**San José, 30 de setiembre de 2020**

**N° 9109-2020**

**Al contestar refiérase a este # de oficio**

**Señora**

**Dra. Sandra Zúñiga Morales, Coordinadora**

**Sub Comisión de Alto Nivel de Ciberdelincuencia**

**y Ciberseguridad del Poder Judicial**

**Estimada señora:**

Muy respetuosamente, le transcribo el acuerdo tomado por la Corte Plena, en la sesión **N° 50-2020** celebrada **el 7 de setiembre del año en curso**, que literalmente dice:

“**ARTÍCULO XV**

**Documento 6983-2020 y 8386-2020**

La magistrada Sandra Zúñiga Morales en su condición de Coordinadora de la Sub Comisión de Alto Nivel de Ciberdelincuencia y Ciberseguridad del Poder Judicial, en oficio N° C-CDCS-01-2020 del 12 de junio del 2020, manifestó:

“En mi condición de Coordinadora de la Comisión de Alto Nivel de Ciberseguridad y Cibercrimen del Poder Judicial, remito la presente *“Ficha técnica para las iniciativas de Ciberseguridad en el Poder Judicial”,* que consiste en una propuesta de trabajo de la referida comisión para el periodo 2020 a 2021, con la finalidad de que sea sometido a consideración de Corte Plena.

En razón de lo anterior, solicito asignar un espacio en agenda para un ejercicio de concientización en torno a temas de ciberseguridad, y la presentación del programa de trabajo para los próximos dos años, que hemos coordinado con funcionarios de la Dirección de Tecnologías de la Información”

- 0 -

Ficha técnica para las iniciativas de

Ciberseguridad en el Poder Judicial

Periodo 2020-2022

|  |
| --- |
| **Información general** |
| Nombre de tema: | Promover y fomentar la ciberseguridad en la infraestructura tecnológica del Poder Judicial. |
| Objetivo de Comisión de Ciberseguridad y Ciberdelincuenciadel Poder JudicialPropuesta focalizada en ciberseguridad.  | Fomentar las mejores prácticas de protección, acceso y resguardo de la información cibernética que permita mantener su confidencialidad, disponibilidad e integridad y de esa manera disminuir la materialización de eventos que puedan poner en riesgo la información sensible de la Institución.Promover y realizar campañas de ciberseguridad a la población Judicial, con el fin de fortalecer la cultura organizacional en temas de seguridad de la información.Promover la colaboración, coordinación y sinergia en temas de ciberseguridad entre el Poder Judicial y otras instituciones, así como entes internacionales.Proponer acciones para mejorar dentro del Poder Judicial la protección, acceso y resguardo de la información que permita mantener la confidencialidad, disponibilidad e integridad de la información sensible de la Institución. |
| Alineamiento con los Objetivos del Desarrollo Sostenible (ODS) y la Agenda 2030 | Objetivos número 9, 16 y 17. |
| Comisión que coordina: | Comisión de Ciberseguridad y Ciberdelincuencia |
| Nombre de la persona que coordina: | Dra. Sandra Eugenia Zúñiga Morales, Magistrada de la Sala de Casación Penal, y Coordinadora de la Comisión de Ciberseguridad y Ciberdelincuencia.   |
| Puntos de contacto: | Sandra Zúñiga Morales, Magistrada Sala TerceraJuan Carlos Cubillo Miranda, Sub Jefe Ministerio PúblicoWalter Espinoza Espinoza, Director del Organismo de Investigación Judicial  |
| Correo Electrónico: | szuniga@poder-judicial.go.crjcubillo@poder-judicial.go.crwespinoza@poder-judicial.go.cr |
| Teléfono: | (506) 2295-4987  (506) 2295-4077 (506) 2295-4070(506) 2256-3503  |
| Periodo de trabajo de la actual propuesta: | 2020-2021 |

1. **Contextualización**

Consta en acta de Corte Plena N°34, del 5 de diciembre de 2016, la creación de la Comisión de alto nivel, denominada “Comisión de Ciberseguridad y Ciberdelincuencia del Poder Judicial”, conformada por los jerarcas de la Fiscalía General de la República, el Organismo de Investigación Judicial, o las personas a quienes dichas jefaturas designen; así como un Magistrado o Magistrada de la Sala Tercera, con el acompañamiento técnico de la Dirección de la Tecnología de la Información.  El propósito planteado era fortalecer el sistema judicial con los mecanismos idóneos para generar acciones de seguridad cibernéticas, que de manera preventiva resguarden los activos institucionales mediante una política de ciberseguridad, así como por otra parte, enfrentar de forma más eficiente la lucha contra la ciberdelincuencia, de ahí que se planteó fortalecer al Ministerio Público en la generación de políticas, directrices y procedimientos para el abordaje idóneo de ese tipo de delincuencia.

