Gestión Unificada de la Ciberseguridad Tecnológica: Alianza vital para evitar males

14/11/2019

El II Taller de Ciberseguridad en las Telecomunicaciones ETECSA 2019 en su jornada correspondiente a este miércoles y con sede en el Hotel Comodoro abordó temas de Ciberseguridad en las Telecomunicaciones y en los dispositivos terminales.

Una de las ponencias desarrolladas durante el día fue ofrecida por el Ministerio del Interior (MININT) la cual abordó el tema de las Experiencias en la Gestión Unificada de la Ciberseguridad Tecnológica en los OACE y entidades priorizadas.

En la ponencia se explicó cómo el desarrollo actual de las Tecnologías de la Informática y las Comunicaciones avanzan a un ritmo vertiginoso, provocando que, en su evolución, se incremente aceleradamente el número de usuarios en las redes de comunicaciones y los servicios. Variadas son las aplicaciones que se desarrollan y despliegan para cumplir con los requisitos de una sociedad cada vez más informatizada.

Con el paso de los años nuevos consumidores acceden a Internet en busca de información, así mismo empresas u otras entidades privadas el gobierno crean espacios para que sus usuarios mantengan un ciclo de retroalimentación adecuado a los tiempos actuales.

Sin embargo, el proceso de Informatización trae consigo una contrapartida porque, aunque se haya dado respuesta activa a los requerimientos de la sociedad, se manifiestan nuevos riesgos que incluyen fraudes informáticos, corrupción, manipulación de la información almacenada en bases de datos y abuso de privilegios sobre los sistemas con el fin de satisfacer necesidades personales.

Para mitigar los riesgos que implica una infraestructura de esta envergadura se han desplegado distintos equipos de seguridad, los cuales protegen el perímetro establecido por la organización, de ataques provenientes del exterior o accesos no autorizados dentro de una misma red.

Cada dispositivo desplegado en la red, ya sea Cortafuegos o Detector de Intrusiones de Hosts o Red generan un registro único de cada evento ocurrido, lo cual permite realizar análisis forenses ante la ocurrencia de violaciones o bien visualizar, en tiempo real, el comportamiento de la infraestructura. El análisis de estos registros constituye un punto clave, pues permite obtener conocimiento sobre las actividades que se llevan a cabo en la infraestructura a partir de eventos y notificaciones.

Para mantener una supervisión sistemática sobre estos elementos se hace necesario establecer una Plataforma de Supervisión de la Ciberseguridad Tecnológica, que aporte conocimientos y permita estar al tanto de las principales vulnerabilidades y ataques favoreciendo la toma de decisiones y la aplicación de medidas técnicas que garanticen la seguridad y vitalidad de los sistemas.

Durante la conferencia se abordaron además las principales experiencias adquiridas por la empresa en la Supervisión de la Ciberseguridad Tecnológica.