PUCE Virtual

CLASE

2

Teoría de la Información y la Comunicación

Tipos de Comunicación y Fundamentos Probabilísticos

QS WORLD UNIVERSITY RANKINGS

Educación de calidad

INTRODUCCIÓN DE LA CLASE

GRADO / POSGRADO / TECNOLOGÍAS

Estudia a tu tiempo
sin interrupciones

EDUCACIÓN EN LÍNEA DE CALIDAD

En el análisis de los sistemas de transmisión de datos dentro de una organización, especialmente en entornos donde la ciberseguridad es prioritaria, no basta con comprender cómo se envían los mensajes; es necesario entender qué tipo de comunicación se está utilizando, cómo circula la información y qué grado de incertidumbre caracteriza a los datos transmitidos. En este contexto, la teoría de la información proporciona las herramientas matemáticas que permiten medir la variabilidad, el riesgo y la previsibilidad de los flujos digitales.

Durante esta segunda semana se abordarán los distintos tipos de comunicación aplicados a sistemas organizacionales, los procesos que intervienen en entornos digitales como redes corporativas, servidores, firewalls o sistemas SIEM (Security Information and Event Management) y los fundamentos probabilísticos que permiten cuantificar el contenido informativo de los datos. Estas bases resultan esenciales para interpretar fenómenos como la generación de logs, la detección de anomalías o la evaluación de tráfico sospechoso. Desde la perspectiva de la teoría matemática de la información, la comunicación no es únicamente un proceso social, sino un fenómeno cuantificable. Autores como Alencar (2015) y Csiszár y Körner (2011) explican que los sistemas digitales pueden modelarse como fuentes probabilísticas cuyos símbolos presentan distintos niveles de incertidumbre. En ciberseguridad, esta incertidumbre puede asociarse con comportamientos normales o con patrones que revelan amenazas.

2 Tipos de Comunicación y Fundamentos Probabilísticos

2.1 Tipos de Comunicación

Desde la perspectiva de la Teoría de la Información, clasificar la comunicación permite modelar probabilísticamente los eventos, identificar patrones normales y detectar comportamientos atípicos. Para ello, la comunicación se clasifica según tres criterios complementarios:

1. Estructura del proceso comunicativo
2. Dirección del flujo de información
3. Naturaleza técnica del sistema de transmisión

Clasificación según su estructura

Es importante distinguir que las clasificaciones presentadas provienen de tradiciones teóricas distintas. La clasificación lineal, interactiva y transaccional proviene de la teoría de la comunicación social (modelos de Schramm y Barnlund).

En cambio, las clasificaciones unidireccionales/bidireccional y analógica/digital pertenecen a la teoría de sistemas de comunicación y a la ingeniería de telecomunicaciones.

a) Comunicación lineal

La información fluye en un único sentido, desde la fuente hasta el destino, sin retroalimentación directa. El receptor no influye sobre el mensaje una vez que este ha sido enviado.

Ejemplo:

- Un servidor envía logs automáticamente a un sistema SIEM.
- Un sensor IDS transmite alertas a una consola central.

En ciberseguridad: La comunicación lineal es común en sistemas de monitoreo automatizado.

b) Comunicación interactiva

Existe un intercambio de mensajes entre emisor y receptor, pero este se produce de manera alternada, no simultánea. Cada parte espera la respuesta de la otra antes de continuar.

Ejemplo:

- Un usuario ingresa credencial.
- El servidor responde validando acceso.
- El usuario recibe confirmación o rechazo.

Implicación en ciberseguridad: Permite autenticación, verificación y control de acceso en tiempo real.

c) Comunicación transaccional

Ambas partes envían y reciben información de manera simultánea y continua. El emisor y el receptor actúan al mismo tiempo, generando un flujo dinámico y bidireccional.

Ejemplo:

- Comunicación cifrada entre cliente y servidor mediante protocolo TLS.
- Intercambio continuo en una sesión VPN.

