Global CYBERSEC CERT

ADQ/DGRMSG/158/12/19

FORTALECIMIENTO DE LA CIBERSEGURIDAD EN EL SENADO DE LA REPÚBLICA

7. MAVAPE, S.A.P.I. DE C.V. entrega Reporte de Actividad en la Red Pública de Internet y Deep y Dark Web.

Carlos Viveros García
Director de Oficina de Proyectos

Dirección de Infraestructura Informática y de Comunicaciones DGIT

31 DIC. 2019

RECEPCIÓN

Nombre: Ivonne Hora: 18:00

	SENADO DE LA REPÚBLICA		
Nombre del Documento:	**Reporte de Actividad en la Red Pública de Internet y Deep y Dark Web**		
Proyecto	Fortalecimiento a la Ciberseguridad		
Proveedor	Global CYBERSEC	Global CYBERSEC CERT	
Identificación:	Entregable	**Versión/Revisión:**	1

Elaboró por parte del Proveedor	**Firma**	**Fecha de elaboración**
Alonso Ríos García Gerente del Blue Team		31-12-2019
Revisó por parte del Proveedor	**Firma**	**Fecha de revisión**
Isaac González Vázquez Líder de Servicio		31-12-2019
Aprobó por parte del Proveedor	**Firma**	**Fecha de aprobación**
Carlos Viveros García Director de Oficina de Proyectos		31-12-2019
Revisó por parte del Senado de la República	**Firma**	**Fecha de revisión**
Alfonso Esteban Barreda Granada Jefe de Seguridad Informática		31-12-2019
Aprobó por parte del Senado de la República	**Firma**	**Fecha de aprobación**
Luis Ángel Martínez Yebra Director de Infraestructura Informática y de Comunicaciones		31-12-2019

Índice

1. Información General

El **Senado de la República**, es una de las dos instituciones que conforman el Congreso de la Unión en México; en ella se aprueban leyes y proyectos que repercuten en todos los aspectos de la vida cotidiana, política y económica de México.

Su relevancia es tan importante, que por ello **Global Cybersec**, acompaña al **Senado de la República** mediante el proyecto de Fortalecimiento a la Ciberseguridad con el servicio de **Análisis de Eventos en la Deep Web & Dark Web**, a fin de descubrir e identificar las amenazas que podrían dañar la infraestructura de redes y telecomunicaciones, al igual que sus servicios de la institución, con el fin de recomendar estrategias y soluciones proactivas adecuadas a la operación, administración e infraestructura en función de sus operaciones de negocio.

2. Objetivo del documento

El presente documento tiene como propósito el análisis de tendencias, relaciones, detección de campañas y comportamientos anómalos en redes sociales, y especto de internet, con respecto a los objetivos incluidos dentro del alcance.

El personal especializado de **Global Cybersec** realiza el análisis con el apoyo de herramientas, procedimientos y guías que permiten la detección de nodos y aristas de interacción, los disparadores de estas. Así como campañas y comportamientos no orgánicos. Análisis de comportamiento de publicaciones, impacto. Detección de redes de usuarios y bots, detección de publicaciones eliminadas, categorías de usuarios, detección de fuentes. Los eventos son tratados como incidentes de seguridad si su comportamiento, efecto, o el objetivo o blanco que persigue, pone en riesgo la información o los componentes de la infraestructura que el negocio requiere para la actividad empresarial.

3. Alcance

El alcance del documento contempla la detección, impacto, análisis y categorización de información entrada en fuentes de información abierta, deep web y dark web, que pudiesen presentar un problema de seguridad informática para el **Senado de la República.**

4. Definiciones y Términos

Términos	Definiciones
Sensor	Dispositivo de seguridad que analiza el tráfico de red de forma pasiva, identificando anomalías y violaciones a las políticas de seguridad de la institución, equipos basados en firmas, que ayudan a la detección de eventos anómalos, de forma puntual.
DMZ	Es la zona desmilitarizada de una red, es decir, es una sección de red de la institución que se encuentra situada entre su red privada y su red externa pública. En seguridad informática, una zona desmilitarizada (conocida también como DMZ, sigla en inglés de demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa (los equipos de la DMZ no pueden conectarse con la red interna). Esto permite que los equipos de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que unos intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida. La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, web y DNS. Y son precisamente estos servicios alojados en

