CORTE SUPREMA DE JUSTICIA
MAGISTRADO

18 de agosto de 2016

Señores
Secretaria Permanente
Secretaría Pro-Tempore
Comisión Permanente de Coordinación y Seguimiento
CUMBRE JUDICIAL IBEROAMERICANA
S. D.

Estimados señores:

En atención a lo acordado en la cláusula 69 de la declaración final de la XVIII Edición de Cumbre Judicial Iberoamericana, cuya Asamblea Plenaria se llevó a cabo el pasado mes de abril en Asunción Paraguay, la cual reza:

> *"Proponemos la inclusión en la Primera Reunión Preparatoria, dada su trascendencia y actualidad, de los temas sobre la ciberseguridad y de la aparición de los ciberdelitos, cuyas particularidades los operadores de justicia han de estar debidamente instruidos."*

En representación del Grupo de "*e-Justicia: Tecnologías en los Poderes Judiciales*", me permito remitir la propuesta trabajada en conjunto, acerca del abordaje que se recomienda dar al tema de "*Ciberseguridad y Ciberdelincuencia*", en la presente edición de cumbre, a efectos de que se autorice su ejecución.

El objetivo del grupo es abordar los temas de Ciberseguridad y Ciberdelincuencia con dos enfoques diferentes ambos como subgrupos del Grupo e-Justicia. El primer grupo desarrollaría la temática acerca de la "*Ciberseguridad*", desde la perspectiva técnica de las Direcciones o Departamentos de Tecnología de las diferentes Instituciones que integran la Cumbre Judicial, creando una guía que facilite a los responsables de dichas

dependencias marcar la ruta en cuanto a estrategias de seguridad de la información custodiada en sus organizaciones, donde se trataría temas como:

1. Marco de control y cultura organizacional
2. Seguridad física
3. Refuerzo de la seguridad en los componentes de la plataforma tecnológica
4. Recursos específicos para el refuerzo de la seguridad informática.
5. Creación de red de alerta con los Poderes Judiciales miembros de Cumbre Judicial.

Se adjunta un primer borrador de documento de trabajo sobre Ciberseguridad que se propone para ser analizado y enriquecido por los países que integren el grupo de trabajo, para este grupo se recomienda la participación de especialistas técnicos con especialización en seguridad informática.

El segundo subgrupo, estaría integrado por operadores del Sistema Judicial, quienes se avocarían a atender la temática de "*Ciberdelincuencia*", desde una óptica técnico-jurídica, de forma tal que se generen insumos prácticos, que coadyuven en la comprensión y tratamiento de las diferentes actividades delictivas asociadas con los delitos informáticos. Con ello, se pretende fomentar un conocimiento base, que permita atender y entender de una mejor manera, aquellos casos que lleguen a estrados judiciales. Este grupo de trabajo podrá desarrollar:

1. Estudio de las regulaciones en delitos informáticos para cada uno de los países que integran la Cumbre Judicial, con el fin de precisar identidad y estandarización en los tipos penales, que permitan facilitar la cooperación jurídica internacional en la materia.

2. Guía técnico-jurídica que contenga elementos básicos para la comprensión de los delitos informáticos.

Tal y como se señaló anteriormente, ambos subgrupos están integrados dentro del ámbito de E-justicia.

Por otro parte, se propone dar continuidad al trabajo realizado por este grupo, el cual supera más de una década, mismo que se ve reflejado en las herramientas desarrolladas y que se encuentran unificadas en el "*Sistema Iberoamericano de E-Justicia*", el cual actualmente es administrado por el Poder Judicial de Nicaragua. En dicho sistema se podrá encontrar la red de puntos de contacto de Tecnologías de los Poderes Judiciales, la red de videoconferencias y sus puntos de contacto, la biblioteca de experiencias tecnológicas de los Poderes Judiciales miembros de Cumbre Judicial y las encuestas relativas a la implementación del Litigio electrónico. Asimismo, colaborar al país anfitrión en la logística de la Feria Tecnológica y la Revista e-Justicia que deberán ejecutarse en el marco de la Asamblea Plenaria de esta edición de cumbre.

Por último, se adjunta una propuesta de estatutos que regirían a este grupo de trabajo, el cual, por la dinámica del mismo, dado la innovación tecnológica, lo cambiante de las

tecnologías y su aplicación en los Poderes Judiciales, además del rol transversal que estas toman en los diferentes grupos de trabajo; se recomienda se convierta en una Comisión Permanente.