En ciberseguridad: La protección debe garantizar confidencialidad, integridad y disponibilidad en ambos sentidos. Además, desde el punto de vista probabilístico, los eventos están altamente correlacionados en el tiempo, lo que influye en el análisis de entropía y tráfico.

Clasificación según la dirección del flujo

Este criterio analiza hacia dónde se mueve la información y si existe o no intercambio en ambos sentidos.

a) Comunicación unidireccional

La información fluye en un solo sentido, desde el emisor hacia el receptor.

Ejemplo:

- Cámaras de seguridad enviando video a un servidor.
- Firewall enviando registros a un SIEM.

Ventaja: Reduce superficie de ataque en sistemas críticos.

Desventaja: No permite confirmación inmediata.

b) Comunicación bidireccional

Existe intercambio de datos en ambos sentidos.

Ejemplo:

- Autenticación en aplicaciones web.
- Consulta a base de datos con respuesta estructurada.

En términos probabilísticos, la bidireccionalidad permite modelar dependencias entre eventos, lo cual es relevante para el análisis de tráfico, detección de anomalías y correlación de eventos de seguridad.

Clasificación según su naturaleza técnica

Este criterio se centra en cómo se representa físicamente la información.

a) Comunicación analógica

Utiliza señales continuas para representar la información.

Ejemplo: Señales eléctricas continuas o audio sin digitalizar.

En ciberseguridad, este tipo tiene poca aplicación directa, pues casi todos los sistemas actuales operan digitalmente.

b) Comunicación digital

La información se representa mediante símbolos discretos (bits).

Ejemplo:

- Paquetes TCP/IP
- Mensajes cifrados
- Logs estructurados

Desde la teoría de la información, este tipo es el más relevante porque permite:

- Modelar la fuente como variable aleatoria.
- Calcular probabilidades.
- Medir entropía.

En sistemas organizacionales, todo evento digital (inicio de sesión, acceso a recurso, transferencia de datos) puede modelarse como símbolo dentro de un alfabeto finito.

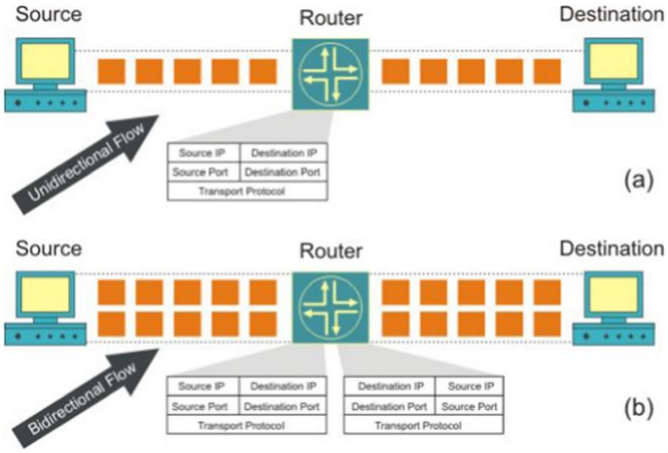
La comunicación en una organización no es homogénea, sino que adopta múltiples formas según su estructura, dirección y naturaleza técnica.

2.1.1 Comunicación Unidireccional y Bidireccional

En una red corporativa, cuando un servidor envía registros a un sistema SIEM sin recibir respuesta, se trata de un proceso unidireccional. En contraste, cuando existe confirmación de recepción o intercambio de datos, se habla de comunicación bidireccional (Figura 1).

Figura 1

Comparación de comunicación unidireccional y bidireccional en redes digitales



Nota. en la parte **(a)** de la figura se representa un flujo unidireccional, donde la información se transmite desde la fuente hacia el destino sin que exista una respuesta directa en sentido contrario. Los paquetes viajan con parámetros fijos, tales como dirección IP de origen, dirección IP de destino, puertos y protocolo de transporte. Desde la perspectiva de la ciberseguridad, la comunicación unidireccional reduce la superficie de ataque, ya que el destino no envía información de retorno que pueda ser explotada por un actor malicioso.

