



Source:

Tomado de Cubadebate

Como parte de la jornada nacional de ciberseguridad en Cuba, comenzó en la mañana de este lunes el taller Ciberseguridad en las Telecomunicaciones 2023, un encuentro científico nacional promovido por la Empresa de Telecomunicaciones de Cuba SA (Etecsa) para concientizar a los usuarios sobre las buenas prácticas en el espacio virtual.

Esta es la cuarta edición del taller, que se desarrollará hasta el miércoles 29 de noviembre en el Teatro San Ambrosio, en el Parque Histórico Militar Morro-Cabaña.

Asistieron a la jornada inaugural el viceministro de Comunicaciones, Ernesto Rodríguez Hernández, la presidenta ejecutiva de Etecsa, Tania Velázquez Rodríguez, el vicepresidente de Inversiones de Etecsa, Luis Adolfo Iglesias Reyes, el director central de la División de Operaciones de Seguridad de Etecsa, Pablo Domínguez Vázquez, directivos, estudiantes y representantes de organismos e instituciones cubanas relacionadas con la ciberseguridad.

En las palabras de apertura, Domínguez Vázquez dijo que el taller “no se trata solo de hacer un alto para reflexionar e intercambiar sobre temas de vital importancia en el abordaje de uno de los mayores desafíos que tiene la humanidad, sino de hacerlo con un enfoque creativo e integrador en el que aunemos fuerzas para enfrentar las crecientes amenazas que se ciernen sobre el ciberespacio internacional”.

Para el directivo de Etecsa, será “un espacio apropiado para el intercambio profesional e incrementar las tan necesarias relaciones de cooperación con un objetivo común: fortalecer la seguridad del ciberespacio nacional, y con ello contribuir a la transformación digital de nuestra sociedad”.

El primer panel de Ciberseguridad en las Telecomunicaciones 2023 fue “Seguridad en los sitios web, tendencias actuales, principales amenazas, controles proactivos”.

Los panelistas analizaron el estado de la seguridad de las aplicaciones web, que tienen un papel preponderante en el desarrollo digital de la sociedad, y sus vulnerabilidades.

El MSc. Henry R. González Brito, jefe de la carrera de Ciberseguridad en la UCI y moderador del panel, señaló que se ha producido un incremento de las vulnerabilidades en las aplicaciones web a nivel global.

Para apoyar su exposición, citó la lista de los 10 mayores riesgos de seguridad en las aplicaciones web, que publicó OWASP (Open Web Application Security Project) en 2021.

Algunos de esos riesgos son la pérdida de control de acceso, las fallas criptográficas, el diseño inseguro, una

configuración de seguridad incorrecta, componentes vulnerables y desactualizados y fallas de identificación y autenticación.

Por su parte, Yan Carlos Sainz Rodríguez, de la Empresa de Tecnologías de la Información (ETI) de BioCubaFarma, abordó las buenas prácticas en el hospedaje seguro de aplicaciones web.

Definió como buenas prácticas los certificados SSL (que garantizan que terceros no intercepten información privada como nombres de usuario y contraseñas), el monitoreo del sitio, la protección contra ataques DDoS (denegación de servicio distribuido), las salvas periódicas, el escaneo de seguridad y la seguridad por niveles.

Sainz Rodríguez también explicó los servicios de ciberseguridad que presta la ETI: diagnóstico de seguridad informática, protección criptográfica, análisis de trazas, consultoría para la gestión segura de redes, entre otros.

Otro tema que abordó el panel fue la importancia de la certificación de la seguridad de las tecnologías de la información.

La certificación mejora la seguridad de la información, genera confianza en los clientes y aumenta la competitividad.

El ingeniero Juan Alfredo Guerra Góngora, de la Dirección de Seguridad Tecnológica de Etecsa, presentó la experiencia de la empresa en controles y pruebas de seguridad en aplicaciones web.

De acuerdo con Guerra Góngora, Etecsa creó una arquitectura de cinco fases para evaluar la seguridad en ese tipo de aplicaciones.

Esa arquitectura se basa en un marco regulatorio, una guía de autoevaluación y desarrollo seguro, un control y prueba de seguridad, y un análisis de riesgo.

“Para nuestra empresa, las pruebas de seguridad son un mecanismo esencial para determinar los riesgos de las aplicaciones y decidir si pueden entrar en producción”, dijo.

Los panelistas refirieron la poca percepción de riesgo de las personas en temas de ciberseguridad.

El segundo panel de la jornada se tituló “Gestión de incidentes de ciberseguridad”.

Su moderador, el director central de la División de Operaciones de Seguridad de Etecsa, Pablo Domínguez Vázquez, explicó los vectores de ataque (vías desde las que se pueden originar violaciones a la ciberseguridad).

Mencionó vectores como los correos o SMS, la navegación web, aplicaciones y contraseñas comprometidas.

“Desde 2021, Cuba cuenta con un modelo de actuación para enfrentar incidentes, la Resolución 105, del Ministerio de Comunicaciones, que prevé cuatro etapas fundamentales, empezando por la preventiva”, dijo.

Los desafíos y la gestión de la ciberseguridad en el país, el phishing y la minería de criptomonedas también fueron analizados en el panel.

En la tarde, el rector de la UCI, Raydel Montesinos Perurena, impartió la conferencia magistral “Ciberseguridad: Estado actual, retos y perspectivas”.

Montesinos Perurena dijo que el robo de información mediante programas malignos es “una gran preocupación”.

Asimismo, dedicó un segmento de la conferencia a la relación de la inteligencia artificial con la ciberseguridad y su uso en los ciberataques.

El rector de la UCI ahondó en la evolución de los programas académicos dedicados a la ciberseguridad en ese centro docente, que comenzaron en 2016, con un programa de educación superior de ciclo corto en Administración de Redes y Seguridad Informática.

También mencionó que la primera graduación de la carrera Ingeniería en Ciberseguridad será el año próximo.

“La importancia de este evento es que ayuda a concientizar a los usuarios”

“La idea del taller es cambiar la visión que se tiene de la ciberseguridad desde el punto de vista de esa dimensión puramente tecnológica, y compartir un grupo de buenas prácticas, de formación, modelos y métodos de protección de riesgo que ayuden a proteger los activos de las organizaciones y los usuarios en el ciberespacio”, afirmó Armando Tito Bertot, jefe del Departamento de Supervisión de Ciberseguridad de Etecsa.

Cuatro ejes temáticos son la base del evento: criptografía, fraude de las telecomunicaciones, seguridad digital y el marco legal.

El también presidente del Comité Científico del taller Ciberseguridad en las Telecomunicaciones 2023 señaló que, en varios foros prestigiosos, como la Unión Internacional de Telecomunicaciones, se habla de seguridad digital como el estadio o fase superior de la ciberseguridad que tiene que ver con el desarrollo mediante nuevas tecnologías.

También se refirió a la campaña de comunicación que desarrolló Etecsa durante el año para fomentar la cultura digital en los clientes y concientizar sobre los riesgos del ciberespacio.

“La importancia de este evento es que ayuda a concientizar a los usuarios”, dijo

Para Bertot, “uno tiene una responsabilidad social con el cliente y debe entender que la generación de valor económico implica la generación de valor social”.

---