Luis Guillermo Rivas Loáiciga

Coordinador Grupo E-Justicia

ANEXO 1

PROPUESTA DE TRABAJO SOBRE SEGURIDAD INFORMATICA GRUPO E-JUSTICIA

Introducción

La seguridad informática busca garantizar la consistencia, integridad y confiabilidad de la información que se gestione a través de medios tecnológicos.

Se parte de la premisa de que no existe la seguridad informática al 100%. Bajo esta óptica, podemos dividir los esfuerzos en esta materia en dos tipos: los que van orientados a mantener la continuidad de los servicios y los que van orientados a recuperarse en el caso en que, a pesar de todos los esfuerzos realizados, se haya presentado una interrupción en los servicios.

El gasto en seguridad informática tiene un comportamiento asintótico con respecto a la mejora que se obtiene al incrementar la inversión en tecnología. Al principio se pueden realizar mejoras muy importantes con poca inversión pero conforme se avanza las mejoras que se obtienen son cada vez menores y para obtenerlas se requiere un mayor gasto.

Por más esfuerzo que se haga, aún la organización con mayor capital y mayores recursos tendrá aspectos susceptibles de mejora. El límite del gasto que se realiza en esta materia lo se define con base en una valoración costo – beneficio y en una adecuada administración de riesgos.

Este análisis debe realizarse tomando como base los diferentes marcos de normas y buenas prácticas entre los que pueden citarse las normas de la familia 27000 de ISO (http://www.iso27000.es/iso27000.html) y el marco de control COBIT en su última versión (http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx).

Se analizarán a continuación diferentes elementos que pueden integrarse en un esquema de seguridad informática. Como se indicó anteriormente este diseño debe maximizar el uso de los recursos disponibles alcanzando así el mayor grado de seguridad que la organización pueda sufragar.

La seguridad informática se ve como una serie de anillos concéntricos en cuyo centro se encuentra la información y cada anillo aporta un grado de seguridad en el campo de su especialidad.

Marco de control y cultura organizacional

El primer elemento de un esquema de seguridad informática es la cultura de los usuarios. Ningún esquema de seguridad, por más fuerte que sea puede compensar los descuidos y faltas que puedan tener los usuarios. Si los usuarios insisten en abrir correos maliciosos, ingresar a sitios dudosos o utilizar software ilegal, no hay forma de cerrar todos los portillos existentes por lo que mediante estas acciones pondrán en riesgo la seguridad informática de la organización.

Se requiere por tanto que se defina en primera instancia un marco de control, compuesto por políticas, procedimientos, reglamentos y sanciones apoyados y aprobados por la administración superior. Como se indicó anteriormente existe mucho camino adelantado en este sentido en los trabajos realizados por la ISO en su familia de normas 27000 y las recomendaciones de ISACA en los documentos de COBIT.

Pero además se requiere instruir al usuario en temas de seguridad informática de tal forma que tenga los elementos para valorar los riesgos a que se enfrenta y las posibles consecuencias de sus actos. Esto puede realizarse mediante diferentes formas tales como campañas de información sobre diferentes temas y cursos específicos.

Sin temor a equivocarse los esfuerzos que se realicen en estos temas cubren más del 50% del trabajo que implica la seguridad informática de la organización y la inversión requerida para su implementación es relativamente baja.

Seguridad física

Este aparte se refiere a elementos que, sin ser específicamente parte de la plataforma tecnológica, resulta de suma importancia para el funcionamiento de esta. Entre los elementos que se pueden mencionar están:

- Red eléctrica: Los equipos que componen la plataforma tecnológica requieren de energía eléctrica para su funcionamiento. Esta energía debe tener los niveles de calidad establecidos por los fabricantes para que los dispositivos no fallen. Pero además se requiere que el diseño de la red eléctrica soporte los equipos que se van a instalar en cada lugar, se requiere un adecuado sistema de tierras que tal forma que la electricidad sobrante se deseche por los canales apropiados y se requiere que la alimentación eléctrica sea continua lo cual implica la

necesidad de contar con sistemas de UPSs y plantas eléctricas que den continuidad al servicio en caso de algún corte en el fluido eléctrico.

