Alianza Nacional de Inteligencia Artificial

MESA DE TRABAJO CIBERSEGURIDAD Y GESTIÓN DE RIESGOS SESIÓN 1 y 2

Documento de conclusiones de Líder de mesa, Eleazar Aguirre Anaya

Temas abordados en las mesas de trabajo

1. Gestión de riesgos en general
2. Usos de IA inaceptables
3. Categorías de riesgos en el uso de la IA
4. Gestión de riesgos contra de la seguridad de la información
5. Ética de la IA

Preguntas detonantes

- ¿Pueden los reguladores o los tribunales solicitar información sobre los sistemas de IA y su funcionamiento interno en virtud del marco normativo?
- ¿Se aplican diferentes estándares de protección de datos para los datos recopilados por entidades públicas y privadas?
- ¿La privacidad y/o el respeto a la vida privada y familiar están protegidos por la ley de protección de datos u otra ley?
- ¿Cómo se podría mejorar la ciberseguridad en la administración pública?
- ¿Qué hace falta para garantizar a la ciudadanía un uso de IA seguro?
- ¿Cómo podríamos diseñar una IA que garantice los derechos a la privacidad?
- ¿Cuáles serían los factores claves a considerar en el diseño de una política de ciberseguridad para IA?
- ¿Qué factores deben estar relacionados para tener una política pública de ciberseguridad efectiva?
- ¿Qué hace falta en materia de medidas preventivas, correctivas y transparencia respecto de la ocurrencia de ciberataques?
- ¿Son suficientes los mecanismos de colaboración público privada para la ciberseguridad? ¿Qué hace falta?

Conclusiones

La metodología empleada para el desarrollo de las mesas consistió en tres etapas por lo menos hasta la redacción del presente documento, una primera etapa de diseño y planeación, en la segunda se desarrollaron las actividades planeadas, por último, en la tercera se presentan las conclusiones.

Con respecto a la primera etapa, desde la visión del líder de mesa se observó que, los instrumentos utilizados permitieron convocar a los diferentes sectores de la sociedad involucrados en el desarrollo e implementación de inteligencias artificiales. Se intuye un proceso previo para la definición de los cinco temas de las mesas de trabajo, así como, un proceso de búsqueda de los diversos roles de especialistas con experiencia en el proceso de diseño, integración, instalación, puesta en operación o uso de Inteligencias Artificiales (IA).

En la segunda etapa se identifican varios elementos de diseño; captar las experiencias, aprendizajes y problemas identificados por los especialistas en los diferentes sectores; la temporalidad en la ejecución de las diversas actividades permitió identificar claramente las prioridades por sector y las posibles relaciones con el resto. Sin embargo, esto también provocó que el control y asignación por pregunta-especialista no fue equitativa y en algunos temas posiblemente faltó tiempo para describirlos de mejor manera.

La tercera etapa está en proceso y por el momento, en este documento se comparten las reflexiones derivadas de las mesas de trabajo que abarcan la identificación del estatus actual de la ciberseguridad y gestión de riesgos en el país, usos de la IA segura y ética en otros países o regiones, finalizando con algunas recomendaciones para abordar las siguientes etapas del proceso.

Ciberseguridad en la administración pública (MX)

No se cuenta con la cantidad suficiente de equipos de seguridad en todas las entidades de gobierno federal (2 CSIRT públicos registrados en el FIRST). Se intuye que esta situación es mayor a nivel estatal o municipal. Sin tener conocimiento a profundidad, se estima una situación similar con la iniciativa privada. Las trasnacionales tienen equipos solidos internacionales para atender las necesidades, en el caso de la mediana o pequeña empresas hay mucho por atender.

Se desconoce la capacidad y madurez de los equipos de seguridad existentes y si cuentan con una plantilla que integre a todos los roles fundamentales recomendados por ENISA o NIST.

La formación y/o capacitación en nuevas tecnologías generalmente es en modalidad reactiva. No se observa un plan integral que tenga como objetivo un nivel de madurez proactivo frente a la ciberamenazas.