En contraste, la parte **(b)** muestra un flujo bidireccional, en el cual la fuente y el destino intercambian información de manera activa. En este caso, los roles de origen y destino se alternan, lo que se refleja en el intercambio de direcciones IP y puertos en los encabezados de los paquetes. Sin embargo, desde el punto de vista de la seguridad, la bidireccionalidad introduce una mayor complejidad, ya que ambos sentidos del flujo deben ser protegidos contra interceptación, manipulación o ataques de tipo replay. Adaptado de *Difference Between Unidirectional and Bidirectional (AskDifference, 2024).*

2.1.2 Comunicación Sincrónica y Asincrónica

En entornos digitales, la comunicación puede requerir simultaneidad (sincrónica) o producirse en momentos distintos (asincrónica). Por ejemplo:

- Autenticación en tiempo real → sincrónica
- Envío de logs cada 24 horas → asincrónica

Según Gorzalka y Deloumeaux (2012), la temporalidad influye en la forma en que se modelan probabilísticamente los eventos transmitidos.

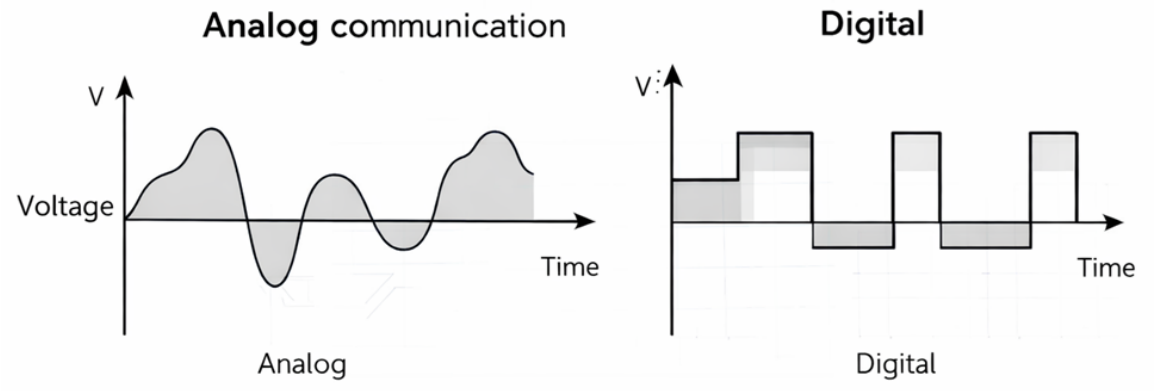
2.1.3 Comunicación Analógica vs Digital

La teoría de la información se enfoca principalmente en sistemas digitales, donde los mensajes se representan mediante símbolos discretos (Csiszár & Körner, 2011). En ciberseguridad, los paquetes de red, bits y registros de eventos constituyen secuencias discretas analizables matemáticamente.

La digitalización convierte eventos organizacionales en secuencias discretas susceptibles de análisis probabilístico.

Figura 2

Comparación e comunicación analógica y digital



Nota: La figura presenta una comparación entre la comunicación analógica y la comunicación digital. En la comunicación analógica, la información se transmite mediante señales continuas en el tiempo, cuyos valores pueden variar de forma infinita dentro de un rango, lo que las hace más susceptibles a la influencia del ruido y más complejas de modelar matemáticamente. En contraste, la comunicación digital representa la información a través de niveles discretos de señal, típicamente asociados a valores binarios, lo que permite una representación estructurada y precisa de los mensajes. Esta discretización constituye la base de la teoría de la información, ya que posibilita el análisis probabilístico de los símbolos transmitidos, el cálculo de métricas como la entropía y la implementación de mecanismos de detección y corrección de errores. En el contexto de la ciberseguridad organizacional, la comunicación digital resulta predominante, pues los eventos del sistema, como accesos, transferencias de datos y registros de actividad, pueden modelarse como secuencias discretas susceptibles de análisis estadístico. Adaptado de Csiszár y Körner (2011).