- Sistemas de control ambiental: Los equipos informáticos operan en rangos de temperatura y humedad establecidos por los fabricantes. En los lugares donde estas condiciones no se cumplan, ya sea por las condiciones propias de la zona o porque se acumula una cantidad importante de equipos que en conjunto violan estos parámetros, se requiere contar con equipos de control ambiental especializados en equipo electrónico. Nuevamente, la continuidad del funcionamiento de la plataforma tecnológica depende de la continuidad de estos sistemas de control ambiental por lo que se requiere que los diseños garanticen esta operación constante
- Sistemas de vigilancia y alarmas: Existen riesgos que pueden controlarse en forma automática mediante la implementación de sistemas de vigilancia y alarmas en áreas específicas. Entre estos riesgos podemos mencionar los de intrusión, calor, incendio e inundación. También se pueden implementar sistemas de circuito cerrado de televisión con la finalidad de que se pueda ver en forma remota lo que sucede en las áreas sensibles de la plataforma tecnológica.
- Control de Acceso: El acceso a las áreas sensibles, es decir, aquellas áreas donde se ubica equipo clave cuya falla podría provocar discontinuidad en los servicios, debe estar controlado. Este control puede realizarse en forma manual o electrónica mediante llavines electrónicos y tarjetas codificadas, sin embargo, solo el personal autorizado debe ingresar a estas áreas.
- Extinción de incendio: Un incendio puede provocar daños cuantiosos en muy poco tiempo al equipo electrónico. El fuego debe controlarse en el menor tiempo posible provocando un daño mínimo a los equipos. Los sistemas tradicionales de extinción de incendios resultan inadecuados por lo que debe optarse por un sistema de extinción de incendios especial para equipo electrónico.
- Mantenimiento de todos estos sistemas: Todos los sistemas que garantizan la seguridad física de la plataforma tecnológica requieren de un adecuado mantenimiento. Sin este mantenimiento los sistemas se deteriorarán incrementando el riesgo de falla. Es imprescindible no solo contar con estos sistemas sino que además se debe programar su sostenibilidad.

Refuerzo de la seguridad en los componentes de la plataforma tecnológica

Cada elemento que compone la plataforma tecnológica ofrece posibilidades para incrementar esta seguridad que no se deben desaprovechar. Estas medidas forman parte de los esfuerzos de bajo costo y mucho impacto en el nivel de seguridad informática de la organización. A modo de ejemplo se pueden citar los siguientes elementos y esfuerzos:

- Equipos servidores: los dispositivos en los que se ejecutan los servicios deben estar diseñados para tal fin. Dejando de lado las características de rendimiento que deben exhibir, deben contar con duplicidad en sus componentes críticos (procesadores, fuentes de poder, tarjetas de comunicación, etc., almacenamiento)
- Sistema operativo de los servidores: En primer lugar, el sistema operativo de los servidores controla el acceso a los recursos; como premisa se tiene que nadie debe tener acceso a un recurso que no necesita ni a privilegios de uso que no necesita. Pero además los sistemas operativos permiten la implementación de mecanismos adicionales que refuerzan la seguridad informática como pueden ser mecanismos de replicación de información o incluso servicios. Deben conocerse e implementarse los mecanismos que mayor beneficio aporten.
- Hipervisores: La virtualización permite agregar una capa adicional de seguridad informática ya que facilitan mecanismos que permiten incrementar la continuidad de los equipos virtuales y en dado caso reducen el tiempo de su recuperación. Pero además permiten una mayor visibilidad en la administración de recursos lo que los faculta para realizar ajustes automáticos a la plataforma que mejoran su desempeño al tiempo que incrementan la continuidad de los servicios. También permiten la implementación de esquemas de intercomunicación de diferentes sitios con lo que se posibilita un mecanismo contingente en caso de una falla de nivel catastrófico de un sitio.
- Dispositivos de almacenamiento: El fin último de la seguridad informática es proteger la información de la organización. No es de sorprender que los dispositivos que almacenan esta información resulten cada vez más sofisticados y confiables, sin embargo, es importante conocer e implementar todas las facilidades que permitan estos equipos. Como ejemplos de estos mecanismos se pueden citar los diferentes arregles de discos, la duplicidad de componentes y las facilidades para replicación de información.
- Bases de datos: Los motores de bases de datos funcionan como contenedores de la información de tal forma que no se puede acceder a esta sino es a través suyo. Para este fin estos productos implementan mecanismos que refuerzan la seguridad tales como administración de privilegios, filtrado de la información a través de vistas, integridad referencial, encripción tanto en el almacenamiento como en la comunicación, replicación y respaldo de la información. Deben habilitarse tantos mecanismos de seguridad como sea posible.
- Dispositivos de red: Los switches, enrutadores, puntos de acceso y otros dispositivos permiten el acceso a los equipos en los que se almacena la información. Esta función les permite también proveer mecanismos de seguridad que impiden que se utilicen equipos, protocolos o mecanismos para accesar información en forma indebida. Entre estos mecanismos podemos citar las VLANs en los switches, las listas de acceso en switches y enrutadores y hasta el propio diseño de la red en sus diferentes capas.
- Sistemas: Dependiendo de la forma en la que se desarrollen los sistemas informáticos de la organización el código fuente de estos puede constituirse en

