TEMBIPORU MARANDU HA ÑEMOASÃIRÃ
Sãmbyhyha
Secretaría NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

TETÃ REKUÁI
GOBIERNO NACIONAL

Paraguay de la gente

INFORME DE COMISIONAMIENTO INTERNACIONAL/NACIONAL

Nombre y Apellido:	Gabriela Patti	Firma:
Dependencia:	CERT-PY	CI Nº: 2682754
Tipo de Funcionario	Permanente X Contratado ____ Comisionado ____ Particular ____	
Fecha de Comisionamiento:	DEL 28/11 AL 02/12	
Resolución N°	Senatics N° 11 / 18	
Evento y/o Misión (nombre, lugar)	Ciberseguridad y Procesos Democráticos, Oxford	
Temas tratados y/o actividades realizadas:	- Presentación de experiencias de diversos países - Análisis y debate sobre amenazas cibernéticas que afectan a procesos democráticos - compromisos y trabajos futuros	
Resultados:	Compromiso de impulsar iniciativas de ciberseguridad aplicados a proteger procesos de elecciones frente a amenazas ciber-neticas	
Compromisos asumidos:	//	
Se anexa copia del Certificado u otros Documentos	Si X (informe y agenda) No ___	
V° B° del Responsable de la Dependencia:	Firma Sello Aclaración Director Centro de Respuestas a Incidentes Tecnológicos	

SECRETARIA NACIONAL DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACION
PRESIDENCIA DE LA REPUBLICA
SENATICS
Asunción

Ciberseguridad de los Procesos Democráticos

Oxford, Reino Unido

29 de noviembre al 01 de diciembre 2018

La Organización de los Estados Americanos (OEA) y el Programa de Ciberseguridad del Foreign Offices del Reino Unido han organizado en conjunto el primer taller Regional **"Ciberseguridad y Procesos Democráticos"** en la Martin School de la Universidad de Oxford de Inglaterra. En el taller han participado responsables de procesos democráticos, centros de respuesta, expertos en ciberseguridad y representantes de la Academia, procedentes de América, Unión Europea y Commonwealth británica.

Se discutieron las diferentes amenazas cibernéticas que pueden afectar a los procesos democráticos, entendiendo que éstos no se limitan al dia de elecciones sino a todos los procesos y sistemas involucrados: registro de votantes, formación de opiniones, votaciones, conteos, etc. Se acordó que garantizar los procesos democráticos y protegerlos frente a los ataques que se producen en el ciberespacio son imprescindibles para garantizar el efectivo desarrollo democratico de las naciones. Las amenazas a nuestro sistema de convivencia democratico en el mundo digital son igual o más importantes aun que en el mundo fisico.

También se destacó que los procesos democráticos deben ser considerados parte de la infraestructura crítica de un país y su capacidad de recuperación. Se recomendó revisar la Declaración Cibernética del Commonwealth, el mayor compromiso intergubernamental del mundo con la cooperación en seguridad cibernética, que se considera una excelente base para las iniciativas que derivan del taller.

Diversos países contaron sus experiencias, buenas y malas, destacándose especialmente la de Reino Unido, los cuales centran sus esfuerzos para proteger los procesos de elecciones de la siguiente manera:

- Auditorías de los sistemas relacionados a los procesos de elecciones, tanto desde el punto de vista de la arquitectura como desde el punto de vista de la implementación (pentesting, evaluación de código, etc.)
- Protecciones ante denegación de servicio
- Asesoramiento, guías y talleres de ciberseguridad para todos los partidos políticos
- Ciberejercicios y simulacros multi-stakeholders relacionados a procesos de elecciones

Se presentó la experiencia Paraguaya, especialmente con respecto a incidentes cibernéticos ocurridos a mediados de 2012 en respuesta a un evento político, lo que disparó los primeros esfuerzos formales y permanentes en materia de ciberseguridad. También se destacó la influencia de amenazas cibernéticas como manipulación de información, explotación de vulnerabiliades, botnets, denegación de servicio y otros, los cuales han afectado a diversos procesos democráticos como por ejemplo el tratamiento de leyes, conteo mediante TREP, etc.

Se habló de la amenaza de la manipulación de información e informaciones o noticias falsas, sin embargo, luego del debate, la mayoría acordó que, si bien es un riesgo real y presente, el aspecto de ciberseguridad debería centrarse en los medios técnicos por los que estos se propagan o masifican, no en el contenido ni en las vulnerabilidades sociales que éstas explotan.

Se habló también de los diferentes tipos de sistemas de votación electrónico, tanto los asistidos electrónicos presenciales (máquinas de votación) y remotos (principalmente, voto por internet). Se habló de las vulnerabilidades técnicas y no técnicas que pueden afectar a estos tipos de sistemas, y las consideraciones que se deben tomar a la hora de decidirse por un sistema para una elección. Se destacó la experiencia de Noruega en primer lugar, seguido por Estonia, se recomendó empezar por pruebas piloto limitadas que consideren las características y los riesgos intrínsecos de cada país.

En febrero y marzo, se reunirán grupos de trabajo subregionales para continuar con el trabajo iniciado en este taller, con el objetivo de generar una guía o marco de trabajo común para la región acerca de cómo proteger los procesos democráticos, limitando el alcance a procesos de elecciones.

Gabriela Ratti

Ing. Gabriela Ratti
Dpto. Capacitación y Difusión
CERT-PY - SENATICs