	estos servidores los únicos que pueden establecer tráfico de datos entre la DMZ y la red interna, como una conexión de datos entre un servidor web y una base de datos protegida situada en la red interna. Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando port address translation (PAT). Una DMZ se crea a menudo a través de las opciones de configuración del cortafuegos, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall).
LAN	Es la red privada de una organización. **LAN** son las siglas de *Local Area Network*, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios). Las redes LAN se pueden conectar entre ellas a través de líneas telefónicas y ondas de radio. Un sistema de redes LAN conectadas de esta forma se llama una **WAN**, siglas del inglés de wide-area network, **Red de area ancha**. Las estaciones de trabajo y los ordenadores personales en oficinas normalmente están conectados en una red LAN, lo que permite que los usuarios envíen o reciban archivos y compartan el acceso a los archivos y a los datos. Cada ordenador conectado a una LAN se llama un **nodo**. Cada nodo (ordenador individual) en un LAN tiene su propia CPU con la cual ejecuta programas, pero también puede tener acceso a los datos y a los dispositivos en cualquier parte en la LAN. Esto significa que muchos usuarios pueden compartir dispositivos, como impresoras o datos.
SSH	Protocolo que sirve para acceder de forma segura a equipos remotos.

	SSH (Secure Shell ó intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix) corriendo. Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a las máquinas y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH. SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible, evitando que terceras personas puedan descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos. Existen 2 versiones de SSH, la versión 1 de SSH hace uso de muchos algoritmos de cifrado patentados (sin embargo, algunas de estas patentes han expirado) y es vulnerable a un hueco de seguridad que potencialmente permite a un intruso insertar datos en la corriente de comunicación. La suite OpenSSH bajo Red Hat Enterprise Linux utiliza por defecto la versión 2 de SSH, la cual tiene un algoritmo de intercambio de llaves mejorado que no es vulnerable al hueco de seguridad en la versión 1. Sin embargo, la suite OpenSSH también soporta las conexiones de la versión 1.
PING	Es un comando que sirve como una utilidad diagnostica que comprueba el estado de la comunicación de un equipo con uno o varios equipos remotos de una red, mediante el uso del protocolo ICMP.

	Packet Internet Groper. Este comando se utiliza para comprobar si una determinada interfaz de red, de nuestra computadora o de otra, se encuentra activa. El PING envia paquetes al IP o host que se le indique, y nos dice cuanto tiempo demoró el paquete en ir y regresar, entre otras pocas informaciones. PING se usa para: resolver el nombre de host para saber su IP o simplemente verificar si una máquina está prendida. Un "ping" sin respuesta no necesariamente significa que la computadora no existe o esta apagada. Si el host o ip al cual se le hace ping tiene un firewall que no permite las respuestas al protocolo ICMP, entonces el "ping" no puede proporcionarnos información.
ICMP	Protocolo de notificación y control de errores. RFC 792. Para intercambiar datos de estado o mensajes de error, los nodos recurren al Internet Control Message Protocol (ICMP) en las redes TCP/IP. Concretamente, los servidores de aplicaciones y las puertas de acceso como los routers, utilizan esta implementación del protocolo IP para devolver mensajes sobre problemas con datagramas al remitente del paquete. Aspectos como la creación, la funcionalidad y la organización dentro de la amplia gama de protocolos de Internet se especificaron en 1981 en la RFC 792. En el caso de la sexta versión del Internet Protocol (IP), la implementación específicaICMPv6 fue definida en la RFC 4443. Por definición, ICMP es un protocolo autónomo aun cuando los diferentes mensajes están incluidos en paquetes IP tradicionales. Para tal fin, el protocolo de Internet trata a la implementación opcional como un protocolo de capas superiores. Los diversos servicios de red que se suelen utilizar hoy en día, como traceroute o ping, se basan en el protocolo ICMP.
HTTP	Protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

	RFC 1945 El Protocolo de transferencia de hipertexto (en inglés, Hypertext Transfer Protocol, abreviado HTTP) es el protocolo de comunicación que permite las transferencias de información en la World Wide Web. HTTP fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force, colaboración que culminó en 1999 con la publicación de una serie de RFC, siendo el más importante de ellos el RFC 2616que especifica la versión 1.1. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. HTTP es un protocolo sin estado, es decir, no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de sesión, y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.
VPN	Red Privada Virtual (RPV). Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada. Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN), es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.1 Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos. Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

