# **5. Vista de seguridad**

La seguridad informática es definida como el proceso de prevención y detección del uso no autorizado de un sistema informático e implica la protección de los recursos informáticos contra intrusos con intenciones maliciosas.

Para que esta vista del software sea de calidad, debe seguir atributos de calidad (conocidos también como “requerimientos no funcionales” o “propiedades de calidad”). Se entiende por atributos de calidad como “propiedades medibles de un sistema informático que indique qué tan bien el sistema satisface las necesidades de los usuarios finales”. Todo atributo de calidad posee los siguientes elementos:

* Origen del estímulo: se indica a cualquier actor que se encontrará interactuando con el sistema.
* Estímulo: condición que debe considerarse cuando arriba al sistema.
* Ambiente: condiciones en la cual el sistema informático se encuentra en el momento que el estímulo es recibido.
* Componentes: hace referencia a los componentes del sistema que son afectados con el estímulo.
* Respuesta: actividad que realiza el sistema.
* Medida de la respuesta: tipo de medida con la cual debe cumplir la respuesta de modo que el requerimiento pueda ser testeado.

Las siguientes áreas son abarcadas por la seguridad informática. Estas son: Disponibilidad, Confidencialidad e Integridad. Para cada una de ellas debe realizarse el análisis correspondiente en cuanto a los atributos de calidad del software.



## **5.3. Integridad**

La integridad de los datos registrados hace referencia a la correctitud y completitud de la información almacenada en una base de datos. Lo que se busca es garantizar que los datos ingresados no sean alterados o modificados sin la autorización correspondiente.

En nuestro sistema, cada usuario no administrador es capaz de registrar su información respectiva y de cambiarla si fuese necesario. Los usuarios no administradores podrán borrar o actualizar un usuario no administrador que ya no conviva en un condominio, de modo que el nuevo vecino pueda registrarse sin algún inconveniente.

El sistema a realizar debe ser capaz de velar por la integridad de los datos personales. Cuando la integridad de datos es segura, tanta información que sea almacenada en una base de datos seguirá fiable y completa por mucho tiempo que esté almacenada o en cada ocasión que se acceda a ella.

|  |  |
| --- | --- |
| **Elemento** | **Descripción** |
| Origen del Estímulo | Intruso o agente externo al sistema |
| Estímulo | Alteración, modificación u obtención de información registrada en el sistema |
| Ambientes | En todo momento |
| Componentes | Todo el sistema |
| Respuesta | Administración de usuarios, restricción de ip |
| Medida de la Respuesta | Número de modificaciones de datos de forma ilícita ya sea a nivel interno o externo (hacker) |