Taller No.4

Lea el material, analice, sintetice, complete el diario de doble entrada. Pd: no es copiar y pegar, donde dice opinión del autor puede poner parte del material, pero lo que plasme en los demás cuadrantes debe ser de su entendimiento, favor completar todos los cuadrantes, justificar texto, revisar ortografía, y demás. Fecha de entrega sábado 7-5-22 (enviar al correo), si por algún motivo no puede enviarlo en la fecha establecida puede hacerlo luego pero no ganara la misma nota.

**Realizado por: Billy Aizpurúa Pittí (4-808-145)**

**DIARIO DE DOBLE ENTRADA**

|  |  |
| --- | --- |
| **Opinión del Autor** | **Opinión Personal** |
| Este documento trata acerca de los delitos informáticos que son infracciones que se realizan a través de las nuevas tecnologías emergentes y tienen el objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos, en la actualidad se conocen diversas situaciones donde las acciones en ciberdelitos han causado un gran número de incidentes en diversos países por ende es de vital importancia que se conozca acerca de los mismos y el cómo poder actuar para solventarlos.  También se documentan diversos tipos de incidentes como son los fraudes cometidos mediante manipulación de computadora, manipulación de datos de entrada, piratería informática entre otros, todos estos delitos tienen una forma de disminuir que pasen en cualquier institución por ende es importante conocerlos; debido a lo mismo e han creado leyes e instituciones que tratan de realizar documentación acerca de los mismos y en caso de que se den cual sería sanción como es la ley 78 del 22 de octubre del 2013 que trata de tipificar los delitos y realizar acciones similares al acuerdo Budapest | Este documento nos sirvió para conocer los diversos delitos que se dan en el área de tecnologías de la información y como estos afectan en si al entorno que nos rodena debido a que prácticamente todos usamos un tipo de tecnología todos los días.  También podemos observar que en Panamá ya existen algunas leyes acerca de cómo las instituciones deberían salvaguardar sus datos y que sucede si estos son vulnerados, pero estos avances en leyes son mínimos con los avances que tiene las diferentes tecnologías y los delitos que se pueden cometer en las mismas por ende es de vital importancia poner suma atención a que en los próximos años mejore los procesos legales en cuanto a lo que se refiere al área de tecnología; pero otro punto importante para que esto suceda es poder capacitar a la población en general acerca de cómo defender su privacidad y sus datos en un entorno virtual |
| **Aspectos Relevantes (5)** | **Conclusiones ( 2 )** |
| * Actualmente Panamá no cuenta con una base sólida para proteger sus datos si llegara a suceder un ataque masivo a entidades que tengan datos sensitivos. * Nuestro país en cuanto a leyes ligadas al área de tecnología estamos dando los primeros pasos para establecer cuáles van a ser las reglas que van a regir los mismos. * Pudimos conocer los diversos tipos de ataques cibernéticos que se dan actualmente. * Ya existe la existencia de antecedentes como es el convenio de Budapest, solo faltaría establecer una forma de cómo realizar o implementar estos consejos en nuestro país. * Toda persona que tenga contacto con tecnología y datos debería tener el conocimiento mínimo para saber cómo resguardar los mismos | * Panamá está realizando sus primeros pininos en el área de tecnología y gracias a diversos factores esto se ha dado de una forma un poco acelerada por ende es de vital importancia que se establezcan las leyes pertinentes para poder proteger a los ciudadanos y personas que día a día utilizan tecnología dentro del territorio nacional * Cada día se comenten miles de ciberdelitos y esto en los próximos años van a ir en aumento exponencialmente por eso es importante que la sociedad tenga el conocimiento de cómo protegerse ante estas amenazas además que se incentive a más personas a estudiar y conocer acerca del mundo de la tecnología |