	La conexión VPN a través de Internet es técnicamente una unión wide area network (WAN) entre los sitios pero al usuario le parece como si fuera un enlace privado— de allí la designación "virtual private network"
Port Mirror, puerto espejo	Es un puerto utilizado en un Switch de red para enviar copias de paquetes de red vistos en el puerto físico del dispositivo. Esto es comúnmente utilizado para aplicaciones de red que requieren monitorear el tráfico de la red, tal como una intrusión no autorizada a algún sistema.
Interfaz de red	Es un periférico que permite la comunicación con aparatos conectados entre sí y también permite compartir recursos entre dos o más computadoras. La capa de interfaz de red **TCP/IP** formatea los datagramas IP de la capa de red en paquetes que las tecnologías de red específicas pueden interpretar y transmitir. Una interfaz de red es el software específico de red que se comunica con el controlador de dispositivo específico de red y la capa IP a fin de proporcionar a la capa IP una interfaz coherente con todos los adaptadores de red que puedan estar presentes. La capa IP selecciona la interfaz de red apropiada basándose en la dirección de destino del paquete que se debe transmitir. Cada interfaz de red tiene una dirección de red. La capa de interfaz de red es responsable de añadir o eliminar cualquier cabecera de protocolo de capa de enlace necesaria para entregar un mensaje a su destino. El controlador de dispositivo de **adaptador de red** controla la tarjeta adaptadora de red. Aunque no es necesario, una interfaz de red se suele asociar con un adaptador de red. Por ejemplo, la interfaz de bucle de retorno no tiene ningún adaptador de red asociado. Una máquina debe tener una tarjeta adaptadora de red para cada red (no tipo de red) a la que se conecta. Sin embargo, una máquina sólo necesita una copia del software de interfaz de red para cada adaptador de red que utiliza. Por ejemplo, si un sistema

principal se conecta a dos Redes en anillo, debe tener dos tarjetas adaptadoras de red. Sin embargo, sólo se necesita una copia del software de interfaz de **Red en anillo** y una copia del controlador de dispositivo de Red en anillo.

TCP/IP soporta los tipos de interfaces de red:

Ethernet Versión 2 estándar (en)
IEEE 802.3 (et)
Red en anillo (tr)
SLIP (Serial Line Internet Protocol)
Bucle de retorno (lo)
FDDI
Óptica serie (so)
PPP (Point-to-Point Protocol - Protocolo de punto a punto)
Dirección IP virtual (vi)

Las interfaces Ethernet, 802.3 y de Red en anillo son para utilizarse con las redes de área local (LAN). La interfaz **SLIP** es para utilizarse con conexiones serie. La interfaz de bucle de retorno la utiliza un sistema principal para devolverse mensajes a sí mismo. La interfaz Óptica serie es para utilizarse con redes ópticas de punto a punto utilizando el Manejador de dispositivos de enlace óptico serie. El **Protocolo de punto a punto** se utiliza normalmente cuando se conecta a otro sistema o red a través de un módem.