A partir de su creación surgen proyectos de interés, muy específicos, como fue a nivel internacional el impulso a una política de cooperación entre varios países que concluyó con la publicación de la Ley de Adhesión al Convenio sobre Ciberdelincuencia, conocido como Convenio de Budapest, de donde surgen posteriormente otras iniciativas, como es lo relacionado con la responsabilidad penal de las personas jurídicas.

Otros proyectos también se mencionaron estos años atrás, entre ellos un proyecto de Convenio Marco de Cooperación Interinstitucional entre el Colegio de Profesionales en Informática y Computación, con el Poder Judicial o, la búsqueda de un cambio en el procedimiento de apertura y respaldo de la evidencia digital; iniciativas aisladas, no articuladas dentro de un programa de trabajo y que incluso, finalmente no han generado resultados de impacto en los objetivos planteados, pero que es necesario retomar a través de un esfuerzo y una agenda coordinada.  En ese sentido, la Comisión de Ciberdelincuencia y Ciberseguridad, somete a consideración un plan de trabajo con acciones para los próximos dos años, con el fin de cumplir los objetivos que justificaron su creación y sobre todo, con el propósito de coadyuvar en asegurar la infraestructura crítica de la institución.

El Poder Judicial cuenta ya con una *“Política de Seguridad de la Información”*, la propuesta que se pretende realizar busca reforzar y mejorar la postura institucional expresada en dicha política, a través de la ejecución de varias actividades tendientes a la salvaguarda de la red y los servicios tecnológicos que brinda el Poder Judicial (iteracción).

Con estas actividades se busca impactar en la conciencia sobre la importancia vital que tiene hoy día la seguridad tecnológica de la institución, captando y ejecutando proyectos que a corto y mediano plazo impliquen acciones concretas para mantener la seguridad, disponibilidad e integridad de la información cibernética.

Para tales efectos se desea gestionar la seguridad a nivel de personas, procesos y tecnología, a lo interno de la organización, pero además se pretende realizar una gestión en seguridad externa, enfocada en la necesidad de llevar a cabo diálogos, acuerdos y alianzas estratégicas con otros agentes.

El objetivo final que se pretende alcanzar es que la institución sea capaz de gestionar personas, tecnologías y procesos, para conseguir el nivel de integridad, confidencialidad y disponibilidad que requiere la organización, alcanzando un riesgo aceptable y siendo resilientes.

A continuación, se hace una propuesta de dos años de trabajo sobre diversos proyectos de impacto, en especial, en el ámbito de la Dirección de Tecnologías de Información y Comunicación (DTIC) y áreas tecnológicas del OIJ; sin que esas actividades plasmadas en el presente documento, sean las únicas, pero sí las que desde esta Comisión se pondrán en marca, en un esfuerzo que deberá ser coordinado con otras desarrolladas a nivel institucional.

Del mismo modo, es importante indicar que para el presente proceso se realiza una categorización de las prácticas claves de gestión que lo conforman, dado que al realizar el análisis se identificó que no existe una relación entre ellas. Por lo anterior, se clasifican como servicios o controles que se deben aplicar para la seguridad de la información institucional.

La clasificación en las que se dividieron las prácticas claves de gestión, son las siguientes:

* + **Gobernanza**

Los servicios de la estrategia cibernética buscan unificar la necesidad de asegurar y apoyar la innovación tecnológica requerida por el Poder Judicial y la transición a un programa de riesgo cibernético, dirigido por la alta administración que equilibra los requisitos para ser seguro, vigilante y resiliente en línea con los niveles aceptables de riesgo.

* + **Aseguramiento**

Estar seguro significa tener controles con prioridad de riesgo para defender activos críticos contra amenazas conocidas y emergentes. Los servicios relacionados al aseguramiento de la información, ayudan a establecer controles centrados en el riesgo en torno a sus activos más sensibles, equilibrando la necesidad de reducir el riesgo y al mismo tiempo permiten la productividad, el cumplimiento de objetivos y la optimización de costos.

