

## **GLOSARIO**

### **1. SEGURIDAD ACTIVA:**

Es la prevención de los ataques o amenazas en tiempo real con la finalidad de mantener la estabilidad y eficacia de la seguridad.

### **2. SEGURIDAD PASIVA:**

Reduce el impacto del daño a través de un conjunto de medidas reactivas para evitar cualquier ataque.

### **3. VULNERABILIDAD:**

Es una debilidad o falla hacia riesgos desconocidos en un sistema.

### **4. NESSUS:**

Es una herramienta de ciber seguridad que realiza el escaneo para identificar malware y partes traseras y además se utiliza para explorador de puntos débiles

### **5. MALWARE:**

Software malicioso que tiene un código para el robo de datos y es usado por los ciber delincuentes

### **6. HOSTING:**

Es el servicio que permite almacenar los archivos, bases de datos, imágenes y otros contenidos de un sitio web en un servidor para que este sea accesible en Internet.

### **7. OUTSARCING:**

Comprenden una externalización de labores informática a manos de un tercero.

### **8. Software y desarrollo de programas:**

Constatar la venta de un producto que conlleva licencias y otros trabajos

### **9. Mantenimiento:**

Es el buen funcionamiento del hardware y del software.

### **10. Consultoría:**

Esta orientada a implementar mejoras.