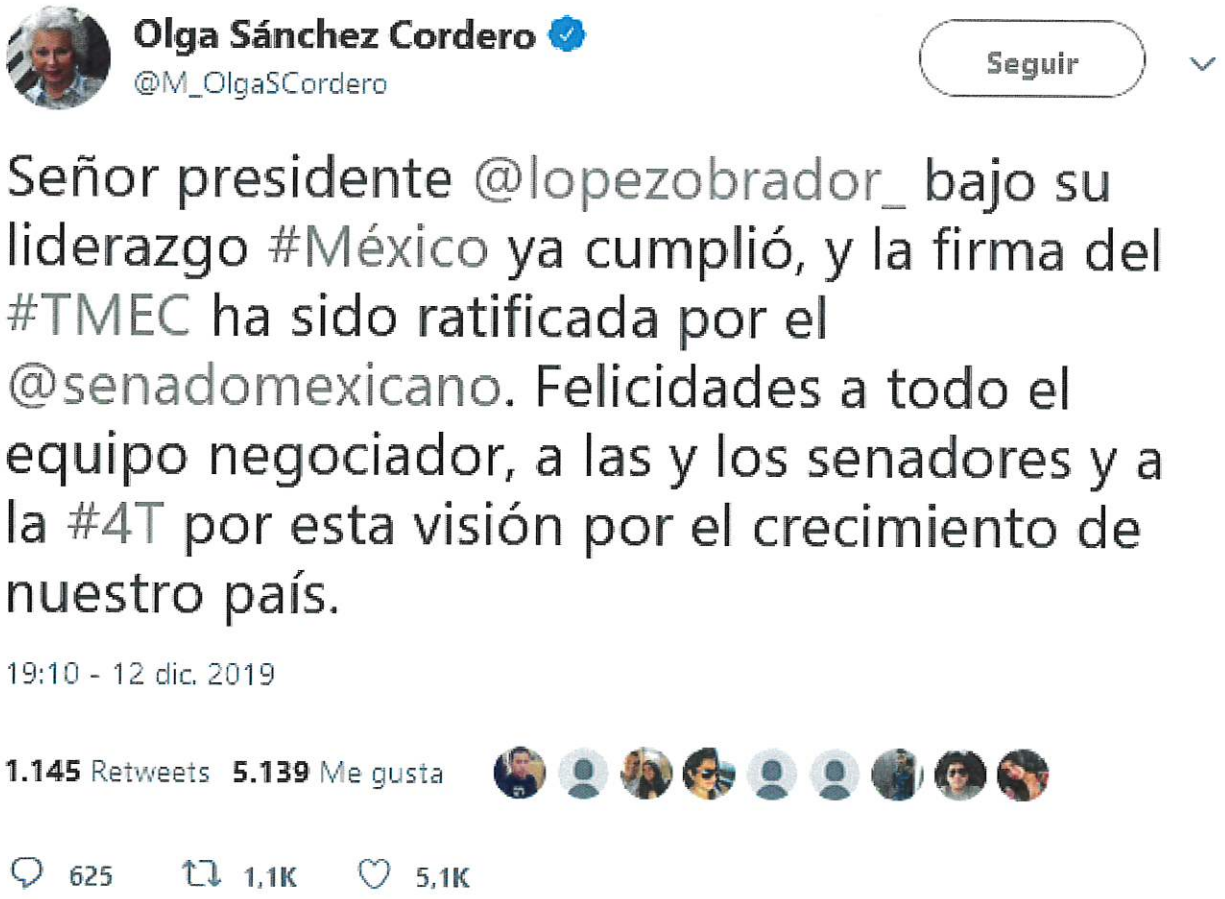
La interfaz de Dirección IP virtual (también denominada *interfaz virtual*) no está asociada con ningún adaptador de red determinado. Se pueden configurar varias instancias de una interfaz virtual en un sistema principal. Cuando se configuran interfaces virtuales, la dirección de la primera interfaz virtual se convierte en la dirección de origen a menos que una aplicación haya elegido una interfaz diferente. Los procesos que utilizan una dirección IP virtual como dirección de origen pueden enviar paquetes a través de cualquier interfaz de red que proporcione la mejor ruta para dicho destino. Los paquetes de entrada destinados a una dirección IP virtual se entregan al proceso independientemente de la interfaz a través de la cual llegan.

