Unidad 6: La probabilidad y el impacto

BLOQUE II – El análisis del ciberriesgo: enfoques cualitativos y cuantitativos

Grado en Ingeniería de la Ciberseguridad, curso 2022-2023

CONTENIDOS

1. Talleres de calibración.
2. Medida de la probabilidad.
3. Medida del impacto.
4. KRIs y otras métricas.

1. Talleres de calibración

- Ya hemos mencionado técnicas como los grupos de discusión, los paneles de expertos y los talleres de calibración cuando hay que estimar valores para la probabilidad y el impacto.
  - Estas técnicas pueden incluir a profesionales y analistas tanto internos como externos.
  - Los grupos suelen ser multidisciplinares, con personas de diferentes perfiles, niveles de conocimiento, intereses.
- Llevar a cabo este tipo de sesiones y que resulten productivas y útiles implica un aprendizaje.

1. Talleres de calibración

- Algunos consejos para la persona que hace de analista:
  - Las personas involucradas tienen que saber qué se espera de ellas: instrucciones claras, estimación de tiempo y esfuerzo.
  - Hay que llevar las sesiones o talleres bien preparados.
    - Desde su convocatoria: AGENDA.
  - Toda la información y datos que se desea que manejen las personas que asisten tienen que estar bien presentados y disponibles con suficiente antelación
  - Hay que trabajar mucho las entrevistas, cuestionarios, etc. y materiales similares.

1. Talleres de calibración

- Hay que saber escuchar, guiar, proponer, desbloquear.
- Ayudan mucho los ejemplos, las preguntas clave, la reducción al absurdo.
- Hay que tener muy claro qué se espera conseguir en cada sesión.
  - Siendo flexible, pero comprendiendo cuál es el producto o entregable ideal o deseado.
- Tiene que quedar claro cómo se alcanza un consenso.

1. Talleres de calibración

- Consenso informal vs consenso formal.
  - Depende del tipo de proceso de análisis.
- Herramientas:

Catálogos, mapas, escalas	Intervalos de confianza	Técnica PERT	Método Delphi

2. Medida de la probabilidad

Fuentes internas

Fuentes externas

2. Medida de la probabilidad

Conocimiento sobre el pasado (históricos)	Conocimiento sobre el presente (evidencias)	Conocimiento sobre el futuro (predicciones)

2. Medida de la probabilidad

Pasado	Presente	Futuro
✓ Documentación sobre incidentes pasados (FI). ✓ Informes de siniestros y contexto de amenazas observado (FE). ✓ Informes técnicos, estudios e investigaciones (FE).	✓ Nivel de madurez y controles desplegados (FI). ✓ Vulnerabilidades existentes (FI). ✓ TTPs actuales (FE).	✓ Resultados de iniciativas de Threat Hunting (FI). ✓ Resultados de procesos de ciber-inteligencia y forecasting (FI/FE). ✓ Informes de previsiones, TTPs futuras (FE).

(FI) Fuente Interna *(FE) Fuente Externa*

2. Medida de la probabilidad

- Enfoques frecuentistas

Valor de la probabilidad	Descripción	Frecuencia (con escalas de 10)
Muy alta (muy frecuente)	Ocurre a diario	100
Alta (frecuente)	Ocurre una vez mensualmente	10
Media (normal)	Ocurre una vez al año	1
Baja (poco frecuente)	Ocurre una vez cada varios 10 años	1/10
Muy baja (muy poco frecuente)	Ocurre una vez cada siglo	1/100

2. Medida de la probabilidad

Valor de la probabilidad	Descripción	Frecuencia
Muy probable	Ocurre cinco veces o más por año	[5, ∞]:1 año = [50, ∞]:10 años
Bastante probable	Ocurre entre dos y cinco veces por año	[2, 5]:1 año = [20, 50]:10 años
Probable	Ocurre menos de dos veces por año	[0.5 , 2]:1 año = [5, 20]:10 años
Poco probable	Ocurre menos de una vez por año	[0.1 , 0.5]:1 año = [1, 5]:10 años
Muy poco probable	Ocurre menos de una vez cada diez años	[0, 0.01]:1 año = [0, 1]:10 años

