BOLETIN DE PRENSA

Boletín número 4533
Ciudad Universitaria, 30 de noviembre de 2022

Realiza la UAEM Jornada de Ciberseguridad

La Coordinación General de Planeación y Administración de la Universidad Autónoma del Estado de Morelos (UAEM), a través de la Dirección General de Tecnologías de la Información y Comunicación (DGTIC), realizaron hoy la Jornada de Ciberseguridad 2022, en el marco del Día Internacional de la Seguridad de la Información.

Esta jornada realizada en formato virtual, tuvo por objetivo presentar a diversos especialistas en ciberseguridad para que impartieran conferencias que ayuden a crear conciencia sobre las amenazas informáticas y riesgos que cualquier persona puede enfrentar al hacer uso de las tecnologías de la información y comunicación, informaron Juan Miguel Mialma López, director de Sistemas Académicos de la DGTIC y Guadalupe Salgado Dorantes, jefa del Departamento de la Unidad de Recursos Digitales Académicos.

La primera conferencia del día estuvo a cargo de Beatriz Romero Valencia, colaboradora de la Dirección de Gestión de la Calidad de la UAEM, quien habló sobre las *Generalidades de la Norma ISO/IEC 27001:2013 y su aplicación*, la cual se trabaja actualmente para implementar en la DGTIC.

La Norma ISO 27000 es una familia de normas internacionales que permiten el aseguramiento, la confidencialidad e integridad de los datos y la información, así como de los sistemas que la procesan. El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información, permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos, además mejora la competitividad y la imagen de una organización, acompañadas de buenas prácticas.

Beatriz Romero explicó que esta familia de normas, han evolucionado con el tiempo y consideran diversas actualizaciones, prácticamente cualquier organización puede implementar las normas que certifican la gestión de la seguridad de la información, además, proponen como fases el ciclo PVHA que indica: Planear, Hacer, Verificar y Actuar.

En este sentido, las fases de un subsistema de control estratégico, permiten establecer metas y objetivos, determinar métodos para alcanzar dichas metas, contar con personal competente y subsistema de control de evaluación, medir el desempeño, tomar acciones de mejora de los resultados y estandarizar, en un ciclo continuo para el buen desarrollo y prácticas de este Sistema de Gestión de la Seguridad de la Información.

Romero Valencia, destacó que la parte medular de la Norma ISO 27001, es la planeación para dirigir e identificar los riesgos de la seguridad de la información, los criterios de aceptación de estos riesgos y evaluar si los resultados obtenidos son consistentes, válidos y evaluables, mantener la información documentada que quede como evidencia de la realización de este proceso.

Los expositores de esta jornada impartieron algunas recomendaciones para evitar robo y/o pérdida de la información, entre otros aspectos, como: *Amenazas de ciberseguridad, perspectiva actual,* a cargo de Sofía Bahena Ángeles, integrante de la Policía Cobernética del estado de Morelos; *Ransomware, medidas preventivas desde un contexto personal y profesional*, impartida por Roberto Espinosa Andrews, colaborador en Hillstone Networks; *Modelo de ciberseguridad Zero-Trust*, a cargo de Carlos Eduardo Villanueva, SE Senior en NetScout; *Ciberseguridad de las mujeres frente a la violencia digital*, impartida por Karla Patricia Alas de Duarte, co-líder del Programa Geek Girls; y *Privacidad de la información de personas usuarias en el uso de servicios digitales*, a cargo de Jesús Coquis Romero, director de Regulación en Materia de Usuarios del Instituto Federal de Telecomunicaciones.

Por una humanidad culta
Una Universidad de excelencia