

CARPETA TÉCNICA “CONSIDERACIONES DE APLICACIONES MÓVILES PARA LA MODALIDAD TRAE TU PROPIO DISPOSITIVO (BYOD)”

La XXIII Reunión del Comité Consultivo Permanente I: Telecomunicaciones/Tecnologías de la Información y la Comunicación (CCP.I),

RECONOCIENDO:

- a) Que el movimiento BYOD (Trae tu propio dispositivo) ha estallado en popularidad y cambiado la manera de trabajar de los empleados, dándoles más libertad para trabajar en cualquier lugar, en cualquier momento usando sus propios dispositivos;
- b) Que si bien las Aplicaciones Móviles son importantes desde el punto de vista social y económico y tienen la capacidad de transformar la manera de hacer negocios, los dispositivos móviles presentan desafíos específicos asociados con la seguridad y privacidad del consumidor;
- c) Que las redes corporativas hospedarán ahora dispositivos personales que no han cumplido nunca con ninguna configuración básica ni han sido evaluados en términos de riesgos de seguridad, comparados con dispositivos entregados por la empresa y en consecuencia el riesgo de amenazas como, entre otras, la instalación de software malicioso;
- d) La responsabilidad de los Estados no solo de promover el acceso a las tecnologías de la información y la comunicación (TICs) sino también de proteger el uso adecuado y su impacto en los usuarios,

CONSIDERANDO:

- a) Que el Punto 2 del mandato vigente del CCP.I aprobado por la V Reunión Ordinaria de la Asamblea de la CITEI establece que debe fomentarse y estimularse en la región el desarrollo de infraestructura de Telecomunicaciones/TIC;
- b) Que el software malicioso en la actualidad apunta a los datos independientemente del propietario. En el caso de empresas, puede llegar a dañar su reputación y eventualmente ocasionar pérdidas de ingresos; el tráfico clandestino de esta información resulta muy lucrativo a los delincuentes cibernéticos;
- c) Que al ingresar más desarrolladores al pujante mercado de las aplicaciones móviles, muchos de ellos no tienen el conocimiento o la capacitación para incorporar mejores prácticas en materia de seguridad como técnicas de codificación, incluidas las pruebas de vulnerabilidad;
- d) Que dado que el control se deja cada vez más en manos del usuario para que auto-gestione sus dispositivos, la exposición al riesgo y la posibilidad de compromiso jamás ha sido mayor;
- e) Que es de esencial importancia contar con una guía o manual regional que contenga las mejores prácticas y políticas de seguridad relacionadas con aplicaciones móviles BYOD,

¹ CCP.I-TIC/doc. 3145/13

TENIENDO EN CUENTA:

Que resulta beneficioso a los Estados Miembros de la CITEL y los Miembros Asociados mantenerse informados acerca del problema cada vez más acuciante de asegurar que se codifiquen, se prueben y se validen hasta un determinado nivel las aplicaciones móviles destinadas a procesar una Propiedad Intelectual (IP) corporativa, tanto por razones de seguridad, privacidad como de gobierno,

RESUELVE:

1. Aprobar la creación de una Carpeta Técnica sobre “Consideraciones de Aplicaciones Móviles para la Modalidad Trae Tu Propio Dispositivo (BYOD)”, en vista del problema cada vez más acuciante de asegurar que se codifiquen, se prueben y se validen hasta un determinado nivel las aplicaciones móviles destinadas a procesar Propiedad Intelectual corporativa tanto por razones de seguridad y privacidad como de gobierno. Se adjunta la estructura de la carpeta técnica en el Anexo de la presente Resolución.
2. Designar como coordinador de la presente Carpeta Técnica al Sr. Faud Khan de la administración de Canadá, quien se ocupará de reunir las contribuciones presentadas por los Estados Miembros y los Miembros Asociados y de actualizar la Carpeta Técnica.
3. Instar a los Estados Miembros y los Miembros Asociados a contribuir al contenido de la Carpeta y utilizarla con el fin de compartir información, concientizar y redactar documentos futuros sobre este tema.

ANEXO A LA RESOLUCIÓN CCP.I/RES. 220 (XXIII-13)

Contenido recomendado

ÍNDICE

Capítulo I: Seguridad en las Aplicaciones Móviles y el movimiento BYOD

Capítulo II: Software malicioso, pirateo y por qué esto ocurre

Capítulo III: Las empresas no logran proteger datos y dispositivos

Capítulo IV: Consideraciones

Capítulo V: Normas y Mejores Prácticas

Capítulo VI: Conclusiones y Recomendaciones

Apéndice A: Acrónimos y términos utilizados

Apéndice B: Artículos y libros sobre BYOD

Apéndice C: Estrategias de seguridad móvil específicas para cada país