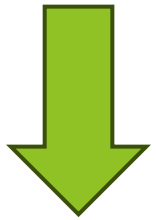
Seguridad Informática

Introducción

¿Qué es Seguridad?

- Ausencia de peligro o riesgo.

- Sensación de total confianza que se tiene en algo o alguien.



Entonces en Informática o I.T

¿Qué debemos Proteger?

¿Qué debemos Proteger?

Son Activos de una Organización

- Información.
- Equipos.
- Usuarios.

SON:
- Vulnerables.
- Amenazados.
- Atacados.

Generan:
- Riesgos.
- Impactos.
- Sufren Desastre.

¿Qué es la seguridad Informática?

¿Qué debería tratar o de que se debería encargar?

Se encarga de generar el conjunto de ***herramientas, técnicas, procedimientos y equipos***, con el fin de garantizar los niveles acordados de CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD, en una Organización o Sistema Informático.

Entonces tenemos:

- Herramientas.
- Técnicas.
- Procedimientos.
- Equipos.

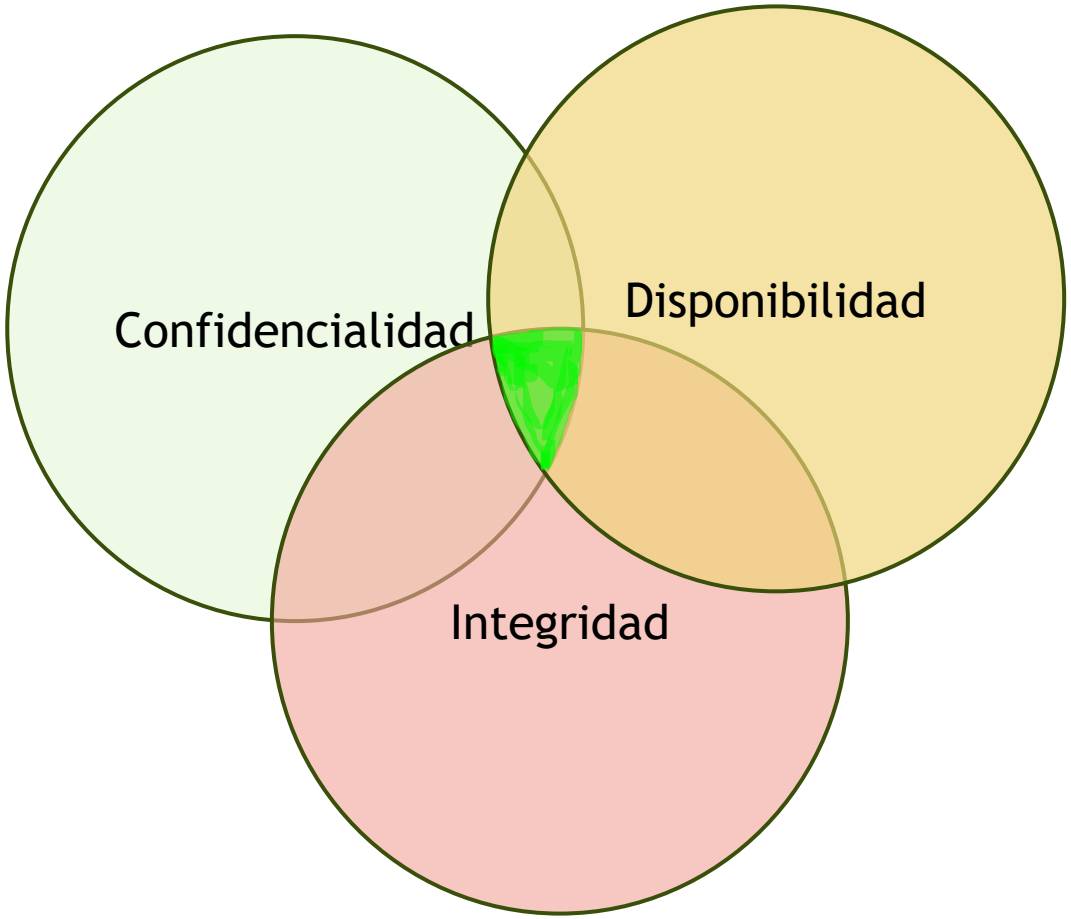
Para Lograr

Surgen los tres pilares de la seguridad

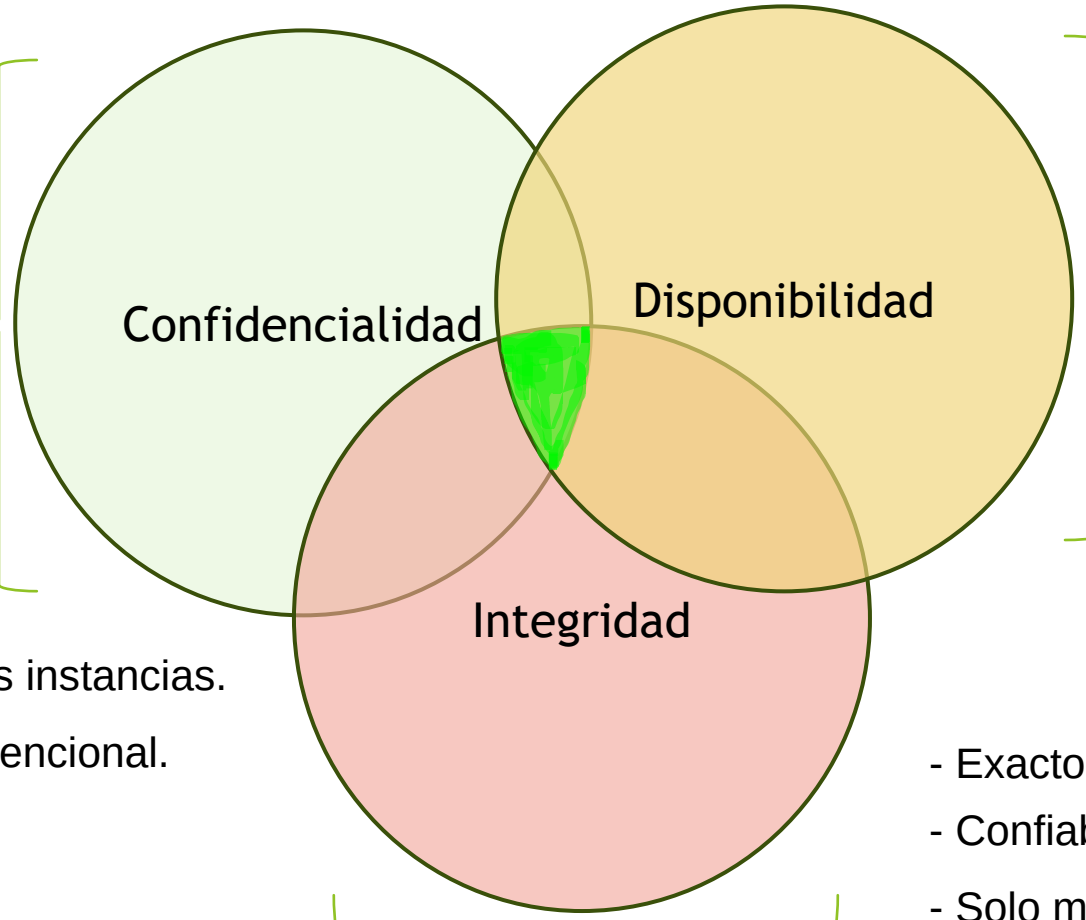
Se reflejan en:

- Políticas de Seguridad.
- Plan de Contingencia.

Nivel de Seguridad



Nivel de Seguridad



- Solo para Personas o Procesos Autorizados.
- Capacidad de Procesamiento.
- Nivel adecuado de Performance.