2.2 Procesos de Comunicación en Sistemas Digitales

2.2.1 Fuente

Más allá de ser un generador de datos, en la teoría de la información la fuente se modela como un proceso estocástico que produce símbolos con ciertas probabilidades.
Formalmente, una fuente discreta puede representarse mediante una variable aleatoria:

$$X = \{x_1, x_2, \ldots, x_n\}$$

donde cada símbolo posee una probabilidad asociada:

$$P(X = x_i) = p_i$$

Este enfoque permite analizar:

- patrones normales de operación
- desviaciones estadísticas
- anomalías en el comportamiento del sistema

Por ejemplo, un aumento inesperado de eventos raros (como múltiples intentos fallidos de autenticación) incrementa la incertidumbre del sistema y puede indicar un ataque. En este sentido, la fuente no solo genera datos, sino que también define el nivel de incertidumbre del sistema de información.

2.2.2 Codificador

En la teoría de Shannon, el codificador cumple principalmente dos funciones:

1. **Codificación de fuente** (source coding)
2. **Codificación de canal** (channel coding)

La codificación de fuente busca reducir redundancias en los datos generados por la fuente para optimizar su transmisión.
Un ejemplo clásico es la compresión de datos mediante algoritmos como:

- Huffman
- Lempel-Ziv (LZ77/LZ78)

La teoría demuestra que el límite inferior de compresión está determinado por la entropía de la fuente:

$$L \geq H(X)$$

donde:

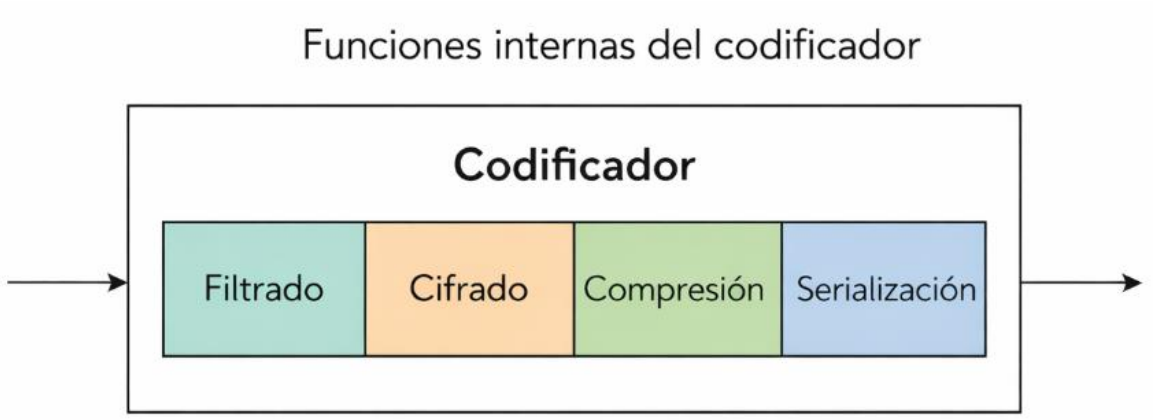
- L es la longitud promedio del código
- $H(X)$es la entropía de la fuente

En contextos de ciberseguridad, la codificación también puede incluir procesos adicionales del pipeline de datos, como:

- normalización de logs
- agregación de eventos
- cifrado de información sensible

Aunque el cifrado pertenece formalmente a la criptografía y no al modelo original de Shannon, en sistemas reales forma parte del flujo de procesamiento antes de la transmisión.