* + **Vigilancia**

Estar atento significa tener capacidades de detección y amenazas para anticipar e identificar proactivamente los ataques cibernéticos reales o potenciales. A medida que se vuelve cada vez más difícil prevenir las infiltraciones y las actividades no autorizadas, las organizaciones necesitan soluciones de detección de amenazas y detección avanzada para identificar rápidamente las actividades anómalas en sus entornos. Los servicios relacionados a la vigilancia brindan capacidades avanzadas de inteligencia de amenazas cibernéticas, monitoreo de amenazas, búsqueda de amenazas y análisis de seguridad para ayudar a proteger sus activos más críticos.

* + **Resiliencia**

Ser resiliente permite que las operaciones de una organización se adapten y respondan rápidamente a cambios dinámicos internos o externos (oportunidades, demandas, interrupciones o amenazas) y continúen las operaciones con un impacto menor. Esto incluye una combinación de muchos procesos tradicionales y nuevos, de las tecnologías existentes y las novedosas. Un programa organizacional integral y resistente, requiere la supervisión y la gobernanza correcta para integrarse y coordinarse con múltiples partes interesadas en los entornos de las operaciones organizacionales, la tecnología, la estrategia, el riesgo y el cumplimiento.

Sobre los cuatro ejes antes descritos, en mayo del 2018, la Presidencia Pro Témpore del Consejo asistió a la LXVI reunión ordinaria de la Comisión de Seguridad de Centroamérica, en donde se reafirmó el compromiso de desarrollar de manera conjunta los temas previamente mencionados.



1. **Justificación**

El dinámico ambiente del mundo, exige que se adopten mecanismos que se ajusten a las nuevas amenazas en el ciberespacio, lo que resulta aplicable también en materia de seguridad, pues con el paso del tiempo han ido surgiendo nuevos eventos delictivos e innovadoras formas de comisión de los ilícitos “clásicos” (en modalidades más complejas, que en muchas ocasiones, mutan a delincuencia organizada), panorama que hace imperativo el desarrollo de gestiones que correlativamente respondan a la necesidad de reaccionar para asegurar las infraestructuras críticas (compuesta por todos los equipos tecnológicos, así como servicios que mantiene y brinda la institución), garantizando el combate a toda esa serie de amenazas o agresiones.

De ahí, el requerimiento de desarrollar estrategias de ciberseguridad para la protección y resguardo de la información institucional, por cuanto resulta de vital importancia que los diferentes actores tomen conciencia sobre la necesidad de fortalecer la protección, acceso y resguardo de la información.

Además se debe destacar que para cumplir con los objetivos propuestos se requiere de la correspondiente dotación de contenido presupuestario, a fin de proporcionar a la institución nuevas tecnologías, capacitación y personal técnico especializado, pero además, se deben generar acuerdos y mecanismos de cooperación con otros actores del ámbito nacional y entidades internacionales.

1. **Objetivos**
	* Objetivo general

Promover e impulsar la protección y resguardo de la información institucional dentro de los niveles aceptables de riesgo, de acuerdo con el Sistema de Gestión de Seguridad de la Información (SGSI) y su política (ver anexo “PJ-SGSI-Política de seguridad de la información 27-01-2020.pdf”).



* + **Objetivos específicos**
* Conocer y tratar los riesgos estratégicos y operacionales de seguridad de la información y continuidad de los servicios brindados por la institución para que se mantengan en un nivel aceptable, incluyendo aquellos relacionados con el cumplimiento de las legislaciones y regulaciones aplicables.
* Trazar una ruta de trabajo que permita determinar los riesgos estratégicos y operacionales de seguridad del Poder Judicial, así como las acciones que posibiliten alcanzar niveles de seguridad aceptables.
* Fomentar que los servicios tecnológicos institucionales y de atención al público establezcan niveles de seguridad aceptables, donde se proteja la confidencialidad de los datos de las personas usuarias, la integridad de la información sensible de los procesos judiciales y se garantice de acuerdo con su nivel de criticidad, que dicha información esté disponible para las personas autorizadas.
* Impulsar que la población judicial sea capacitada y comprometida con el cumplimiento de las políticas, lineamientos y procedimientos relativos a la seguridad de la información, así como personal profesional técnicamente preparado para asegurar que las medidas de protección definidas puedan ser correctamente implementadas y administradas durante todo su ciclo de vida.
* Fortalecer las alianzas a través de procesos de comunicación entre Comisión de Seguridad de Centroamérica-SICA, el Consejo Judicial Centroamericano y del Caribe, así como otras entidades nacionales e internacionales, orientado hacia la Ciberseguridad en materia de cooperación en términos de capacitación y estandarización de los procesos a ejecutar.
1. **Resultados esperados**

