

PREVENCIÓN DE PÉRDIDAS

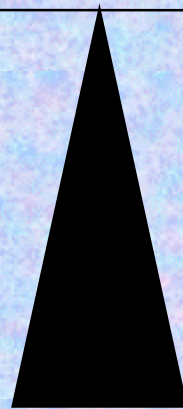
**Fraude Informático y
Seguridad Informática**

Lic. Pedro Bettoli

Los riesgos varían de un sistema informático a otro, por lo tanto los controles han de ser proporcionales a los riesgos.

RIESGOS


CONTROLES



FACTORES DE RIESGO EN UN SISTEMA INFORMÁTICO

Son todos aquellos que ponen en peligro la **integridad**, la **operatividad** y la **privacidad** de la información

	INTEGRIDAD	OPERATIVIDAD	PRIVACIDAD
Catástrofe climática		●	
Incendio		●	
Hurto		●	
Sabotaje	●	●	
Virus Informáticos	●	●	
Fraude Informático	●	●	●
Imponderables: Crisis del 200	●	●	
Intrusión		●	●



Mantener las tres características en el mismo nivel de importancia puede ser difícil en sistemas de mediana o gran complejidad

EJEM PLO 1

Sistema de cajeros automáticos de bancos

EJEM PLO 2

Sistema de un área de investigación y desarrollo

EJEM PLO 3

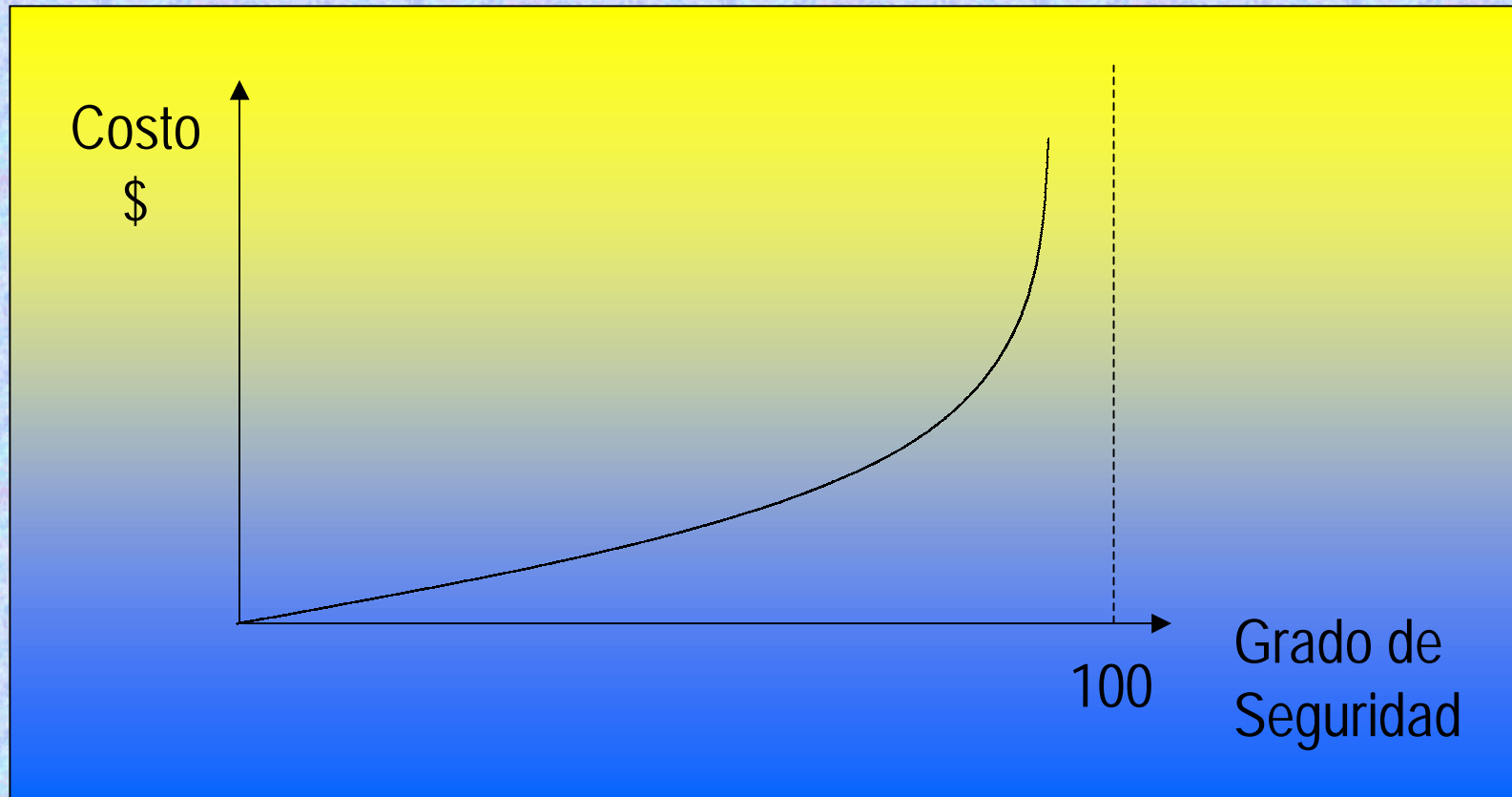
Sistema de un área de simulación y modelización matemática

