# GUIA PARA TONTOS : TP 6.1 Seguridad

1) Identificar:

a) **VULNERABILIDADES**: "por donde me van a entrar" = debilidad que presenta un sistema inf.
ej: "falla en el protocolo" = "SO desactualizados" = "red insegura" = "falta de capacitación"

**ACTIVOS VULNERABLES**: son algunos de los siguientes. APUNTE FINAL PAG 142

- Hardware
- Software
- Datos e Información
- capacidad de procesamiento
- personal d?
- fondos

⚠ especificar QUÉ datos ⇒ ≠ impactos siempre

**AMENAZAS**: circunstancia, donde algo o alguien tiene el potencial de explotar una vulnerabilidad

ej: "obtención de contraseñas" = "intersección tráfico wifi entre PC y router" = "ataques a ciertos hosts" = "Ransomware"

**RIESGOS**: formato: "Existe una «X probabilidad» de que «amenaza» debido a «vulnerabilidad» causando «pérdida»"

Interesa poner esa cifra → IMPACTO (valoración de pérdida)

ej: "hay un 80% de probabilidad de que se obtengan las contraseñas aprovechando el fallo del protocolo WPA2 y que accedan a información" ACLARAR CUAL)

b) Clasificar AMENAZAS

sobre qué tipo de activos actúan

"intangible"

| | FISICO | LOGICO |
|---|---|---|
| ACCIDENTAL (no intencional) | - fallos en equipos<br>- fallo en sup.<br>- inundación<br>- incendio | - error del usuario<br>- error de programación<br>- error en la config. |
| DELIBERADA (premeditado) | - robo<br>- sabotaje | - virus<br>- piratería<br>- fraude<br>- hacker. |

ATAQUES
- PASIVOS → - no modifica info, solo escucha → - afecta confidencialidad de los datos
- ACTIVOS → - modifica info → - afecta integridad de los datos

c) políticas y medidas (por c/ política plantearnos varias)

- **Generales**: de carácter amplio, indican qué se puede hacer o no durante la operaciones de los sistemas.
- **De Aplicación Específicas**: indicaciones precisas, son como normas o reglas (deben refinarse)

**PROHIBITIVAS**: "todo lo que no está expresamente permitido está prohibido"

usar cuando necesito absoluto control de la situación

ej: "**Solo** se suministrarán (lo único permitido es) puntos de acceso a la red que tiene el protocolo WPA2 o versiones posteriores a la X (ej: en la que se solucionan dichos fallos).
"**Todos** los dispositivos que van a tener acceso a las redes deberán estar conectados a una VPN"

**PERMISITIVAS**: "todo lo que no está expresamente prohibido está permitido"

ej: "Se prohibe fumar en la sala donde se encuentran los servidores"

HAY UN DOC CON MUCHOS TIPOS Y EJEMPLOS, FIJATE AHÍ (pedir a peto)

Para cada Política, planteamos MEDIDAS → LINEAS DE DEFENSA

| | | | |
|---|---|---|---|
| 1° | Prevención | Evitar amenaza ocurra | -Se define la Política<br>-Detectar vulnerabilidades<br>-ej: "navegar por sitios c/ https"<br>"utilizar cierta VPN"<br>"actualizaciones necesarias" |
| 2° | Detección | Detener Amenaza | -Detectar ataques<br>-Primera línea fallo<br>-ej: "detector humo" |
| 3° | Recuperación | Amenaza tuvo éxito y tenemos que recuperar nos | -Se pierde el activo<br>-ej: "reemplazar puntos de acceso"<br>"backups" |

2)

a) ya vimos

b)

| Riesgo | Perdida Potencial | Consecuencia Primaria | Consecuencia Secundaria |
|---|---|---|---|
| | Activos Vulnerables | Los 3 aspectos<br>- Disponibilidad<br>- Integridad<br>- Confidencialidad | - Perdida confianza, imagen, prestigio, etc |

| Elementos Amenazados | Cantidad | Valor Unitario | Monto |
|---|---|---|---|
| | | | |

| Amenaza | Prob. Agresión | Prob Exito | Frec. de Perdida | Perdida Pot. ($) | Perdida Esperada ($) |
|---|---|---|---|---|---|
| | | | | | |

defines el rango vos

por ej:

BAJA: 0-25 %

INTERMEDIA 25-50 %

ALTA 50-75 %

MUY ALTA 75-100 %

Frecuencia perdida = Prob. Agresion × Prob. Exito

Perdida Esperada = Perdida Potencial × Frecuencia Perdida

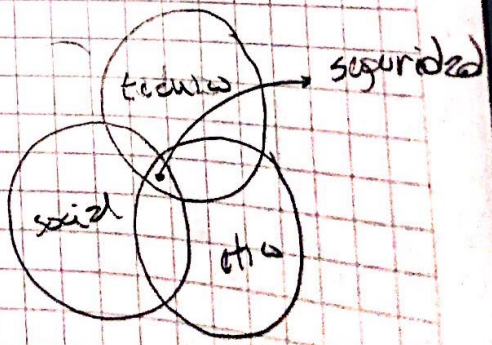
Costo daño potencial = Costo Perdida × Frecuencia Perdida

"modo seguro"

TECNICO: - Lineas de def. Herramientas Lab.
"Consistencia en datos"
"en la vida real viuda y casada en el sistema"

ETICO: valores sociales, que se debe hacer o no con la info. - confidencialidad

LEGAL: normas internas y ext. regulan uso de la info




"se superponen"