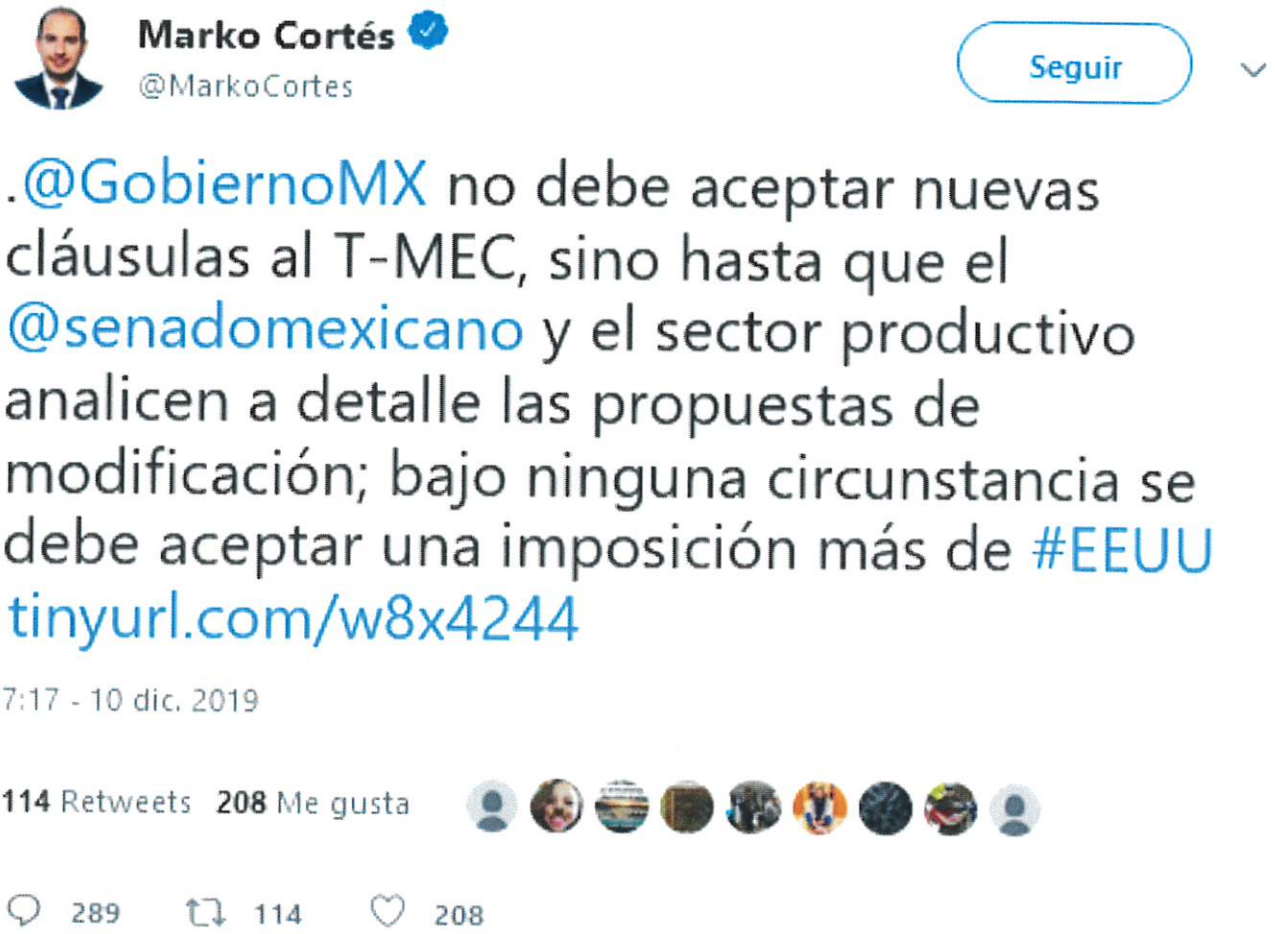
5. Hallazgos

En esta sección se presentan el análisis de cibervigilancia en redes en el mes de diciembre 2019, así como como las estadísticas de estos.

- **Caso TMEC**

El Pleno del Senado de la República en sesión extraordinaria aprobó el T-MEC el 19 de junio de 2019. La Secretaria de Gobernación Olga Sánchez Cordero realizo un tweet desde su cuenta personal etiquetando al senado mexicano.





- **Designación de Ministra de la SCJN**

El 4 de diciembre se llevó a cabo la reunión en la que comparecieron las aspirantes a ministra de la Suprema Corte de Justicia de la Nación. Al obtener la mayoría constitucional de dos tercios de los votos, Margarita Ríos-Farjat fue designada por el Pleno del Senado de la República. La Mesa Directiva informó que como resultado de vaciar y clasificar los documentos contenidos en la urna donde se emitieron los votos, "se identificó que se depositaron 122 cédulas de votación, dos sobres vacíos, dos objetos, un barco de papel y un avión".