Plan de Contingencia

- Resguardo
- Recuperación
- Redundancia

-Control de Acceso

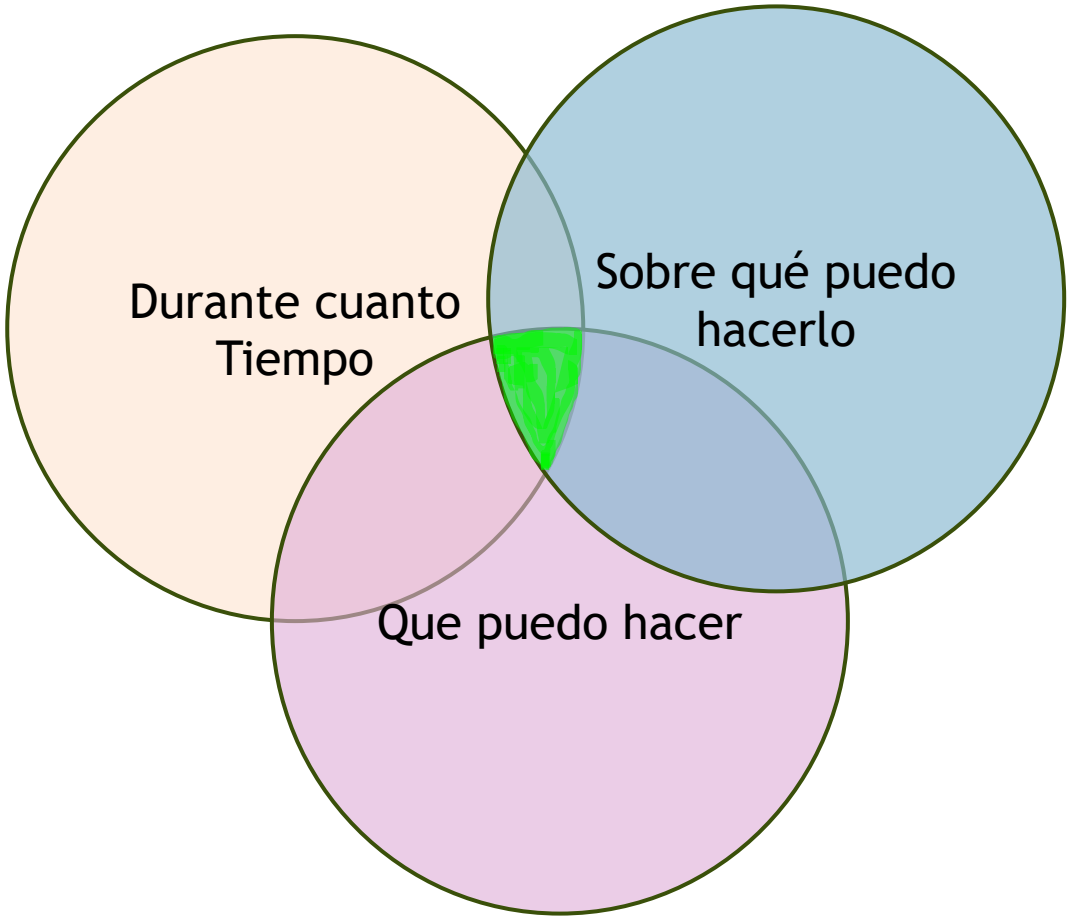
-Ingeniería Social

- Personal autorizado.
- Secreto en todas sus instancias.
- Perdida Casual o Intencional.

- Exacto.
- Confiable.
- Solo modificado por Personas y Procesos Autorizados.