una debilidad o en una fortaleza. Existen múltiples ataques informáticos que aprovechan descuidos en los programas entre los que se pueden citar la inyección SQL y la ingeniería reversa. Es importante que los desarrolladores apliquen buenas prácticas de programación para que sus sistemas formen parte de los muros que protegen la información de la organización. Otro aspecto importante a tener en cuenta es la actualización constante del código; programas desactualizados utilizan componentes desactualizados y potencialmente vulnerables por lo que el código debe estar en constante revisión con el fin de mantenerlo lo más actualizado posible.

- Equipos terminales del usuario: Los equipos terminales son un elemento que comúnmente se descuida y se constituye en punto de falla de la seguridad informática. Debe limitarse lo que el usuario pueda hacer con este de tal forma que un descuido de su parte no comprometa, en la medida de las posibilidades, la seguridad informática de la organización. Deben además deshabilitarse todos los elementos que no se usen ya que, en su configuración de fábrica podrían resultar de fácil acceso. También deben habilitarse mecanismos que mejoren la confiabilidad de los equipos, tal es el caso de los discos duros en espejo para evitar pérdidas de información en las computadoras. Es importante aclarar que en este aparte se incluyen también equipos como impresoras que se conectan a la red y que podrían tener habilitados protocolos o servicios que permitan la conexión a la red de un delincuente informático. En este sentido se recomienda estandarizar lo más posible y definir claramente la configuración que cada tipo de dispositivo deba tener.
- Mecanismos de respaldos: El buen uso de estos recursos reduce sustancialmente la pérdida de información. En la actualidad existen múltiples opciones que permiten llevar los tiempos de pérdida de información y de recuperación a valores muy razonables, sin embargo, mientras más eficientes sean estos mecanismos más costosos serán por lo que la organización deberá determinar cuál es el que puede costear y administrar el riesgo residual.
- Sistemas de monitoreo:

Recursos específicos para el refuerzo de la seguridad informática

Además de la seguridad que se puede implementar propiamente con los componentes de la plataforma tecnológica de la institución existen una serie de recursos que se adicionan específicamente para solventar debilidades en materia de seguridad informática. Algunos de estos recursos resultan onerosos para muchas organizaciones sin embargo debe valorarse su uso, aún y cuando se limite a áreas muy críticas de la plataforma. Entre estos recursos se puede mencionar:

- Firewall: Estos dispositivos, también conocidos como paredes de fuego, trabajan por denegación por omisión, es decir, lo que no está expresamente autorizado está denegado. Se utilizan para controlar el flujo de información entre dos redes o segmentos de estas. Existen firewalls que trabajan en capas 3 y 4 y otros que trabajan a nivel de aplicación en la capa 7 del modelo OSI. La gama de opciones para un dispositivo de este tipo va desde uno hecho con una PC con dos o más tarjetas de red y una distribución de Linux hasta los más sofisticados que reconocen mediante inteligencia artificial posibles ataques y los repelen. Algunos tienen, previo contrato de servicio, conexión con el fabricante para que este alimente y actualice las firmas (patrones de ataques que reconoce el dispositivo) y las diferentes listas de sitios potencialmente peligrosos para que el administrador defina si se bloquea o se permite el acceso a esos sitios. El fin último de un firewall es permitir el tráfico estrictamente necesario y su efectividad estará en relación directa con la habilidad de su administrador.
- Antimalware: Los delincuentes informáticos generan software que, una vez que ha ingresado en la organización, puede ejecutar diferentes acciones, desde borrar información hasta dar acceso al hacker para que tome control del equipo en que se instaló. Para evitar este riesgo existen productos que se encargan de revisar en cada equipo de la plataforma el software que ingresa. Para que este esquema sea efectivo el software debe estarse actualizando constantemente para incorporar las nuevas amenazas que van surgiendo y para incorporar mejoras a su funcionamiento y efectividad. Estos productos consumen un porcentaje importante de la capacidad de cómputo de los equipos y también tienen un consumo significativo de ancho de banda en la red por lo que su correcta administración resulta crucial para que se constituyan en una solución y no en un problema.
- Antispam: Mención aparte merece el recurso que se encarga de evitar que ingrese correo basura a la organización. Este correo es molesto, consume recursos de red, de almacenamiento y de procesamiento y podrían presentar patrones virales que lo faculten a reproducirse con lo cual se agravan los problemas indicados y además se compromete la credibilidad de la organización al convertirla en fuente de correos indeseados.
- Análisis de vulnerabilidades: Los diferentes productos de software que se instalan en los equipos que componen la plataforma de la organización no son perfectos. Con el paso del tiempo se detectan fallos que los delincuentes informáticos pueden utilizar para sobrepasar los mecanismos de seguridad que se hayan establecido. Estos fallos se conocen como vulnerabilidades. Encontrar y reparar estas vulnerabilidades es una labor titánica por lo que se han desarrollado productos que buscan, con base en la información que publican los distintos fabricantes, estas vulnerabilidades y las informan a tiempo junto con una recomendación para su reparación de tal forma que se hace posible mantener el nivel de vulnerabilidad de los equipos en un rango aceptable.
- Prevención de intrusos: Dado que no se puede asumir que los esquemas de seguridad, en ningún caso, son impenetrables, siempre existe la posibilidad de

que un delincuente informático vulnere esas defensas y logre llegar hasta los dispositivos críticos de la organización. Los sistemas de prevención de intrusos contemplan esta posibilidad e incorporan mecanismos para detectar y repeler el acceso de intrusos a los dispositivos clave.

- Administrador de contenidos: A pesar de las advertencias y capacitaciones los usuarios podrían por alguna razón terminar tratando de ingresar a un sitio en internet inadecuado, ya sea por su contenido o porque representa un riesgo potencial para la seguridad informática de la organización. Mediante la administración de contenidos los sitios que se pueden accesar se pueden limitar conforme a las políticas organizaciones evitando riesgos y pérdida de tiempo laboral.
- Correlación de eventos: La mayoría de los dispositivos de la plataforma tecnológica de la organización generan eventos que en forma aislada podrían no dar mayor información pero que si se correlacionan con los que generan otros dispositivos podrían indicar la materialización de algún riesgo. Este tipo de productos buscan recolectar los eventos que generan los distintos dispositivos y realizar una correlación para determinar comportamientos que de otra forma pasarían inadvertidos.

Conclusión

Se han presentado distintos puntos y recursos que pueden ayudar a mejorar el nivel de seguridad en una organización.

En ningún caso estas listas pueden considerarse exhaustivas ni estáticas. Existen otros elementos que podrían mencionarse y además es un mundo en constante evolución por lo que se requiere una constante actualización, sin embargo los elementos mencionados han resultado de consideración por mucho tiempo en el tema y son ejemplos de la complejidad y magnitud de la tarea que implica la seguridad informática de una organización.

No existe la seguridad al 100% sin embargo toda organización está en la obligación de realizar su mejor esfuerzo cubriendo el mayor porcentaje posible con los recursos que pueda asignar al tema. Al respecto se puede observar que existen elementos cuyo costo es manejable por lo que no habría pretexto para no implementarlos, mientras que hay otros que, aunque deseables podrían caer fuera del presupuesto por lo que debe analizarse bien la posibilidad de aplicarlos aunque sea en forma parcial.

La sostenibilidad del esquema resulta, igual que en otras áreas de suma importancia. De nada sirve realizar el esfuerzo inicial para implementar un producto si no se puede dar sostenibilidad al esfuerzo una vez realizado.