|  |
| --- |
| **I Semestre 2020** |
| 1. Requerir a la DTI la identificación de las necesidades más urgentes de atención a nivel de seguridad en la infraestructura tecnológica, para poder estructurar una ficha técnica y una ruta de trabajo por dos años, por parte de la Comisión.
2. Elaboración de “*Ficha técnica y ruta de trabajo*”.
3. Presentar la ficha técnica y ruta de trabajo a las autoridades institucionales pertinentes y lograr su respectiva aprobación.
4. Consultar al Departamento de Tecnología de la Información, sobre proyectos específicos en ciberseguridad que recomienda en aras de promover e impulsar la protección y resguardo de la información institucional dentro de los niveles aceptables de riesgo.
5. Presentar y solicitar la aprobación a Corte Plena de los proyectos en ciberseguridad para promover e impulsar la protección y resguardo de la información institucional dentro de los niveles aceptables de riesgo, para que se ordene, cuando sea pertinente, a la Dirección de Planificación la preparación del presupuesto requerido:

5.1 Formular propuesta de concientización de la población judicial sobre los riesgos, el uso y el manejo de la información cibernética.5.1 Formular propuesta de protección y resguardo de la información institucional.  |

|  |
| --- |
| **II Semestre 2020** |
| 1. Retomar examen y negociación del Convenio Marco de Cooperación Interinstitucional entre el Colegio de Profesionales en Informática y Computación, con el Poder Judicial.
2. Reforzar las políticas y lineamientos de seguridad de la información existentes a nivel institucional.
3. Capacitación de seguridad informática a las personas usuarias.
4. Definir un enlace sostenible a nivel interinstitucional y con organismos internacionales para obtener información y capacitación.
5. Crear un protocolo de seguridad, para los funcionarios que desarrollan sus labores bajo la modalidad de teletrabajo.
 |

|  |
| --- |
| **Año 2021** |
| 1. Desarrollar un proyecto que defina la estrategia para la obtención de un Centro de Operaciones de Seguridad (SOC) a nivel institucional.
2. Desarrollar un proyecto que defina la estrategia para la obtención de una plataforma de concientización y entrenamiento a las personas usuarias.
 |

1. **Acciones de visibilidad**

Incentivar una cultura organizacional en temas de Ciberseguridad y protección de la información institucional.

Impulsar los mecanismos de protección.

1. **Participantes**
* Corte Plena.
* Consejo Superior.
* Comisión de Ciberseguridad del Poder Judicial.
* Dirección de Tecnología de Información y Comunicaciones.

Los tres ámbitos que conforman la institución.

|  |
| --- |
| ***1.    RUTA DE TRABAJO 2020-2021*** |
| ***I Semestre 2020*** |
| **Acciones** | **Responsable** | **Mes** | **Virtual /**  | **Resultados esperados** |   |
| **Presencial** |   |
| 1. Reuniones y la correspondencia necesaria con los funcionarios de la Dirección de Tecnologías de la Información (DTI) para la identificación de las necesidades más urgentes de atención a nivel de seguridad en la infraestructura tecnológica del Poder Judicial.  | Coordinadora de la Comisión y Equipo de Apoyo | Febrero | Presencial y correspondencia | Informe de DTI sobre las necesidades más urgentes de atención a nivel de seguridad en la infraestructura tecnológica, para poder estructurar una ficha técnica y una ruta de trabajo por dos años, por parte de la Comisión.  |   |
| 2. Investigación del estado de la situación y necesidades, reuniones e intercambio de correspondencia con funcionarios de la DTI, para la elaboración de la Ficha Técnica y Ruta de Trabajo.  | Coordinadora de la Comisión y Equipo de Apoyo | Febrero a marzo | Presencial y correspondencia  | Ficha técnica y ruta de trabajo |   |
| 3. Convocar a la Comisión de Ciberdelincuencia y Ciberseguridad para la aprobación de la ficha técnica y ruta de traba | Coordinadora de la Comisión y Equipo de Apoyo | Junio | Virtual | Aprobación de la ficha técnica y ruta de trabajo.  |   |
| 4. Solicitar se agende ante Corte Plena presentación de la ruta de trabajo de la Comisión para su aprobación.  | Coordinadora de la Comisión y Equipo de Apoyo | Junio  | Presencial | Aprobación de la ficha técnica y ruta de trabajo por parte de Corte Plena. |   |
| 5. Reuniones y correspondencia la Dirección de Tecnologías de la Información (DTI) para concretar las propuestas sobre proyectos a desarrollar en ciberseguridad, para promover la protección y resguardo de la información del Poder Judicial. | Coordinadora de la Comisión y Equipo de Apoyo | Febrero a junio | Presencial y correspondencia | Concretar primeras propuestas de proyectos en ciberseguridad, para promover e impulsar la protección y resguardo de la información.  |   |