Mínimos Privilegios

Mínimos Privilegios



Aumenta el nivel de Seguridad

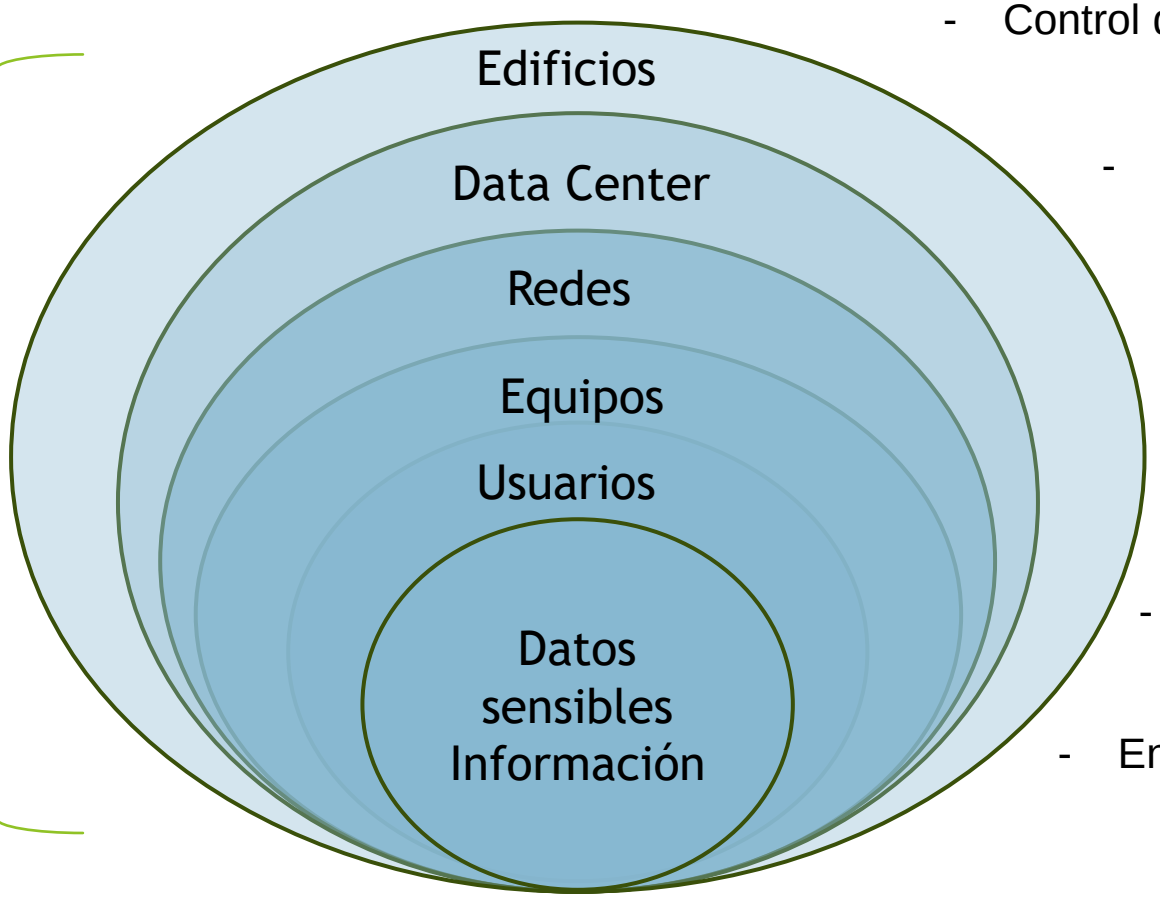
Niveles de Seguridad Informática

- Bajo normativas Nacionales e Internacionales.

- Políticas de Seguridad.

- Plan de Contingencia.

- Capacitación.



- Control de Acceso
- Performance
- Segmentación de Redes
- Configuración Robusta
- Gestion de usuarios
- Encriptación

Fin Introducción

Seguridad Informática y de la Información

Seguridad FÍSICA: cuando se protege la parte *hardware* del sistema informático de amenazas materiales, ya sean provocadas o accidentales.

Seguridad LÓGICA: cuando es el *software* lo que se protege, es decir, programas y datos.

Seguridad Aplicada

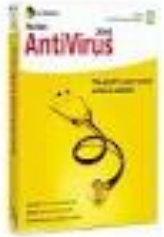
Seguridad ACTIVA: la que se aplica con el objeto de **detectar** y/o **prevenir** amenazas.

Seguridad PASIVA: aquella que, una vez producido el ataque, error o daño, se aplica para **reducir** al máximo los efectos producidos y, en la medida de lo posible, **recuperar** el sistema.

FÍSICA

vs

LÓGICA



ACTIVA

vs

PASIVA

Vulnerabilidades

- Se trata de cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático.

- Estos “agujeros de seguridad” pueden estar relacionados con múltiples causas. Es muy importante corregir cualquier vulnerabilidad detectada, porque constituye un peligro potencial para el sistema en general.

Amenazas

- Son cualquier entidad o circunstancia que atente contra el buen funcionamiento de un sistema informático.

- Hay amenazas que afectan a los sistemas de forma involuntaria, como, por ejemplo, un desastre natural.

Amenazas pasivas: su objetivo es obtener información relativa a una comunicación.

Amenazas activas: tratan de realizar algún cambio no autorizado en el estado del sistema.

