Estimados lectores:

Nos complace presentar el segundo número de la revista Telemática de 2018. El tema central es la Ciberseguridad, aspecto muy importante a tener en cuenta en estos momentos en que se incrementa el acceso a las nuevas tecnologías de la información y se abre a nuestras entidades ya la población un mundo nuevo de posibilidades.

En la presente edición se presentan varios artículos relacionados con al análisis de malware y su detección. En el artículo "DETECCIÓN DE MALWARE EN ANDROID UTILIZANDO APRENDIZAJE AUTOMÁTICO" se aborda, como indica su título, el tema de la detección de programas malignos en aplicaciones Android por métodos de aprendizaje automático, lo que posibilita detectar nuevas amenazas desconocidas. Como complemento, en el trabajo *"SEGURMÁTICA SEGURIDAD MÓVIL: MÁS ALLÁ DE LA DETECCIÓN DE MALWARE ANDROID"* se presenta una aplicación antivirus para sistemas operativos Android y otras disponibilidades adaptadas a los entornos de seguridad del ciberespacio cubano. En el artículo "*ENFRENTANDO LOS RANSOMWARES"* se explica la esencia de la infección por *ransomwares*, una de las infecciones más peligrosas y destructivas de los últimos años producidas por los grupos cibercriminales, y la manera en que se trabaja en el laboratorio de Segurmática para combatir esos flagelos.

Como parte a los enfrentamientos a ciberataques está la propuesta del "SISTEMA PARA LA DETECCIÓN DE ATAQUES PHISHING UTILIZANDO CORREO ELECTRÓNICO", un ataque *phishing* utiliza técnicas de ingeniería social y engaño con el objetivo de que las víctimas se infesten con un programa maligno o que las misma entreguen información personal; en este sentido se propone una arquitectura orientada a servicios que integra y correlaciona patrones de comportamiento para la detección de este tipo de ataques. Con el artículo "MODELO PARA LA DETECCIÓN DE ATAQUES A LAS APLICACIONES WEB E INTERCAMBIO DE CIBERAMENAZAS" se propone un modelo para la prevención de ciberataques a aplicaciones web a partir de análisis de patrones de comportamiento utilizando el SIEM de código abierto OSSIM, de esta manera se logra un sistema de detección temprana de ataques que podría ser generalizado en las entidades del país. En este mismo sentido el artículo "SOLUCIÓN DE CIBER-SEGURIDAD PERIMETRAL PARA REDES DE DATOS EMPRESARIALES" propone una solución de seguridad para proteger el tráfico de entrada y salida de las redes informáticas de una entidad, integrando el filtrado de paquetes, prevención contra intrusos, y detección de malware entre otras capacidades.

Desde el punto de vista de la protección de los datos empresariales, el artículo "CERTIFICADO DIGITAL DE DOCUMENTOS PDF EN DISPOSITIVOS CON SISTEMA OPERATIVO ANDROID", propone una herramienta para proceder a la firma digital de documentos PDF procesados en dispositivos Android. Este es un ejemplo de la implementación de certificados digitales y buenas prácticas en el manejo de la información, proceso que necesita de mayor concientización por parte de los directivos y de todos individuos involucrados en la seguridad.

Muy interesante resulta la propuesta de "SERVICIOS DE AUTENTICACIÓN Y AUTORIZACIÓN ORIENTADOS A INTERNET DE LAS COSAS**",** donde se propone el uso de certificados digitales para garantizar la robustez de la seguridad en el entorno de este tipo de dispositivos. Teniendo en cuenta que el

ambiente IoT ha sido uno de los más atacados por los cibercriminales, es imprescindible emplear estos y otros métodos para garantizar su seguridad.

En los trabajos propuestos se refleja la labor que realizan entidades de Cuba relacionadas con la ciberseguridad para contribuir a la informatización de la sociedad de manera segura y con independencia tecnológica. Confiamos que la presentación de estos temas cree conciencia sobre los riesgos de ciberseguridad existentes al informatizar la sociedad y que sirva de acicate para que otros investigadores contribuyan con trabajos en esta importante área.

Juan Miguel Alonso Torres
Director de Desarrollo, Segurmática.
Presidente Comité Científico. Seminario Iberoamericano de Seguridad de la Tecnologías de la Información.