DOCUMENTO DE PROFUNDIZACIÓN

Teoría de la Información y la Comunicación

Recurso 1

Recurso 1

Un sistema de monitoreo registra los siguientes tipos de eventos:

Evento	Probabilidad
NORMAL	0.5
ALERTA	0.25
ERROR	0.15
CRÍTICO	0.10

Se pide:

1. Calcular la **entropía** $H(X)$

Fórmula para aplicar:

$$H(X) = -\sum p(x_i)\log_2 p(x_i)$$

Cálculo:

$$H(X) = -[0.5\log_2(0.5) + 0.25\log_2(0.25) + 0.15\log_2(0.15) + 0.10\log_2(0.10)]$$

Valores:

- $\log_2(0.5) = -1 \Rightarrow 0.5(-1) = -0.5$
- $\log_2(0.25) = -2 \Rightarrow 0.25(-2) = -0.5$
- $\log_2(0.15) \approx -2.737 \Rightarrow 0.15(-2.737) = -0.4106$
- $\log_2(0.10) \approx -3.322 \Rightarrow 0.10(-3.322) = -0.3322$

Suma:

$$H(X) = -(-0.5 - 0.5 - 0.4106 - 0.3322)$$
$$H(X) \approx 1.74 \text{ bits}$$

2. Calcular la **entropía máxima** H_{max}

Número de eventos (n):

$$n = 4$$
$$H_{max} = \log_2(4) = 2 \text{ bits}$$

3. Determinar la **redundancia** R

$$R = \frac{H_{max} - H(X)}{H_{max}}$$

$$R = \frac{2 - 1.74}{2} = 0.13$$

4. Interpretar el resultado en un contexto de ciberseguridad

   El sistema presenta baja redundancia (13%), lo que indica una alta variabilidad en los eventos.

   Interpretación:

   - No existe un evento dominante extremo
   - Hay diversidad de comportamiento
   - Puede representar:
     - Tráfico dinámico
     - Sistema en operación normal con variabilidad

   Sin embargo:

   - La presencia de eventos como **ERROR** y **CRÍTICO** sugiere monitoreo activo

Se recomienda análisis continuo para detectar cambios en la entropía