Figura 3
Funciones internas del codificador



Nota. En el modelo clásico de Shannon, el codificador realiza funciones de compresión y codificación de canal. En sistemas reales de ciberseguridad, el pipeline de procesamiento suele incorporar también mecanismos de cifrado, que pertenecen al ámbito de la criptografía y no forman parte del modelo original de Shannon.. Elaboración propia adaptado de la estructura general de sistemas digitales de comunicación descrita por Alencar (2015). (Miguel Ortiz Navarrete)

2.2.3 Canal

En la teoría de la información, el canal no se analiza solo como medio físico, sino como un sistema que introduce incertidumbre en la transmisión. Shannon definió el concepto de capacidad del canal, que representa la máxima tasa de información que puede transmitirse de forma confiable:

$$C = \max_{p(x)} I(X;Y)$$

donde:

- $I(X;Y)$es la información mutua entre la entrada y salida del canal.

En redes organizacionales, esta capacidad puede verse limitada por:

- congestión de red
- latencia
- errores de transmisión
- ataques de denegación de servicio (DoS)

Cuando el volumen de datos supera la capacidad del canal, se produce:

- pérdida de paquetes
- retrasos
- degradación del servicio

Comprender estas limitaciones es esencial para diseñar sistemas de comunicación robustos.

2.2.4 Decodificador

El decodificador no solo reconstruye los datos originales, sino que también puede implementar mecanismos de detección y corrección de errores.
Estos mecanismos se basan en la introducción de redundancia controlada durante la codificación de canal.
En sistemas de seguridad, el proceso de decodificación también puede incluir:

- verificación de integridad mediante hashes
- validación de firmas digitales
- reconstrucción de paquetes fragmentados

Estas operaciones permiten detectar si los datos fueron:

- corrompidos por errores
- alterados durante la transmisión
- manipulados por un atacante

2.2.5 Destino

El destino es el componente que finalmente interpreta la información recibida.
Desde el punto de vista de la teoría de la información, el destino transforma la señal recibida en conocimiento útil para el sistema.
En entornos de ciberseguridad, esto suele ocurrir en plataformas de análisis como:

- sistemas SIEM
- motores de correlación de eventos
- plataformas de análisis de comportamiento (UEBA)

Estos sistemas procesan grandes volúmenes de datos y aplican técnicas estadísticas o de aprendizaje automático para identificar:

- patrones normales
- desviaciones
- posibles incidentes de seguridad

2.2.6 Canal y Ruido

En la teoría de la información, el ruido se modela como una perturbación probabilística del canal. Uno de los modelos más simples es el canal binario simétrico (Binary Symmetric Channel, BSC).
En este modelo:

- cada bit transmitido tiene probabilidad p de invertirse; la tabla 1 muestra esta probabilidad

Tabla 1

Probabilidad de invertirse por cada bit trasmitido

Bit transmitido	Bit recibido	Probabilidad
0	0	1−p
0	1	p
1	1	1−p
1	0	p

Nota: Tabla de probabilidad por bit transmitido

En sistemas de redes, el ruido puede representar:

- errores de transmisión
- interferencias electromagnéticas
- pérdida de paquetes
- alteraciones intencionales del tráfico

Desde la perspectiva de ciberseguridad, algunas formas de ruido pueden ser **intencionales**, como:

- inyección de tráfico malicioso
- manipulación de paquetes
- interferencia deliberada en comunicaciones inalámbricas

El análisis probabilístico de estos fenómenos permite diseñar mecanismos de detección y mitigación de anomalías en el tráfico de red.

Figura 4

Tipos de ruido en sistemas digitales con etiquetas adaptadas a ciberseguridad

Nota. Figura adaptada del concepto de ruido en comunicaciones digitales, incorporando aspectos de ciberseguridad como interferencia en logs, tráfico de red y perturbaciones maliciosas. Basado en conceptos presentados en Comunicaciones digitales: elementos y tipos de ruido en sistemas (Studocu, s.f.) y Noise in communication systems (Slideshare, s.f.).

2.3 Fundamentos de Probabilidad para Teoría de la Información

La teoría de la información se fundamenta en la probabilidad, pues la incertidumbre depende de la distribución de los eventos. La teoría de la información no estudia los mensajes por su significado, sino por su incertidumbre. Y la incertidumbre solo puede medirse si sabemos qué tan probable es que ocurra cada evento.

¿Por qué la incertidumbre depende de la probabilidad?