EJEM PLO 4

Sistema de un área de administración contable



RELACION COSTO-SEGURIDAD

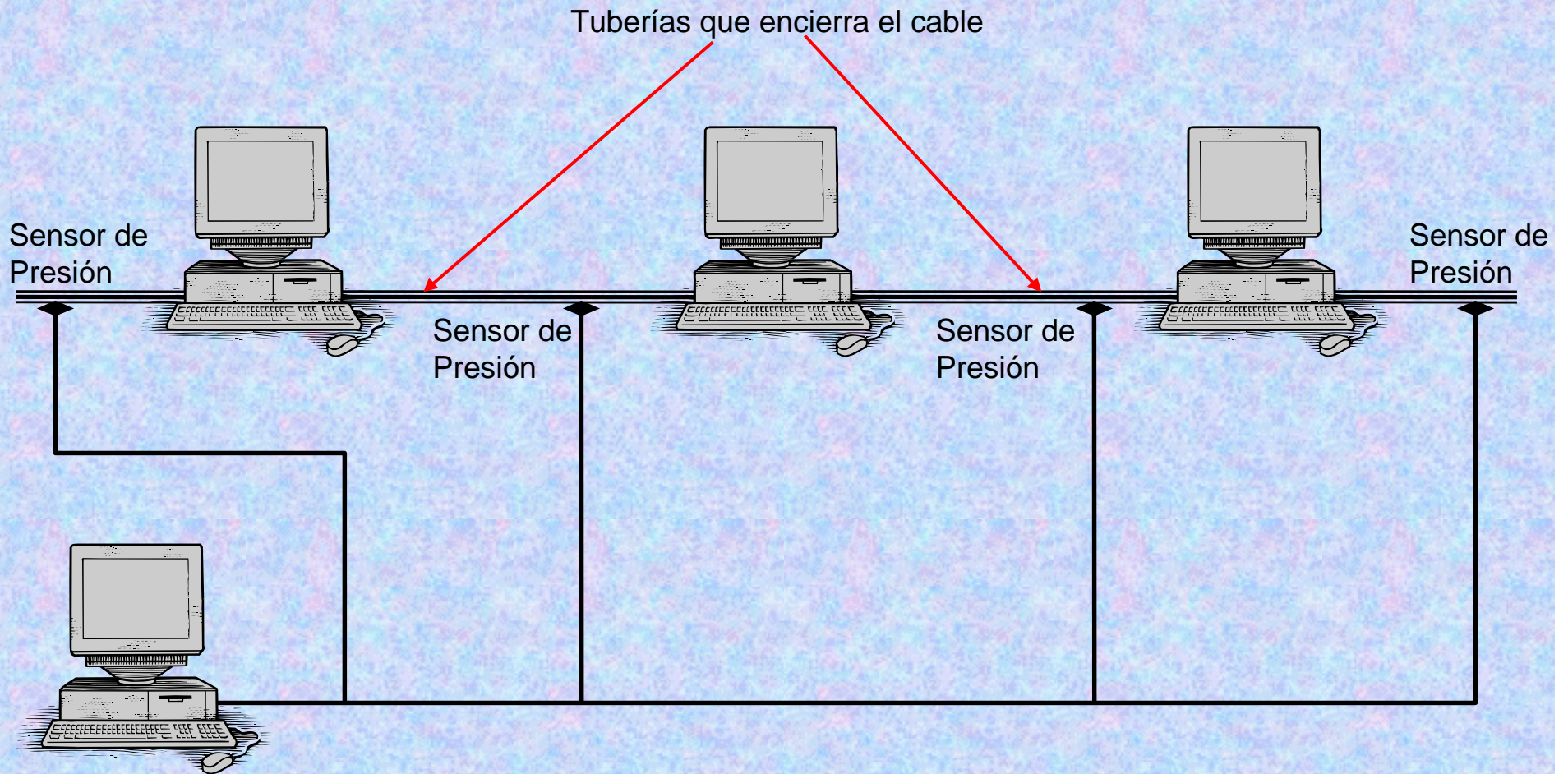


El **costo** de la seguridad de un sistema es, en principio, proporcional al grado de **seguridad** requerido. Pero esta proporcionalidad se pierde a medida que nos acercamos al 100% de seguridad y se vuelve exponencial.





EJEMPLO DE CALBEADO DE ALTO NIVEL DE SEGURIDAD




RELACION OPERATIVIDAD-SEGURIDAD

OPERATIVIDAD:

1

SEGURIDAD

La **operatividad** y la **seguridad** de un sistema son inversamente proporcionales, si una aumenta la otra disminuye. Esta es una de las leyes inamovibles de la seguridad informática.



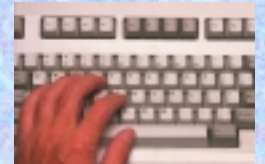
**FRAUDE
INFORMÁTICO**



MÉTODOS DE FRAUDE

TODO MÉTODO DE FRAUDE DEBE PASAR POR DOS ETAPAS:

1) ACCESO O ENTRADA AL SISTEMA



2) METODO DE MANIPULACIÓN