Margarita Ríos-Farjat
@MargRiosFarjat

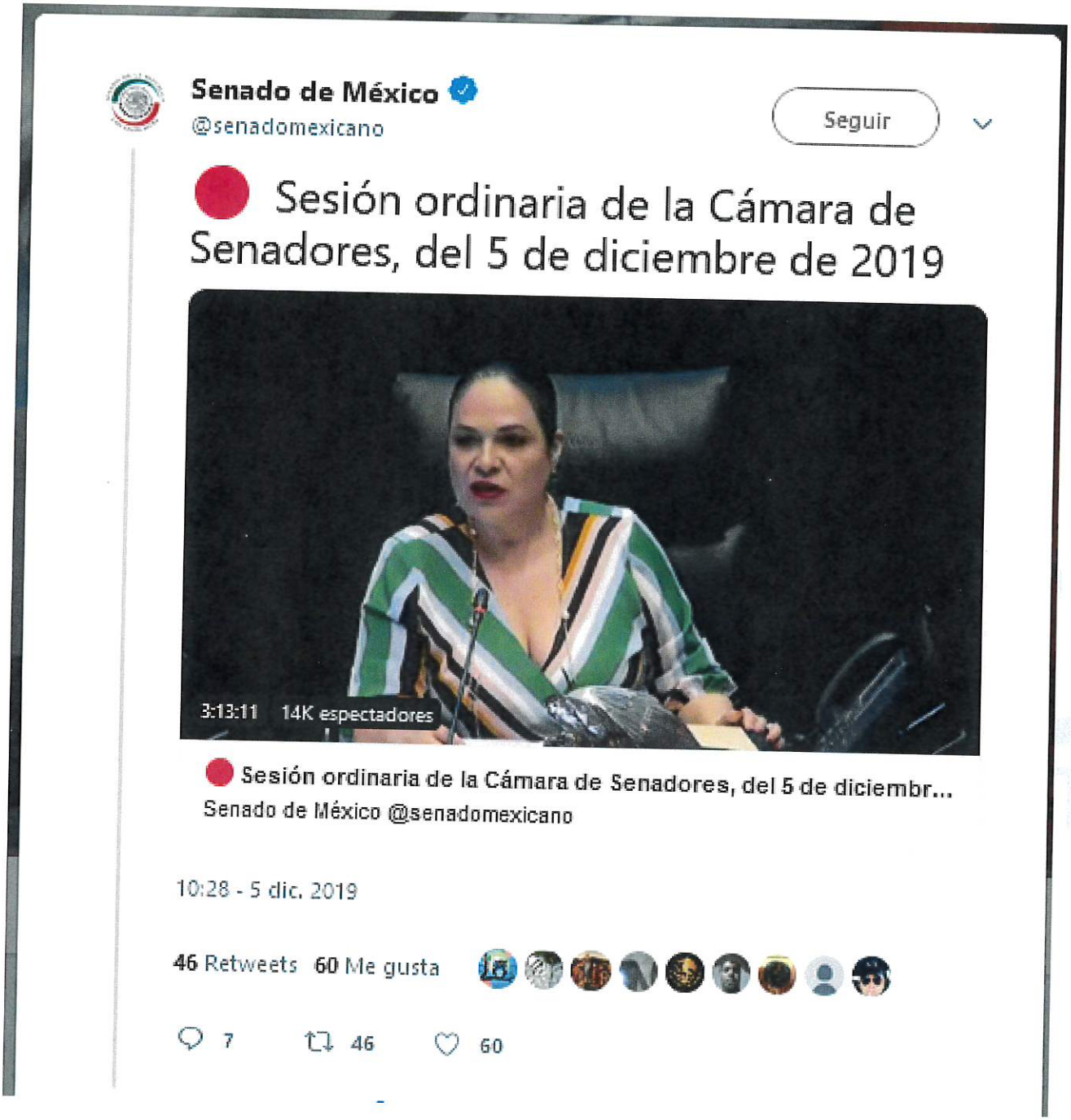
Seguir

Agradezco al @senadomexicano por haberme designado Ministra de la @SCJN, tras un proceso cívico y democrático, donde participé con otras destacadas abogadas que tienen el mayor de mis respetos y reconocimiento, @magalonik y @DianaAlvarez_M. Un gusto haber coincidido.

