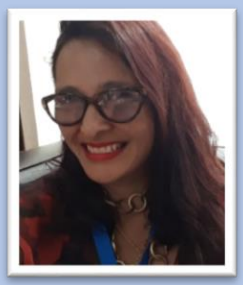
Reseña de

Ciberseguridad, Privacy y Ética en el Internet de las Cosas (IoT) por Félix Uribe



Escrito por: **Niurka Hernandez G.**

Profesora y Conferencista en Ciberseguridad a nivel Latinoamericano 2008- actual, academia cátedras de: Proyectos Sociotecnológicos TIC, Seguridad Informática, Auditoría de Sistemas, prueba y validación de software, fundamentos de ingeniería de requisitos y análisis, gestión de proyectos informáticos, fundamentos de diseño de software, Seguridad y defensa y Delitos informáticos.

Profesional especialista en Seguridad información, Redes y Telecomunicaciones y Ciberseguridad, con experiencia de más de 20 años, prestando servicios en proyectos relevantes a nivel Latinoamericano en el área de Ciberseguridad; Asesorías y en el montaje de Servicios de SOC (Security Operation Center), Inteligencia y Correlación Internacional de los servicios de CERT (Computer Event Response Team); Asesoría y consultoría en Fundamentos Creación y Manejo de Equipo de Respuesta a Incidentes de Seguridad Cibernética en Latinoamérica. En Internet Society Capitulo: ISOC Cybersecurity SIG Cargo Vice Presidente 2017-actual. Certificaciones de ISACA. CRISC y Certificación Europea sobre CyberCriminalidad y Pruebas Electrónicas (CCE).

El día miércoles 15 de mayo 2019, contamos con la visita del señor Félix Uribe, profesional de la seguridad en la tecnología de la información (TI) con una amplia experiencia en el campo de la ciberseguridad, privacidad, y seguridad de la información en los sectores públicos y privados.

En el ámbito Académico, es Profesor Asociado Adjunto en el Programa de Política y Gestión de Ciberseguridad de la University of Maryland, University College (UMUC) donde imparte cursos de ciberseguridad, privacidad y cibercriminalidad. En el estado de New York, fue profesor en el departamento de Matemáticas y Ciencias Informáticas en Mercy College y es el creador de la página Uribe100.com

la cual proporciona noticias, enlaces e información en el campo de la ciberseguridad y la privacidad. Su interés actual de investigación se centra en cuestiones que abordan los desafíos de ciberseguridad y privacidad en el Internet de las Cosas (IoT) y cuyos resultados ha presentado en varias conferencias nacionales e internacionales. El mismo dictó una conferencia titulada "Ciberseguridad, Privacy y Ética en el Internet de las Cosas (IoT)", la cual les comparto a continuación:

"Aunque no existe una definición exacta de lo que hoy día llamamos el Internet de las Cosas (IoT), en pocas palabras, yo particularmente lo defino como "La red de dispositivos (cosas) capaces de interactuar con otros dispositivos y seres vivos a través del Internet o a través de una red privada local o global no conectada al Internet." Esta interacción se lleva a cabo a través de sensores, actuadores y protocolos de comunicación. Entre los dispositivos de IoT más comunes podemos mencionar las bocinas, luces, puertas, y cámaras inteligentes entre otros.

Es palpable hoy día de ver los dispositivos IoT instalados en varios dominios en todos los sectores de la sociedad tales como en la transportación, la salud, y en las nuevas "ciudades inteligentes" por mencionar algunos de estos.

Varias de las recientes estadísticas publicadas por instituciones relacionas con el IoT, predicen que para el 2020 entre 30 y 50 billones de estos dispositivos estarán conectados al Internet. Es de notar, que, al mismo tiempo, con la instalación masiva de estos, está poniendo en riesgo la ciberseguridad y la privacidad de los individuos e instituciones que los usan si no se lleva a cabo la debida implementación de controles que eviten su uso con fines maliciosos. Además de abordar los temas de ciberseguridad y privacidad es importante también el uso ético que se les dé a estos dispositivos.

En el ámbito de la ciberseguridad, los riesgos con los dispositivos IoT como vector de ciberataque generalmente se pueden dividir en 1) riesgos con los dispositivos mismos dado la escasa implementación de la seguridad en su fabricación y 2) riesgos con la forma en que se utilizan. Por ejemplo, la utilización de estos para el espionaje industrial.

En el ámbito de la privacidad, podemos mencionar los riesgos tales como la colección no autorizada y masiva de datos (datos y metadatos) por parte del fabricante o de terceros, la vigilancia/seguimiento por parte de empresas y gobiernos, la invasión del perfil médico y la falta de políticas de privacidad en los dispositivos mismos.

Para combatir la falta de ciberseguridad y privacidad en el mundo del IoT, instituciones públicas y privadas están creando soluciones técnicas que se puedan utilizar tanto en la fabricación, así como en el uso de los dispositivos ya instalados. Un ejemplo de esto es el proyecto "Manufacturer Usage Description" o MUD, del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos. El objetivo de este proyecto es permitir a los fabricantes de dispositivos IoT la implementación de reglas durante su fabricación que eviten que estos sean utilizados maliciosamente una vez instalados.

Por último, es importante recalcar la ética en el uso de la masiva cantidad de datos que se coleccionan a través de estos dispositivos y la monetización de estos por aquellos que los coleccionan o de terceros. Si la colección inicial de los datos se llevó a cabo con un propósito específico, no es ético su uso posteriormente con otros fines que no fueron originalmente expresados al consumidor.

En conclusión, el crecimiento exponencial de los dispositivos IoT y

sus aplicaciones cotidianas exige abordar las preocupaciones actuales de seguridad y privacidad que afectan la confiabilidad del actual ecosistema de IoT en el mundo. Si queremos proteger la seguridad y la privacidad de las futuras generaciones, tenemos que empezar hoy y no mañana."

Esta presentación permitió conocer de primera mano cómo se encuentra el avance del IoT, cuál ha sido su impacto en la sociedad y hasta dónde hay proyecciones de llegar, así como poder observar ejemplos prácticos de la tecnología en directo. Me parece muy interesante las preguntas que le realizaron nuestros estudiantes de cómo hacer para regular este tipo de tecnologías desde este momento debido a que, si sigue avanzando como hasta ahora, no podrán colocarse limites en su uso e implementación en todos los ámbitos, considero que este tipo de actividades deben ser concurrentes, ya que son enriquecedoras tanto del cuerpo docente como de los alumnos.