|  |
| --- |
| ***1.    RUTA DE TRABAJO 2020-2021*** |
| ***II Semestre 2020*** |
| **Acciones** | **Responsable** | **Mes** | **Virtual /**  | **Resultados esperados** |
| **Presencial** |
| 6. Reunión con personeros del Colegio de Profesionales en Informática y Computación, para retomar Convenio Marco de Cooperación Interinstitucional.  | Comisión de Ciberdelincuencia y Ciberseguridad  | A definir, dependiendo de aprobación.  | Presencial/virtual.   | Presentar propuesta en torno al Convenio Marco de Cooperación Interinstitucional entre el Colegio de Profesionales en Informática y Computación, con el Poder Judicial. |
| 7. Campaña de divulgación de política de seguridad de la información.  | Comisión de Ciberdelincuencia y Ciberseguridad Departamento de Prensa y Comunicación Organizacional  | Segundo semestre 2020 | Virtual  | Reforzar las políticas y lineamientos de seguridad de la información |
| 8. Establecer como obligatorio un curso de capacitación de seguridad informática y seguridad de la información al ingresar al Poder Judicial y en el caso de los funcionarios que ya se encuentran laborando, como parte del proceso de formación continua.    | Comisión de Ciberseguridad y Ciberdelincuencia y Dirección de Gestión Humana | Segundo semestre 2020 | Correspondencia y virtual | Capacitación de seguridad informática a los usuarios  |
| 9. Establecer plan de acción para definir un enlace sostenible a nivel interinstitucional y con organismos internacionales para obtener información y capacitación | Comisión de Ciberseguridad y Ciberdelincuencia y Dirección de Tecnologías de la Información  | Segundo semestre 2020 | Correspondencia, virtual, presencial. | Definir un enlace sostenible a nivel interinstitucional y con organismos internacionales para obtener información y capacitación. |
| 10. Desarrollar un protocolo de seguridad y buenas prácticas, para los funcionarios que laboran bajo la modalidad de teletrabajo.  | Comisión de Ciberseguridad y Ciberdelincuencia y Dirección de Tecnologías de la Información | Segundo semestre 2020 | Correspondencia, virtual, presencial. | Protocolo de seguridad y buenas prácticas, para los funcionarios que desarrollan sus labores bajo la modalidad de teletrabajo. |

|  |
| --- |
| ***1.    RUTA DE TRABAJO 2020-2021*** |
| ***2021*** |
| **Acciones** | **Responsable** | **Mes** | **Virtual /**  | **Resultados esperados** |
| **Presencial** |
| 11. Definir pautas para desarrollar un proyecto que establezca la estrategia para la obtención de un Centro de Operaciones de Seguridad (SOC)a nivel institucional. | Comisión de Ciberdelincuencia y Ciberseguridad y Dirección de Tecnologías de la Información |  | Correspondencia | Desarrollar un proyecto que defina la estrategia para la obtención de un SOC a nivel institucional.  |
| 12. Definir pautas para desarrollar un proyecto que establezca la estrategia para la implementación de una plataforma de concientización y entrenamiento a las personas usuarias.  | Comisión de Ciberdelincuencia y Ciberseguridad y Dirección de Tecnologías de la Información |  | Correspondencia | Desarrollar un proyecto que defina la estrategia para la obtención de una plataforma de concientización y entrenamiento a las personas usuarias. |

-0-

La magistrada Zúñiga, en oficio N° C-CDCS-02-2020 de 15 de julio de 2020, expresó:

 “En mi condición de Coordinadora de la Comisión de Alto Nivel de Ciberseguridad y Cibercrimen del Poder Judicial, remito la presente *“Ficha técnica para las iniciativas de Ciberseguridad en el Poder Judicial”,* que consiste en una propuesta de trabajo de la referida comisión para el periodo 2020 a 2021, con la finalidad de que sea sometido a consideración de Corte Plena.