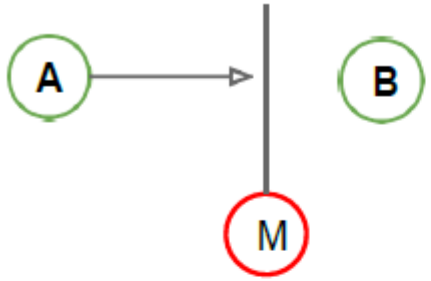
Ataques

- Son acciones que tratan de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control del mismo.

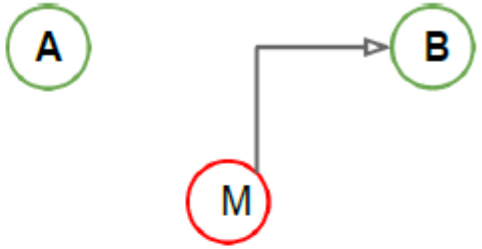
- Se trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema.

- Normalmente un ataque informático pasa por las siguientes fases: reconocimiento, exploración, obtención de acceso, mantenimiento del acceso y borrar las huellas del ataque.

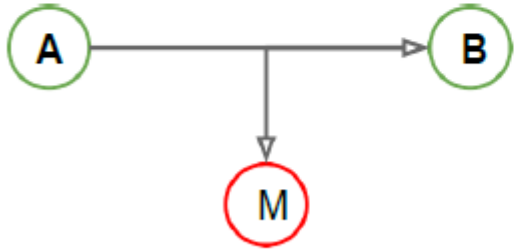
Posibles ataques a la información



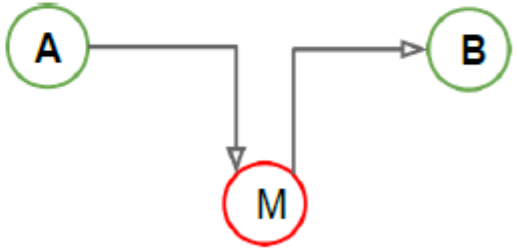
INTERRUPCIÓN



GENERACIÓN



INTERCEPTACIÓN



MODIFICACIÓN

Riesgo

Trata de estimar en una medida cual es la probabilidad de que se materialice una amenaza.

El impacto sería, cual es el alcance o daño causado en el caso de que una amenaza se materialice.

Aumento del Riesgo

Minimizar el Riesgo

Integridad

- Consiste en garantizar que la información solo pueda ser **modificada** por las personas autorizadas o usuarios legítimos, independientemente de su intencionalidad.

Confidencialidad

- Garantiza que la información solo es **accesible** e interpretada por personas o sistemas autorizados.

Disponibilidad

- Consiste en asegurar que la información es accesible en el **momento adecuado** para los usuarios legítimos.

Autenticidad

- Además, existen otros principios de seguridad que se consideran como deseables en todo sistema informático:

No repudio

No repudio de origen

No repudio de destino

Estructura y Dominios de Control

Políticas de Seguridad

- Se trata de una **declaración** de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.

- Tienen como objetivo **concientizar** a los miembros de una organización sobre la importancia y sensibilidad de la información y también de los servicios críticos.

Políticas de Seguridad

A la hora de elaborar las políticas de seguridad se deben tener en cuenta los siguientes aspectos:

- Generar las **reglas y procedimientos** para los servicios críticos.
- Definir las **acciones** que se ejecutaran y el **personal** que deberá estar involucrado.
- Clasificar los activos a proteger en función de su **nivel de criticidad**, de forma que los sistemas vitales sean los más protegidos y no se malgasten recursos en proteger aquellos activos con menor importancia.

Plan de Contingencia

- El plan de contingencia contiene **medidas detalladas** para conseguir la **recuperación del sistema**, es decir, creadas para ser utilizadas cuando el sistema falle, no con la intención de que no falle.
- Su creación debe abarcar las siguientes fases:

1.-Evaluación

2.-Planificación

3.-Realización de pruebas

4.-Ejecución

5.-Recuperación

- El plan de contingencia deberá ser revisado periódicamente para que siempre pueda estar de acuerdo con las **necesidades de la organización**.
- Algunas de las medidas que debe contemplar: tener redundancia, tener la información almacenada de manera distribuida, tener un plan de recuperación y tener al personal formado y preparado.