Imagina dos situaciones en una organización:

Caso 1

El 99% de los accesos al sistema son correctos.

Solo el 1% son fallidos.

Aquí casi siempre ocurre lo mismo. Hay poca sorpresa. La incertidumbre es baja.

Caso 2

El 50% de los accesos son correctos.

El 50% son fallidos.

Aquí no sabemos qué ocurrirá en el siguiente intento. Hay más sorpresa. La incertidumbre es alta.

La diferencia entre ambos casos está en la distribución de probabilidades.

2.3.1 Variable Aleatoria

¿Qué es una variable aleatoria discreta?

Formalmente, una variable aleatoria discreta se define como una función

$$X: \Omega \to \mathbb{R}$$

definida sobre un espacio de probabilidad $(\Omega, \mathcal{F}, P)$.

Esto significa que: X es una función que toma resultados del experimento y los convierte en números reales.

Ω representa **todos los resultados posibles de un experimento**.

F es el **conjunto de eventos que podemos medir probabilísticamente**.

P es una función que asigna **probabilidades a los eventos**.

Ejemplo en ciberseguridad:

Ω= {Login correcto, Login fallido}

F={∅,{ Login correcto },{ Login fallido }}

Significa que nuestra variable aleatoria *X* puede tomar dos valores posibles.

Si asumimos los datos del caso 1 como probabilidades observadas en la organización:

Definimos la variable aleatoria:

$$X(login\_correcto) = 0$$
$$X(login\_fallido) = 1$$

Se llama discreta cuando puede tomar un número finito o contable de valores.

Ejemplo:

$$X = \{0,1\}$$

con probabilidades

$$P(X = 0) = 0.9$$
$$P(X = 1) = 0.1$$

En términos prácticos, esto significa que:

- **X** es la variable aleatoria
- $\mathbf{x_i}$ son los valores posibles que puede tomar

¿Qué nos permite hacer esto?

- Medir la incertidumbre (entropía).
- Detectar cambios en la distribución.
- Identificar anomalías.
- Caracterizar matemáticamente el flujo de información.

2.3.2 Distribución de Probabilidad

Alencar (2015) indica que la información transmitida depende no solo del evento sino de su probabilidad.

Tabla 2

Ejemplo de distribución de eventos de autenticación

Evento	Probabilidad
Acceso exitoso	0.9
Acceso fallido	0.1

Nota. Elaboración propia con base a los datos del caso 1 (Miguel Ortiz Navarrete)

2.3.3 Independencia y Dependencia

Dos eventos son independientes si la ocurrencia de uno no afecta la probabilidad del otro.

Formalmente:

$$P(X_{t+1} \mid X_t) = P(X_{t+1})$$

Es decir:

La probabilidad del siguiente evento no depende del anterior.

Los eventos son dependientes si la probabilidad del siguiente evento cambia dependiendo del anterior. En sistemas reales, los eventos pueden no ser independientes. Por ejemplo:

- Un ataque de fuerza bruta genera múltiples intentos fallidos consecutivos.

Esto introduce correlación temporal, fenómeno estudiado por Csiszár y Körner (2011) en el análisis de sistemas sin memoria y con memoria.

Formalmente:

$$P(X_{t+1} \mid X_t) \neq P(X_{t+1})$$

Fuentes sin memoria

Una fuente sin memoria es aquella en la que cada símbolo generado es independiente de los anteriores.
Matemáticamente:

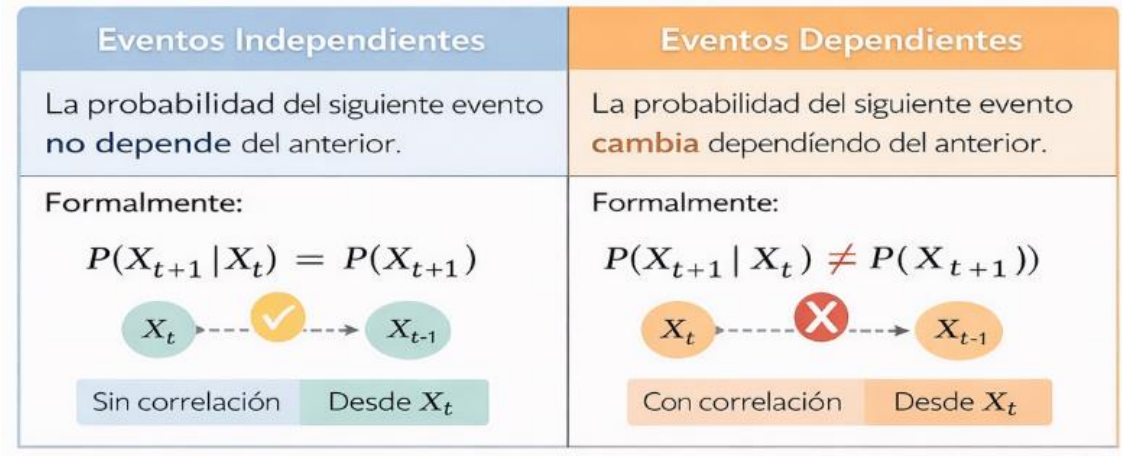
$$H(X_1,X_2,\ldots,X_n)=\Sigma H(X_i)$$

Fuentes con memoria

Una fuente con memoria presenta dependencia entre símbolos consecutivos, lo que puede modelarse mediante cadenas de Markov.
En este caso:

$$H(X_1,X_2,\ldots,X_n) < \Sigma H(X_i)$$

Figura 5
Independencia vs. Dependencias: probabilidad de eventos



Nota: En sistemas reales, los eventos pueden no ser independientes. Por ejemplo:

- Un ataque de fuerza bruta genera múltiples intentos fallidos consecutivos
- Esto introduce correlación temporal, fenómeno estudiado por Csiszár y Körner (2011) en el análisis de sistemas sin memoria y con memoria.

2.4 Incertidumbre y Contenido Informativo

2.4.1 Información como reducción de incertidumbre

Gorzalka y Deloumeaux (2012) señalan que la información puede interpretarse como la reducción de incertidumbre ante la ocurrencia de un evento.

Aquí aparece el término clave: Entropía

La entropía mide la incertidumbre promedio asociada a una fuente de información.

2.4.2 Entropía de Shannon

La entropía fue introducida por Claude Shannon en 1948 como una medida cuantitativa de la incertidumbre promedio asociada a una fuente de información discreta.

La entropía se define como:

$$H(X) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i)$$

donde:

- Xes una variable aleatoria discreta.
- $p(x_i)$es la probabilidad del símbolo x_i.
- El logaritmo en base 2 expresa la información en bits.

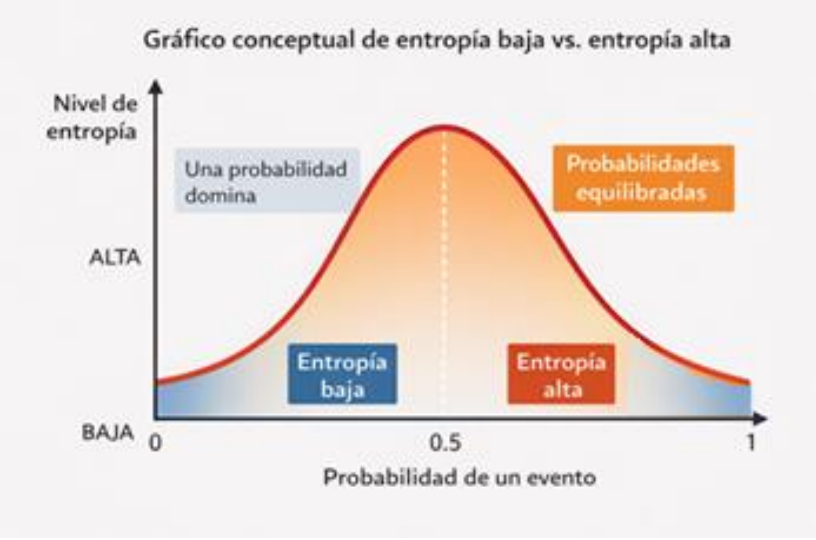
¿Qué mide realmente la entropía?