Las principales pretensiones de la Comisión son las siguientes:

1. Poner en conocimiento de Corte Plena la hoja de ruta y los proyectos que ella contiene, considerando los aportes que puedan realizar las señoras Magistradas y los señores Magistrados.
2. Lograr la aprobación de Corte Plena de los objetivos y las acciones por realizar enumerados en la Ficha técnica.
3. Se giren instrucciones al Departamento de Gestión Humana para que se establezca como obligatorio y, en consecuencia, se comience a impartir el curso de capacitación de seguridad informática y seguridad de la información a las funcionarias y los funcionarios de primer ingreso al Poder Judicial, así como a las personas que ya se encuentran laborando en la institución, como parte del proceso de actualización y formación continua.
4. Se declaren estas iniciativas de interés institucional.
5. Se inste al Departamento de Planificación del Poder Judicial y al Consejo Superior a apoyar los objetivos y las acciones expuestas en la Ficha técnica a fin de que a los proyectos de la Comisión de Ciberseguridad se les asigne un contenido presupuestario que permita su puesta en marcha y ejecución, por ser de interés institucional.

En razón de lo anterior, solicito asignar un espacio en agenda para exponer el programa de trabajo en materia de Ciberseguridad para el presente año y el próximo, a fin de lograr la respectiva aprobación de las Magistradas y los Magistrados de la Corte Suprema de Justicia en los términos apuntados.”

- 0 -

Indica la Presidenta en ejercicio, magistrada Solano: “Este artículo está referido a la coordinación de la Sub Comisión de Alto Nivel de Ciberdelincuencia y Ciberseguridad del Poder Judicial que nos remite una ficha técnica para las iniciativas de Ciberseguridad en el Poder Judicial, lo cual presenta la magistrada Zúñiga".

Manifiesta la magistrada Zúñiga: "Me corresponde como Coordinadora de la Comisión de Ciberseguridad y Ciberdelincuencia del Poder Judicial hacer exposición de una ficha técnica.

Es importante recordar que mediante el acta de Corte Plena N° 34-2016 del 5 de diciembre del 2016 fue creada esta Comisión, integrada por los jerarcas de la Fiscalía General de la República, del Organismo de Investigación Judicial, de un magistrado de la Sala Tercera; con el acompañamiento técnico de la Dirección de Tecnología de la Información.

En meses pasados, nos hemos estado reuniendo de manera continua para hacer una propuesta y decidimos dividir la propuesta por temática, primero en el tema de ciberseguridad y posteriormente abordar el tema de ciberdelincuencia.

 ¿Y por qué es que esta ficha técnica nosotros la presentamos en Corte Plena para la aprobación?, y más que para la aprobación, para la construcción también en ella de los señores y señoras magistradas, porque consideramos que es una propuesta que incluso tiene interés institucional, todos somos muy conscientes de la realidad actual del tema de las redes sociales, de los peligros que también tenemos frente a las nuevas tecnologías, y es por esa razón que con esta ficha técnica también se solicitó que los proyectos que aquí se incluyen fueran declarados de interés institucional.

 El proyecto que se propone, en este caso referido al tema de ciberseguridad, tiene como objetivo el fomentar las mejores prácticas de protección, acceso y resguardo de la información cibernética, que a su vez permita mantener la confidencialidad, la disponibilidad y también la integridad, de manera que se pueda disminuir la materialización de posibles riesgos institucionales.

Y entonces con esa visión nos sentamos para hacer una propuesta y presentarla, esta propuesta incluye una serie de prácticas y también la propuesta de algunos proyectos que tienen objetivos específicos.

 En primer lugar, se procuraba conocer y tratar los riesgos estratégicos y operacionales de seguridad de la información, en los servicios que nosotros tratamos.

También trazar una ruta de trabajo que permitiera determinar esos riesgos, y a su vez hacer propuestas concretas y aceptables respecto a la seguridad.

Como un tercer aspecto, también nos interesaba fomentar que los servicios tecnológicos institucionales y de atención al público mantuvieran niveles de seguridad aceptables, protegiendo la confidencialidad de los datos, de las personas usuarias, la integridad de la información sensible de los procesos judiciales, y además que se garantizara un nivel aceptable de criticidad.

 También queríamos sentar un impulso para que la población judicial fuera capacitada y sensibilizada especialmente en estos temas.