En el país hay espacios insuficientes de formación sobre temas de tecnología emergente y algunos de sus egresados migran al extranjero por opciones más atractivas.
Las herramientas tecnológicas preventivas y reactivas son de importación y no es sencillo mantener las licencias por largo tiempo. En el caso de la seguridad nacional, resulta necesario desarrollar herramientas tecnológicas nacionales para hacer frente a las amenazas.
Al momento se observan algunos resultados aislados para generar capacidades como nación.

Uso de IA seguro a nivel Global

Recientemente se observa un gran interés por conocer y concientizar a la población sobre la IA.
En varios países se está trabajando por legislar el proceso ético y seguro del ciclo de vida del desarrollo de las Inteligencias artificiales. En la actualidad son pocos los países que cuentan con regulación en la materia.
En los últimos meses se observó la aplicación de medidas reactivas a productos en el mercado por grandes proveedores de tecnología. Se desconoce el estado de vulnerabilidad/sesgo que tienen las IAs que se encuentran actualmente en el mercado.
Insuficientes especialistas en IA en la academia, solo una porción de los especialistas inicia su formación en IA seguras.
No se identifica la formación de especialistas de IA en operaciones, los que actualmente operan y mantienen a las existentes, tienen una formación diferente y han sido capacitados para desarrollar sus actividades.
Actualmente se encuentran en desarrollo las herramientas de seguridad para IA, en operaciones se ubican adaptaciones tradicionales.

Las observaciones identificadas para lograr IA éticas

Definir un plan de acción integral con metas y alcances a mediano y largo plazo, robustecer frente a factores políticos o administrativos sexenales.
Definición del marco conceptual nacional de IA.
Definir una política nacional de ciberseguridad para IA, sería deseable contar con una política nacional de ciberseguridad que contemple a las tecnologías emergentes.
Diseño holístico, considerando el ciclo de vida completo y siempre bajo la perspectiva de mejora continua (TRL). Establecer los mecanismos de control que garanticen un ciclo de diseño de IA segura (marco de trabajo de gestión del riesgo de la IA del NIST).
Garantizar que se aplicará de facto lo establecido en la ley.

Recomendaciones para abordar las siguientes etapas

Proponer e impulsar una política pública de ciberseguridad holística y efectiva.
Aprovechar los recursos disponibles para resolver los problemas nacionales en la modalidad de consorcio (Gobierno-Industría-Academía).
Garantizar la formación de calidad en materia digital desde nivel elemental (enfoque de diseño, evitar acotarlo al nivel de usuario).
Garantizar el impulso del desarrollo de tecnología nacional, considerando el ciclo de vida completo de la tecnología (9 niveles TRL).
Evaluar las medidas preventivas, correctivas y transparencia respecto de la ocurrencia de ciberataques.
El alcance inicial ya es insuficiente, pensar en desarrollar y fortalecer capacidades nacionales en:

- Proactividad y resiliencia.
- Investigación, desarrollo tecnológico e Innovación (I+D+i).
- Empleo de herramientas nacionales en operaciones de infraestructura crítica.
- Obligatoriedad de la colaboración público-privada.
- Garantizar la inversión de ambas partes enfocada en incrementar capacidades nacionales.
- Establecer obligatoriedad y mecanismos para el cumplimiento.

Con relación a la metodología empleada, se llegó al objetivo de diseñar, planear y desarrollar las mesas de trabajo. Se desconoce los instrumentos y métricas empleados para medir los resultados obtenidos y presentar el análisis de los mismos.

Agradezco la invitación a participar por la Senadora Alejandra Lagunes, los miembros de la ANIA y a todos los especialistas que compartieron sus conocimientos en las mesas de trabajo.

Finalmente, es materia de celebración y reconocimiento porque este tipo de ejercicios se den en nuestro país. Mis felicitaciones a la Senadora Lagunes por la visión y dedicación al proyecto. Deseo que nuestra pequeña visión desde el Laboratorio de Ciberseguridad del IPN, aporte en la construcción de un México más seguro, poniendo *la técnica al servicio de la patria*.