La cantidad promedio de información que produce una fuente al emitir un símbolo.

Más incertidumbre → mayor entropía.
Más predictibilidad → menor entropía.

No mide el "contenido semántico", sino la estructura probabilística de los datos (Figura 6).

Figura 6
Gráfico conceptual de entropía baja vs. entropía alta



Nota. Esta figura ilustra cómo cambia la entropía dependiendo de la distribución de probabilidades de los eventos, con entropía baja cuando una probabilidad domina y entropía alta cuando las probabilidades son equilibradas. En el extremo izquierdo (probabilidad cercana a 0), y en el extremo derecho (probabilidad cercana a 1), la entropía es baja. En el centro del gráfico, cuando la probabilidad es 0.5, la entropía alcanza su valor máximo.

. Adaptado de *Information Theory* (Alencar, 2015).

A continuación, veremos paso a paso como pasar de la variable aleatoria discreta a la entropía (basado en el caso 1).

Como paso 1 se debe definir la variable aleatoria discreta, en el caso 1 se estableció que la variable aleatoria discreta X tiene dos valores posibles

X={Login correcto, Login fallido}

P(Login correcto)=0.9
P(Login incorrecto)=0.1

Como paso 2 se debe definir la información como un evento; En teoría de la información (Claude Shannon), la información asociada a un evento se define como:

$$I(x) = -\log_2 P(x)$$

¿Por qué logaritmo?

- Porque la información debe crecer cuando la probabilidad disminuye.
- El logaritmo convierte multiplicaciones de probabilidades en sumas.
- Base 2 → la unidad es bits.

Calculamos la información de cada evento

Login correcto (0.9)

I(Login correcto)=-log₂(0.9)
=-(-0.152) ≈0.152 bits

Poco sorprendente → poca información.

Login fallido (0.1)

I(Login fallido)=-log₂(0.1)
=-(-3.322) ≈3.322 bits

Mucho más raro → más información.

Como paso 3 pasamos de información individual a incertidumbre promedio; un sistema no produce un solo evento, sino muchos. Entonces necesitamos el promedio ponderado de la información de todos los eventos posibles. Eso es la entropía *H(X)*

H(X)=-(0.9 log₂ 0.9+0.1 log₂ 0.1)
H(X)=-(0.9 (-0.152)+0.1 (-3.322))
H(X)=-(-0.137-0.332)
H(X)=0.469 bits

Como paso 4 interpretamos la entropía del sistema:

Esto significa:

- El sistema tiene baja incertidumbre.
- El comportamiento es bastante predecible.
- El login correcto domina la distribución.

AskDifference. (2024). *Unidirectional vs. bidirectional — what's the difference?* **https://www.askdifference.com/unidirectional-vs-bidirectional/**

Alencar, M. S. (2015). *Information Theory*. Momentum Press.

Csiszár, I., & Körner, J. (2011). *Information theory: Coding theorems for discrete memoryless systems* (2nd ed.). Cambridge University Press.

Gorzalka, J. D., & Deloumeaux, P. (2012). *Information theory: New research*. Nova Science Publishers.

Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal, 27*, 379–423.

Studocu. (s. f.). *Comunicaciones digitales: elementos y tipos de ruido en sistemas*. https://www.studocu.com/co/document/sena-sofiaplus/gestion-de-redes-de-datos/comunicaciones-digitales-elementos-y-tipos-de-ruido-en-sistemas/125491757

Slideshare. (s. f.). *Noise in communication systems* [Presentación]. https://www.slideshare.net/slideshow/noise-in-communication-system/40737704

PUCE Virtual

síguenos en:

www.pucevirtual.puce.edu.ec