Y finalmente pues también se tenía el propósito de fortalecer algunas alianzas a través de proceso de comunicación entre esta Comisión y algunas entidades nacionales e internacionales especializadas.

Nosotros nos propusimos una serie de resultados para este año y para el siguiente, y en una reunión anterior ya se habían dado algunos detalles de cuales eran esos resultados, pero básicamente nos propusimos, en primer lugar, tener un acercamiento con la Dirección de Tecnología de la Información para conocer de las necesidades urgentes de atención a nivel de seguridad en la infraestructura, en la tecnología, para poder estructurar precisamente la ficha técnica que se les presenta, así como una ruta de trabajo.

 En segundo lugar también, pues era importante no solamente contar con los integrantes de la Comisión sino también podérselas presentar a Corte Plena para su aprobación, y queríamos entonces lograr algunos productos básicos, por ejemplo, que se autorizara a la Dirección de Gestión Humana el incluir cursos de capacitación sobre ciberseguridad, tanto en las personas de primer ingreso, como cursos de actualización para los funcionarios y funcionarias actuales del Poder Judicial, que nos permitieran establecer una barrera efectiva contra, más bien en procura de una mejor seguridad de nuestros sistemas informáticos.

 También nosotros teníamos por propósito dar a conocer la política institucional sobre precisamente estos temas, nosotros tenemos una política que ha sido muy poca difundida y que consideramos vital sea del conocimiento de todo el funcionariado del Poder Judicial.

También queríamos reforzar las políticas y lineamientos de seguridad de la información, nos pareció también muy importante ahora sobre todo con los números que el día de hoy nos han expuesto, tanto la máster Nacira Valverde Bermúdez como la licenciada Maricruz Chacón Cubillo en el tema de lo relacionado al teletrabajo, parece fundamental establecer un protocolo de seguridad y buenas prácticas para los funcionarios que desarrollaran sus labores bajo esta modalidad.

Y además otro aspecto que también vemos, es la posibilidad de poder proyectar un programa de estrategia para la obtención de herramientas, que nos sean de utilidad en este tema, además de desarrollar un proyecto que defina la estrategia para la obtención de una plataforma de concientización y entrenamiento de las personas usuarias.

 Estos productos nosotros tenemos planeado o que sea el trabajo de esta Comisión por dos años, y estos son los proyectos que como mínimo estamos planteando, y que se lo sometemos a consideración de todos ustedes.

Quedo a su disposición para cualquier duda y agradezco la atención, no sin antes solicitar con todo respeto el apoyo por ser este un tema actual de suma relevancia en el que urge un respaldo.

Como ven, no solamente cubre prácticas, sino también vamos un paso más allá pensando en la posibilidad de plantear a Corte proyectos específicos, pero para lo cual también requeriríamos el apoyo de Corte, porque estaría también de por medio la colaboración de la Dirección de Planificación, de la Dirección de Tecnología de la Información, y por ese motivo es indispensable obtener la aprobación de todos ustedes señores y señoras, para poder continuar laborando, muchas gracias".

 Prosigue la Presidenta en ejercicio, magistrada Solano: "Creo que el trabajo que viene haciendo esta Subcomisión es sumamente importante.

Cuando iniciamos con la emergencia nacional y empezamos a ver los temas, no solo de los protocolos en las diferentes jurisdicciones, sino también en el uso de las herramientas tecnológicas para poder llevar a cabo las audiencias mediante medios electrónicos, vimos como la Dirección de Tecnología de la Información nos dijo que la institución iba a utilizar la herramienta Teams por temas de seguridad, que si bien es cierto teníamos que pagar la licencia, era mucho más segura que la herramienta Zoom, que es una herramienta de libre acceso, pero tratándose de la materia que nosotros conocemos se hacía necesario resguardar seguridad, y conocemos como todos los días nos damos cuenta de las llamadas que nos hacen a parientes y a amigos.

 Y desde la Sala Penal también la cantidad de asuntos que han llegado y que se ha incrementado toda la delincuencia que tiene que ver por medios electrónicos e informáticos.

De manera que el hecho de que sobre todo en materia penal no tengamos un expediente electrónico, sino que ha habido en muchos casos que tengamos que recurrir a otro tipo de herramientas para poder seguir trabajando en el contexto de la emergencia, que como señalaba la magistrada Chacón en horas de la mañana, esto no está pronto a solucionarse, sino que no sabemos durante cuánto tiempo más vamos a estar en la emergencia.