La principal fuente de riesgos para la seguridad informática está en el usuario mismo, sin embargo, está también es la fuente cuya prevención requiere un menor esfuerzo y una menor cantidad de recursos por lo que debe en todo momento ser una de las principales prioridades.

La seguridad informática constituye un sistema de componentes que interactúan para proteger la información que se gestiona a través de la plataforma tecnológica. Los componentes y el diseño de la solución son propios de cada organización y de sus posibilidades y necesidades, sin embargo, en todo momento, la maximización del costo – beneficio de los recursos es clave y para esto deben seguirse las normas y buenas prácticas existentes con el fin de no duplicar esfuerzos que ya se han realizado.

La delincuencia informática no reconoce fronteras; esto permite concluir que lo que afecte a una organización muy posiblemente esté afectando a las otras. Los esfuerzos de los equipos encargados de la seguridad informática en cada organización deben tener una estrecha coordinación con los de sus pares con el fin de compartir información y generar sinergia en la solución de las distintas situaciones que deban enfrentar.

ANEXO 2

PROPUESTA DE NORMAS COMISION PERMANENTE DE E-JUSTICIA

(TECNOLOGÍAS EN LOS PODER JUDICIALES DE IBEROAMERICA)

1. PREAMBULO

   El proceso jurisdiccional y la administración de justicia son herramientas para tomar la decisión de un caso controvertido sometido al juez para restablecer un derecho violado. Las partes argumentan y gestionan ante el juez quien dicta resoluciones y decide el asunto. Ese intercambio de opiniones y gestiones se realiza mediante el uso de la palabra escrita o hablada. El juez escucha, contrasta y decide. La máquina de escribir fue una tecnología que aumentó la velocidad de la decisión porque permitía registrar la palabra hablada con mayor rapidez. La computación, la digitalización, la informática, la grabación, la transmisión a distancia, el análisis de datos, la inteligencia artificial, los artefactos voladores no tripulados, los drones, la nube, son nuevas tecnologías que se desarrollan a velocidad vertiginosa y se adaptan completamente a la actividad jurisdiccional. Ya su uso impacta esa tarea y apenas empezamos a entender todos los usos que pueden dársele en la tramitación y decisión judicial. La llamada cuarta revolución industrial impactará de forma total lo judicial, vemos información acerca de la robotización que permite decisiones sencillas y repetitivas que multiplicaría el número resoluciones y el anuncio del impacto en la labor abogadil, que se anuncia en opiniones sobre profesiones del futuro que sufrirán impactos por la aplicación de las nuevas tecnologías. Los Poderes Judiciales deben enfrentar ya la incorporación inevitable de ese futuro que ya está aquí para que la transición sea positiva y beneficiosa para los usuarios. De ahí la importancia de este tema en las Cumbres de Presidentes de Cortes de Iberoamérica por su obligación de prever la adopción y adaptación de esos nuevos aparatos, en la tramitación, pero también en los principios y filosofía de la ciencia, del arte de resolver conflictos.

2. NATURALEZA

   La Comisión de E-Justicia (Tecnologías en los Poderes Judiciales) de Cumbre Judicial Iberoamericana es un órgano dependiente de la Asamblea Plenaria de la Cumbre Judicial Iberoamericana cuyo objetivo es apoyar a los Poderes Judiciales con guías que marquen el Desarrollo y uso de las nuevas tecnologías en quehacer judicial y de sus áreas de apoyo, marcando una ruta de adopción de tecnologías que garantice la innovación, la mejora continua de los procesos, el acceso por medios electrónicos a la justicia, la seguridad de la información y cualquier otro aspecto relacionado.

3. OBJETIVOS GENERALES
   a. Proponer guías de desarrollo tecnológico para los poderes judiciales miembros de cumbre judicial.
   b. Impulsar la innovación y el uso de las herramientas tecnológicas como apoyo en la mejora de los procesos judiciales y las áreas de apoyo, así como en el acceso a la justicia.
   c. Impulsar el uso de buenas prácticas y el compartimiento de experiencias en materia tecnológica entre los Poderes Judiciales de Iberoamérica.

