

# **Unidad III**

## **La seguridad informática**

### **3.1. Conceptos básicos: Sistemas confiables.**

Una forma de mejorar la habilidad de un sistema de defensa contra intrusos y programas maliciosos, es implementar tecnología de Sistemas Confiables (Trusted Systems).

### **3.2. Ataques internos, ataques externos.**

Los ataques externos, a pesar del impacto que causan en la opinión pública, no han resultado tan caros en comparación con los internos", enfatizó el experto.

### **3.3. Políticas de seguridad:**

#### **3.3.1. Creación de un plan,**

La Dirección ha definido y documentado esta Política de Seguridad asegurando que:

Es adecuada al propósito de la Organización.

Incluye el compromiso de cumplir con los requisitos de los clientes y de mejorar continuamente la eficacia del Sistema de Gestión

Proporciona un marco de referencia para establecer y revisar los objetivos.

Se comunica a todos los empleados de ACTIONS DATA y a las personas que trabajan en su nombre.

#### **3.3.2. Procedimientos,**

Un manual de procedimientos es el documento que contiene la descripción de actividades que deben seguirse en la realización de las funciones de una unidad administrativa, o de dos o más de ellas.

El manual incluye además los puestos o unidades administrativas que intervienen

precisando su responsabilidad y participación.

Suelen contener información y ejemplos de formularios, autorizaciones o documentos necesarios, máquinas o equipo de oficina a utilizar y cualquier otro dato que pueda auxiliar al correcto desarrollo de las actividades dentro de la empresa.

En el se encuentra registrada y transmitida sin distorsión la información básica referente al funcionamiento de todas las unidades administrativas, facilita las labores de auditoria, la evaluación y control interno y su vigilancia, la conciencia en los empleados y en sus jefes de que el trabajo se está realizando o no adecuadamente.

### **3.4. Evaluación de riesgos:**

#### **3.4.1. Activos a proteger,**

serían ya el máximo nivel que podemos obtener de protección del mismo. Cuando todo lo demás falla, los activos físicos deberían de permanecer. De modo que estos seguirían siendo útiles. No estamos hablando de un apocalipsis zombi, sino de una crisis muy fuerte, como algunas de las que se han vivido a lo largo de la historia.

Un ejemplo de un **buen activo físico es una vivienda**. Tiene una utilidad que es alojarse en la misma, existe un buen sistema de protección de la propiedad, etc. En cambio un mal activo físico en el que invertir es un ordenador, puesto que la obsolescencia lo hace cada vez más inútil a medida que salen mejores modelos de la competencia.