LITORALPRESS

Fecha: 18-07-2024
Fuente: Diario Estrategia
Título: ?Ciberseguridad e IA: Conoce cómo trabajar una estrategia digital de manera eficaz

Visitas: 11.637
VPE: 38.984

Favorabilidad: No Definida

Link: https://www.diarioestrategia.cl/texto-diario/mostrar/4934436/ciberseguridad-e-ia-conoce-como-trabajar-estrategia-digital-manera-eficaz

Aprovechar las ventajas y controlar los riesgos que supone el ecosistema digital, son los principales objetivos de la industria actual. Con este propósito, la Facultad de Ingeniería y Ciencias de la **Universidad Adolfo Ibáñez** realizará una masterclass titulada: "Tríada del cumplimiento digital: ciberseguridad, inteligencia digital y datos personales". La cita es para el jueves 18 de julio, a las 19:30 horas, vía zoom.   El encuentro estará a cargo de la abogada Antonia Nudman, Asociada Senior del grupo IP, Tech and Data de Albagli Zaliasnik (AZ); y moderado por **Ricardo Seguel**, director académico del Magíster en Ciberseguridad **UAI**.   Una de las principales preocupaciones de las empresas e instituciones públicas es el cumplimiento normativo local e internacional, ya que cada día son azotadas por el creciente volumen de las amenazas digitales, los ataques a la infraestructura tecnológica y el robo de datos.

En esta sesión conversaremos cómo abordar ese tridente del cumplimiento desde la estrategia, la gestión de riesgos y el gobierno de datos.   La ciberseguridad, la IA y los datos personales forman tres pilares fundamentales en base a los que se estructura gran parte de la era digital, donde el activo informático tiene un valor intrínseco asociado.

Por una parte, la ciberseguridad es la rama que busca proteger los activos informáticos, los sistemas y las redes digitales, que claramente involucran datos que se representan como información altamente relevante y sensible (pudiendo o no, adquirir la naturaleza de personal); mientras que la IA es una ciencia que funciona en base a datos, tanto en la estructura del sistema de IA como en la finalidad.   En este sentido, Antonia Nudman explica que: "Existe una conexión y dependencia entre los datos propiamente tal y los fundamentos de la ciberseguridad e IA. Asimismo, cuando los datos son personales, mantienen su regulación y estándar propio, lo que eleva los requisitos normativos y riesgos de la operación.

De este modo, los tres pilares estructuran las bases que deben estar presentes en todo tipo de actividad que involucre el manejo de herramientas digitales".   Por su parte, **Ricardo Seguel** afirma que Chile ha avanzado mucho en materia de ciberseguridad, tras la actualización de la Ley de Delito Informático y la Ley Marco de Ciberseguridad, sin embargo, queda mucho por hacer. "La amplitud de la ley marco requiere que se especifiquen proyectos de ley que tomará tiempo aún en materias de protección de datos personales (en discusión en el congreso), seguridad de la infraestructura crítica del país, ciberinteligencia y contra-inteligencia para perseguir el crimen organizado en Chile en colaboración con otros países, normativas para que las empresas reguladas y no reguladas e instituciones públicas suban el estándar de ciberseguridad, como también potenciar y hacer crecer el capital humano especializado en todas estas materias es vital".   La expositora a cargo de esta masterclass, enfatiza que la importancia de un análisis acabado de la naturaleza de los activos informáticos, finalidades y datos que se utilicen en los sistemas de IA y de los propios datos intrínsecos que existan en cada organización. "Este debate nos otorgará los lineamientos para elaborar una estrategia que permita cumplir con los estándares regulatorios para disminuir los riesgos de cada operación y además, detectar oportunidades respecto a las posibilidades que tiene cada organización, para dar una finalidad al activo informático y/o datos que maneje a nivel interno, dependiendo de cada rubro en particular", puntualiza la experta.   Actualmente existen herramientas que son diseñadas en base al tipo de información y rubro que maneje cada organización, por lo que la herramienta más recomendada es aquella que se desarrolla a medida para cada uno de los intervinientes. "Las habilidades que siempre son sugeridas, dicen relación con la capacitación y trabajo interconectado de los equipos, trabajando en base a protocolos diseñados en base a las necesidades de cada institución, que permiten involucrarse y llevar control con cada una de las unidades o departamentos y en cada etapa o ciclo de vida del activo informático, generando trazabilidad en el manejo de la información", añade Nudman.   La especialización del capital humano en ciberseguridad es transversal a todas las organizaciones y a todas las áreas de una organización, desde el directorio pasando por los ámbitos estratégicos, tácticos y operativos, ya que es una capacidad primordial que debemos capacitar y concientizar para todos los colaboradores.

Así, **Ricardo Seguel**, concluye que "contar con una estrategia o plan director de ciberseguridad es primordial para los directorios y la gestión del Gobierno, Riesgo y Cumplimiento (GRC), para la transparencia, para la implementación del sistema de prevención de delitos económicos (Ley Nro. 20.393 y 21.595) e informáticos (Ley Nro 21.459), para la Gestión de Riesgo y control interno, para la implementación de estándares de seguridad de la información como ISO

27001, NIST CSF, CIS, etc. y para el cumplimiento normativo del regulador o superintendencia de una determinada industria, entre otros".   La inscripción para esta clase magistral está abierta y es gratuita.   Ingresa al siguiente link: https://mkg.uai.cl/postgrados-nuevo/charlas/triada-de-cumplimiento-digital/page/contact Uso de cookies Utilizamos cookies propias y de terceros para mejorar la experiencia de navegación, y ofrecer contenidos y publicidad de interés. Al continuar con la navegación entendemos que se acepta nuestra política de cookies