4. FUNCIONES
    a. Impulsar la innovación y el uso de las tecnologías como instrumentos de apoyo a la función judicial y de las áreas de apoyo de las mismas, así como impulsar el acceso a la justicia haciendo uso de las nuevas tecnologías, para lo cual se crearan Guías que deberán irse renovando conforme el avance en las tecnologías.
    b. Asesorar sobre temas diversos que impliquen el uso de las Tecnologías y que los grupos de trabajo deberán ir proponiendo conforme evolucionen las tecnologías.
    c. Apoyar a los países anfitriones de las reuniones plenarias en la coordinación de las ediciones de Feria Tecnológica y la Revista de E-justicia. Ambos producto de este grupo de trabajo.
    d. Velar por la actualización del Sistema Iberoamericano de e-justicia.
    e. Fungir como eje transversal de apoyo a los demás grupos de Trabajo de Cumbre Judicial, cuando el proyecto contenga algún componente tecnológico.

5. COMPOSICION

    La Comisión Permanente de E-justicia, estará constituida por los países que deseen formar parte de la misma (no existe límite de integrantes), adquiriendo en el momento de su postulación la responsabilidad y compromiso de trabajo en equipo para cumplir con los planes de trabajo del grupo para ese periodo.

6. OBLIGACIONES DE LOS INTEGRANTES

    Los miembros integrantes se comprometen a:
    a. Participar en las actividades organizadas por el grupo, las cuales se llevaran a
    b. cabo preferentemente a través de la utilización de los medios tecnológicos disponibles.
    c. Difundir y hacer uso de las herramientas tecnológicas desarrolladas dentro del grupo e-justicia.
    d. Dentro de los planes de trabajo establecidos en cada periodo, asumir la responsabilidad por la ejecución los planes de acción, recomendaciones y políticas establecidas.
    e. informar a la presidencia periódicamente sobre los logros obtenidos en los compromisos adquiridos.
    f.

7. PRESIDENCIA y SECRETARIA TECNICA

    En la primera reunión que celebre la Comision, se designara un Presidente o Presidenta de la Comisión quien además asumirá la Secretaria Técnica, cuyo mandato será por una edición de cumbre con posibilidad de reelección.

    Las funciones de la presidencia serán, entre otras:
    a. Presidir las sesiones de trabajo de la Comisión.
    b. Representar a la Comision ante las demás instancias de la Cumbre Judicial.
    c. Convocar a reuniones ordinarias y extraordinarias de la Comisión.
    d. Recibir, tramitar y archivar las solicitudes de asesoría, consultas o cualquier otro requerimiento que se formule.
    e. Ejecutar acuerdos adoptados por la Comisión.
    f. Dar Seguimiento al uso de las herramientas desarrolladas por los grupos de trabajo así como mantener actualizada la base de datos de contactos de

Directores y Directoras de Tecnología así como de los puntos de contacto de la red de Videoconferencias.

g. Velar por la actualización del Sistema Iberoamericano de E-justicia, así como por la comunicación de las novedades en el mismo.
h. Coordinar los trabajos de la comisión con las Secretarias Permanente y protempore , así como la Comisión Permanente de coordinación y seguimiento.
i. Suscribir, en representación de la Comision, los informes escritos que presente a la asamblea Plenaria u a la comisión Permanente de Coordinación y Seguimiento.
j. Elaborar las actas de las reuniones ordinarias y extraordinarias de la Comision y remitirlas a la Secretaria Permanente de la Cumbre y a la Comisión de Coordinación y Seguimiento.
k. Proponer, dar seguimiento y socializar los planes de trabajo de la Comisión para el periodo de vigencia.

8. REUNIONES

Se realizaran conforme a los requerimientos del plan de trabajo. Cuando los temas los permitan se realizara una combinación entre reuniones virtuales y reuniones presenciales.

9. OBSERVADORES

Se podrá invitar como observadores a las actividades que se estimen convenientes, a
Representantes de instituciones de derecho público o privado vinculados con el sector
Justicia y tecnología, profesionales, personas usuarias, organismos no gubernamentales representantes del sector académico y de investigación y agrupaciones comunitarias. Del ámbito tecnológico.

10. ENMIENDAS

Estas normas de funcionamiento podrán ser enmendadas por la Asamblea Plenaria, a petición de la propia Comisión de E-justicia o de la Comisión de Coordinación de Seguimiento.

1. ENTRADA EN VIGOR

El presente Estatuto entrará en vigor a partir del mismo día de su aprobación en la Asamblea Plenaria de la XXXXXXXCumbre Judicial Iberoamericana.