De manera que el poder tener protocolos para maximizar la seguridad en la institución se hacen necesarios, por eso es que la propuesta que se hace por parte de la magistrada Zúñiga como coordinadora de esta Subcomisión, que es de suma relevancia, trabajan no solo, como ella indica, con la Dirección de Tecnología de la Información, con la Dirección de Planificación, con el Organismo de Investigación Judicial; en realidad hace ver la necesidad de que nosotros tengamos protocolos diferentes, por eso es que me parece muy importante la propuesta que se nos hace.

Le doy las gracias a la magistrada Zúñiga por el estudio que se han permitido hacer con tanto detalle de lo que nos presentan".

 Expresa la magistrada Varela: "Para pedir que esta propuesta que nos hacen se le de todo el apoyo institucional que se requiere, como usted lo acaba de señalar, señora Presidenta en ejercicio, este no es un tema menor, va ligado íntimamente con lo que ahora estamos utilizando mucho, las herramientas tecnológicas, entonces es muy necesario que la institución no escatime en seguridad en este tema, solamente".

 Añade la Presidenta en ejercicio, magistrada Solano: "Muy bien, creo que si no hay ninguna observación adicional, el acuerdo sería aprobar la propuesta que se nos hace por parte de la Subcomisión de alto nivel de ciberdelincuencia y ciberseguridad del Poder Judicial, y aprobar la ficha técnica para las iniciativas de ciberseguridad en el Poder Judicial y declararlo de interés institucional, por cuanto se hace como una necesidad.

Creo que ante la emergencia tanto a nivel mundial como a nivel nacional, ha visto cual es la importancia que tiene el uso de las herramientas tecnológicas y que de alguna manera la reticencia que habíamos tenido para utilizar estas herramientas en otros momentos, pareciera que esto vino para quedarse.

 De manera que el poder tener protocolos que resguarden la información que maneja este poder de la República es necesario.

Magistrada Zúñiga, si usted quería hacer alguna otra observación".

 Agrega la magistrada Zúñiga: "Nada más dar las gracias no solamente a los señores magistrados y magistradas, sino también a todo el equipo de la subcomisión, específicamente a las personas designadas por la señora Fiscala General de la República, Emilia Navas Aparicio, y al Director del Organismo de Investigación Judicial, máster Walter Espinoza Espinoza; estamos también en este momento tratando de organizarnos con don Juan Carlos Murillo del Ministerio Público y don Erick Lewis Hernández del Organismo de Investigación Judicial, para hacer también una propuesta específica sobre ciberdelincuencia, pero decidimos que como los temas son tan bastos los íbamos a presentar de forma separada.

Muchas gracias por el apoyo de esta iniciativa".

Dice la Presidenta en ejercicio, magistrada Solano: "Muy bien si no hay ninguna otra objeción aprobaríamos la ficha técnica tal y cual se nos ha propuesto”

Sin objeción alguna, **se acordó:** Tener por hecha la exposición de la magistrada Zúñiga, en su condición de Coordinadora de la Sub Comisión de Alto Nivel de Ciberdelincuencia y Ciberseguridad del Poder Judicial, en consecuencia: **1)** Aprobar los objetivos y las acciones por realizar enumerados en la “Ficha técnica para las iniciativas de Ciberseguridad en el Poder Judicial”, para el periodo 2020 a 2021. **2)** Declarar estas iniciativas de interés institucional. **3)** Girar instrucciones a la Dirección Gestión Humana para que se establezca como obligatorio y, en consecuencia, se comience a impartir el curso de capacitación de seguridad informática y seguridad de la información a las funcionarias y los funcionarios de primer ingreso al Poder Judicial, así como a las personas que ya se encuentran laborando en la institución, como parte del proceso de actualización y formación continua. **4)** Instar a la Dirección de Planificación y al Consejo Superior a apoyar los objetivos y las acciones expuestas en la ficha técnica, a fin de que a los proyectos de la Comisión de Ciberseguridad se les asigne un contenido presupuestario que permita su puesta en marcha y ejecución, por ser de interés institucional.”

**Atentamente,**

**Lic. Silvia Navarro Romanini**

**Secretaria General**

**Corte Suprema de Justicia**

c: Consejo Superior del Poder Judicial

Dirección de Gestión Humana

 Dirección de Planificación

Sra. Katherine Reyes Molina, Secretaria Ejecutiva de la Sala Tercera de la Corte Suprema de Justicia

Diligencias / Ref: (**6983-2020 y 8386-2020**)

*Claudio*