clic en un vínculo que le dirige a un sitio web falso, donde se le indica que introduzca el nombre de usuario y la contraseña de su cuenta bancaria. El phishing es uno de los tipos de ciber-delito más frecuentes, y los ladrones constantemente cambian y actualizan sus estafas con el propósito de engañarle.

Pharming o redireccionamiento a sitios web falsos. Para intentar cometer este tipo de fraude, los hackers instalan un código malicioso en su equipo personal o un servidor para dirigirle a sitios web falsos sin que usted lo sepa. Pueden dirigirle a un sitio web de compras fraudulento y hacerle introducir información de pago sin que usted sepa que se trata de un sitio ilegítimo.

Spam por mensajería instantánea. Éste es un correo electrónico no deseado que se envía a través de mensajería instantánea (IM). Los mensajes pueden incluir spyware, registradores de pulsaciones, virus y vínculos a sitios de phishing.

Spyware. Consiste en un software que un hacker instala de manera oculta en su equipo para recoger información personal. También puede utilizarse para dirigirle a sitios web falsos, cambiar su configuración y apoderarse de su equipo de otras maneras.

La protección de datos personales se encuentra regulada en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, dirigida a personas físicas o morales de carácter privado, y en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, aplicable para cualquier entidad que ejerza recursos públicos (los tres niveles de gobierno, órganos autónomos, partidos políticos, fideicomisos y fondos públicos).

Sin embargo, el marco jurídico sobre ciberseguridad en nuestro país aún es difuso y laxo, por lo que existe desinformación sobre las obligaciones de quienes prestan servicios en línea, así como de los derechos de los usuarios y las buenas prácticas para disminuir posibles riesgos.

Hasta hoy, el INAI solo ha emitido recomendaciones a las instituciones educativas respecto a la protección de datos personales. Estas son[12]:

- Contar con Aviso de Privacidad y ponerlo a disposición de los titulares a través de los medios requeridos.

[12] Consultado el 17 de abril de 2020. Ver más en: https://www.quadratin.com.mx/educativas/deben-escuelas-responsables-en-resguardo-datos-personales/

- Implementar un programa de protección de datos personales que sea de fácil acceso y entendimiento para estudiantes, padres de familia y personal académico y administrativo.
- Tomar precauciones para que, al divulgar calificaciones de los estudiantes éstas no puedan ser relacionarlas con el alumno en particular.
- Implementar las medidas legales pertinentes al momento de publicar las fotografías, imágenes, nombres o cualquier otro dato personal de los alumnos en redes sociales o páginas de internet.
- Considerar si el estudiante es menor o mayor de edad para evaluar si la autorización del tratamiento de los datos personales corresponde al titular o a sus tutores.
- Promover los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) entre los estudiantes y sus tutores. Tomar precauciones adicionales respecto del tratamiento de datos personales sensibles y la obtención del consentimiento para las finalidades requeridas.
- Los Responsables deben tener la previsión de recabar sólo los datos estrictamente necesarios para la finalidad indicada, evitando resguardar más datos de los necesarios.

Como podemos apreciar, ninguna está encaminada a establecer mecanismos de seguridad en las plataformas digitales que utilizan las instituciones educativas, por lo que resulta urgente que las personas estudiantes y sus tutores cuenten con información puntual y de fácil comprensión sobre seguridad en línea y con ello mitigar el riesgo de amenazas cibernéticas durante la Jornada Nacional de Sana Distancia.

Por lo anteriormente expuesto, en nombre del Grupo Parlamentario de Movimiento Ciudadano, me permito someter a consideración de esta Honorable Asamblea la siguiente proposición con

Punto de Acuerdo

Primero. La Cámara de Diputados del Honorable Congreso de la Unión exhorta respetuosamente a la Secretaría de Educación Pública para que, en coordinación con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, diseñen y emitan a la brevedad un protocolo de ciberseguridad en actividades escolares mediante plataformas digitales, dirigido a las comunidades escolares públicas y privadas de todos los niveles educativos.

Segundo. La Cámara de Diputados del Honorable Congreso de la Unión exhorta respetuosamente a la Secretaría de Educación Pública para que, en coordinación con la Secretaría de Seguridad y Protección Ciudadana, establezca un mecanismo de atención a integrantes de comunidades escolares que resulten víctimas de algún delito cibernético en sus actividades educativas durante la Jornada Nacional de Sana Distancia.

Dado en el Palacio Legislativo de San Lázaro, a 27 de abril de 2020

Diputada Julieta Macías Rábago