INICIATIVA QUE ADICIONA EL ARTÍCULO 140 BIS AL CÓDIGO PENAL FEDERAL, A CARGO DE LA DIPUTADA ROCÍO BARRERA BADILLO, DEL GRUPO PARLAMENTARIO DE MORENA

La suscrita, Rocío Barrera Badillo, integrante de la LXIV Legislatura por el Grupo Parlamentario de Movimiento Regeneración Nacional, en ejercicio de la facultad conferida en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos; 55, fracción II, del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos; y 6, numeral 1, fracción I, y 77 del Reglamento de la Cámara de Diputados, somete a consideración de esta asamblea iniciativa con proyecto de decreto por el que se adiciona el artículo 140 Bis al Código Penal Federal, al tenor de la siguiente

Exposición de Motivos

Hoy, las tecnologías de la información se han convertido en herramientas indispensables para nuestras actividades cotidianas y como pilar fundamental para potenciar el crecimiento de las economías del mundo. Son la mayor fuente de consulta de información y una de las mayores plataformas comerciales, por lo que también son el medio frecuente para realizar actos ilícitos.

Los ataques informáticos constituyen un problema cada vez más grave a escala mundial, a grado tal que países como Estados Unidos han designado incluso comisiones especiales destinadas a establecer el potencial de daño que representan los sabotajes informáticos.

En el ámbito mundial, el costo de sabotajes informáticos para las empresas en 2017 aumentó en 27.49 por ciento en comparación con 2016. Compañías de Francia, Alemania, Italia, Japón, Reino Unido y Estados Unidos gastaron en conjunto 11 mil 700 millones de dólares en tratar de mitigar los ciberataques.

A escala regional, de acuerdo con un trabajo de Microsoft junto con la OEA, el costo de los sabotajes informáticos alcanzó 800 millones de dólares en Brasil, 300 millones en México y 460 millones en Colombia. Destaca que la industria financiera es de las más expuestas a ataques de este tipo; por tanto, es de las que más invierte en seguridad para prevenir el fenómeno.

El sabotaje informático abarca todas las conductas dirigidas a eliminar o modificar funciones o datos en una computadora sin autorización, para obstaculizar su correcto funcionamiento es decir causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.

Hay dos tipos de actores involucrados en el sabotaje informático:

1. Sujeto activo: La persona que comete el delito informático. Son los delincuentes, que tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Ejemplo el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

2. Sujeto pasivo: La víctima del delito informático. Las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a una red doméstica, pero en especial a los conectados a redes públicas o privadas.

El sabotaje puede causar la destrucción física del hardware y el software de un sistema y la eliminación de los elementos lógicos del sistema como son: la inutilización, o alteración de datos, programas, bases de datos información, documentos electrónicos, contenidos en cualquier soporte lógico, sistemas informáticos o telemáticos.

Técnicas por medios de las cual se comete un sabotaje informático *(El fraude informático. Consideraciones generales,* http://www.eumed.net/rev/cccss/14/ecra.html):

• Virus informático: Es un programa de computación o segmento de programa indeseado que se desarrolla y es capaz de multiplicarse por sí mismo y contaminar los otros programas que se hallan en el mismo disco rígido donde fue instalado y en los datos y programas contenidos en los distintos discos con los que toma contacto a través de una conexión.

• Bombas lógicas: La actividad destructiva del programa comienza tras un plazo, o por la aparición de determinada señal (que puede aparecer o puede no aparecer), como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo con lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar.

• Cáncer de rutinas: En esta técnica, los programas destructivos tienen la particularidad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos.

• Troyanos: Son programas creados para que a través de un archivo servidor se genere un acceso y luego ponerse a la escucha para que el atacante desde el programa cliente se conecte al servicio y pueda utilizar el ordenador de la víctima de forma remota.

Medidas preventivas:

• Encriptación: Proceso mediante el cual una rutina es codificada de tal manera que no pueda ser interpretada fácilmente. Es una medida de seguridad utilizada para que al momento de transmitir la información ésta no pueda ser interceptada por intrusos.

• Sistemas de protección de cortafuegos o *firewalls:* Un cortafuegos *(firewall* en inglés) es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

• Un buen firewall para internet puede ayudarle a impedir que extraños accedan a su PC desde internet. Los firewalls pueden ser de dos tipos, de software o de hardware, y proporcionan una frontera de protección que ayuda a mantener fuera a los invasores no deseados de internet.

• Antivirus: Es un software que se instala en el ordenador y permite prevenir que programas diseñados para producir daños, o *virus,* dañen el equipo. También tiene la misión de limpiar ordenadores ya infectados.

• Antitroyanos: Es un programa desarrollado para combatir software malicioso –malware–, como los troyanos o *backdoors.*

Actualmente, la nueva modalidad es de pequeños ataques informáticos, pero de manera constante, que no produzcan perjuicios notables que alerten a las víctimas, centrados principalmente en infectar computadoras, clonar tarjetas bancarias, destruir bases de datos de empresas o de instituciones de gobierno.

El problema de fondo es que la mayoría de los delitos informáticos permanecen en la impunidad. Por tanto, se propone tipificar en el Código Penal Federal el delito de sabotaje informático, que tiene lugar cuando alguien modifica, desvía, elimina, daña o realiza cualquier acto que altere ilícitamente el normal funcionamiento y contenido en los sistemas de información, tecnologías de la información o cualquiera de sus componentes, para obtener un beneficio para sí o para otro.

Por lo expuesto y fundado sometemos a la consideración de esta soberanía la aprobación del siguiente proyecto de

Decreto por el que se adiciona el artículo 140 Bis al Código Penal Federal

Único. Se **adiciona** el artículo 140 Bis al Código Penal Federal, para quedar como sigue:

Artículo 140 Bis. Se impondrá pena de cuatro a ocho años de prisión y de mil a mil quinientos días multa, al que dolosamente inutilice, altere o dañe temporal o permanentemente, un sistema informático o de archivos electrónicos, o los portales electrónicos de consulta de información a los que hace referencia la Ley General de Archivos.

Transitorio

Único. El presente decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Palacio Legislativo de San Lázaro, a 3 de septiembre de 2019.

Diputada Rocío Barrera Badillo (rúbrica)