EL ACCESO O ENTRADA AL SISTEMA SE PUEDE DAR POR DOS MOTIVOS:

1 QUIEBRE DE CONFIANZA DEL PERSONAL DE LA EMPRESA

2 HABILIDAD DEL INTRUSO

Consecuencias:

IMPUNIDAD

ANONIMATO



TIPOS DE MANIPULACIÓN

FALSIFICACIÓN DE LOS DATOS DE ENTRADA

De los datos

+

De los códigos

-

ERRORES, MALOS AJUSTES Y DAÑOS AL HARDWARE

MANIPULACIÓN DE LAS BASES DE DATOS

MANIPULACIÓN CUENTAS TRANSITORIAS

MANIPULACIÓN DE DATOS DE SALIDA

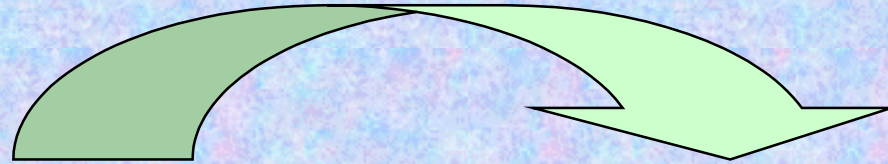
UTILIZACIÓN DE HERRAMIENTAS DE SOFT ESPECIALES

RETOQUES DE PROGRAMAS



CONCLUSIONES GENERALES

Podremos considerar que un sistema informático garantiza **LA SEGURIDAD** y previene **EL FRAUDE** cuando contempla los siguientes factores:



FACTOR HUMANO

- Motivación y ética del personal
- Conciencia de las consecuencias
- Profesionales interdisciplinarios

FACTOR TECNOLÓGICO

- Técnicamente confiable
- Políticas adecuadas