23:55 - 5 dic. 2019

1.159 Retweets **4.773** Me gusta

391 1,2K 4,8K



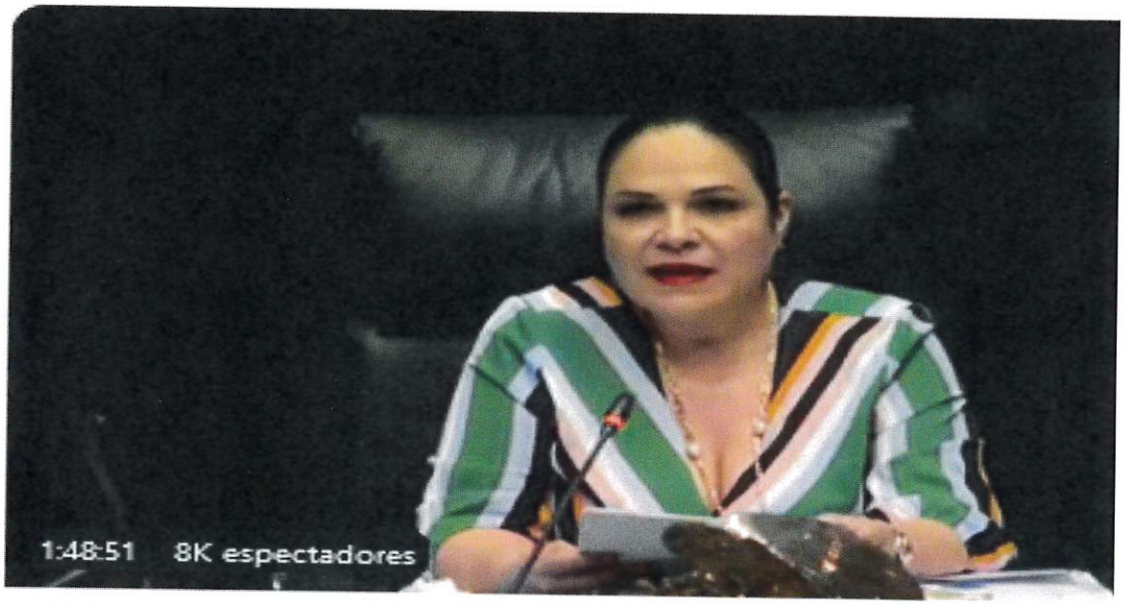
Senado de México @senadomexicano · 5 dic. 2019

Se declara receso.

6 6 19

Senado de México @senadomexicano · 5 dic. 2019

Segunda parte de la sesión ordinaria de la Cámara de Senad diciembre de 2019



Segunda parte de la sesión ordinaria de la Cámara de

Senado de México @senadomexicano

14 34 26

Senado de México @senadomexicano · 5 dic. 2019

La Secretaría de la Mesa Directiva informa que en la elección de la Ministra de la @SCJN se depositaron:

- 122 cédulas,
- 2 sobres vacíos y
- 2 objetos de papel

6 19 31

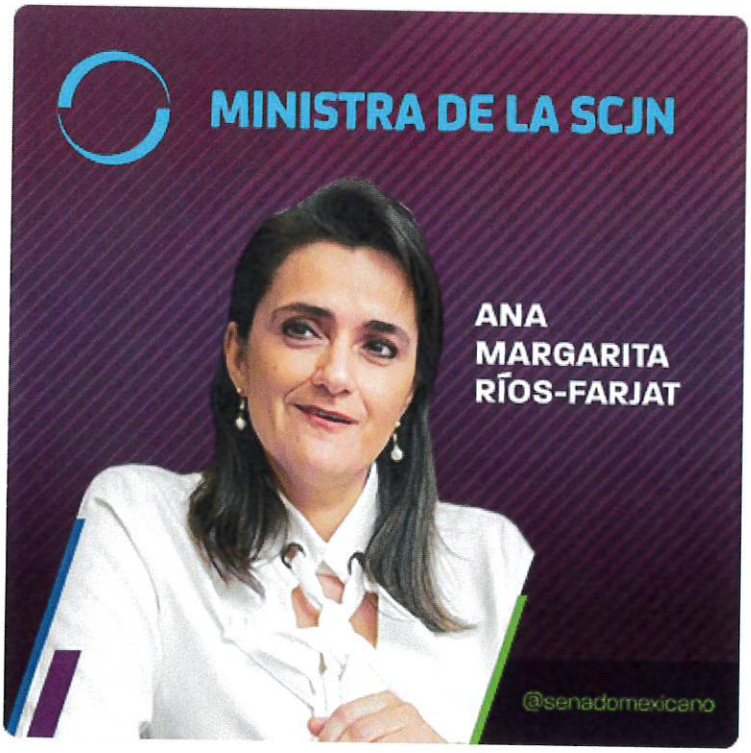
Senado de México @senadomexicano · 5 dic. 2019

✅ Se emitieron 122 votos:

- 1 @DianaAlvarez_M
- 25 @magalonik
- 94 @MargRiosFarjat

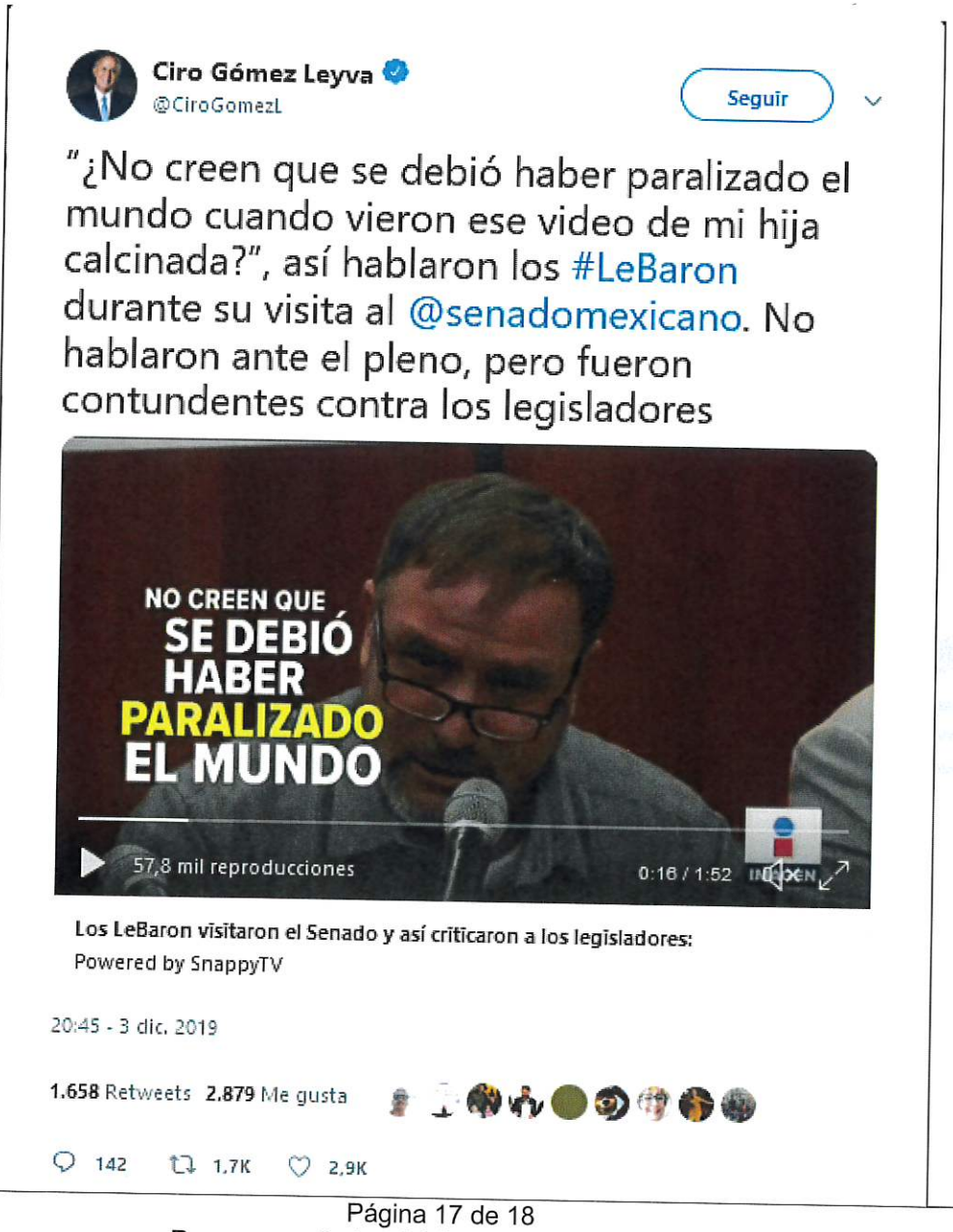
0 abstenciones y
2 votos nulos.

Con la aprobación de la mayoría calificada se elige a @MargRiosFarjat como Ministra de la @SCJN.



- **Visita de LeBarón al Senado de la República**

El 3 de diciembre Julián LeBarón visita al Senado de la Republica en una reunión de trabajo con el senador independiente Emilio Álvarez Icazo, llevaron una petición de justicia por el asesinato de sus familiares. Por su parte, Adrián LeBarón exigió al Senado que los ayude, y especialmente a la nueva la comisionada de la Comisión Nacional de Derechos Humanos (CNDH), Rosario Piedra



6. Conclusiones

Se encontraron diferentes publicaciones que afectan a grupos políticos, senadores en partícular y personas que laboral en el **Senado de la República**, sin embargo, no fueron encontrados hallazgos relevantes que puedan poner en riesgo la infraestructura tecnológica del **Senado de la República**.