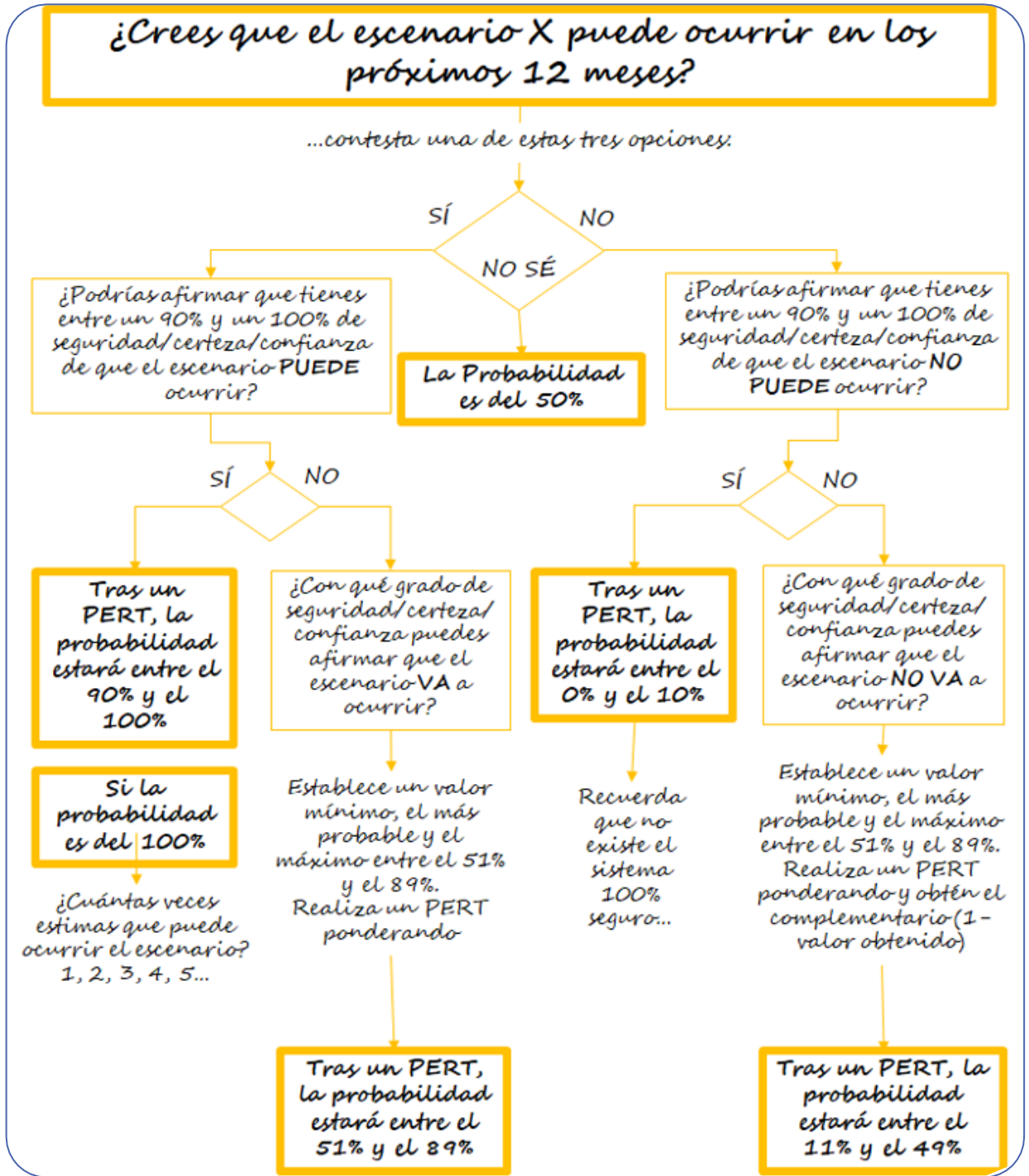
2. Medida de la probabilidad

- Enfoques basados en grado de exposición, nivel del madurez, atractivo para el adversario

Grado de vulnerabilidad	Descripción	Valor de la probabilidad
Muy alto	La existencia de 1 vulnerabilidad que sea muy fácil de explotar, asegura la materialización de la amenaza	85% -100%
Alto	La existencia de 1 vulnerabilidad que sea bastante fácil de explotar, facilita mucho la materialización de la amenaza	84% - 70%
Medio	La existencia de 1 vulnerabilidad que sea fácil de explotar, facilita la materialización de la amenaza	69% - 50%
Bajo	La existencia de 1 vulnerabilidad difícil de explotar, podría contribuir a la materialización de la amenaza	49% - 30%
Muy bajo	La existencia de 1 vulnerabilidad bastante difícil de explotar contribuye vagamente a la materialización de la amenaza	29% -15%.
Despreciable	La existencia de 1 vulnerabilidad muy difícil de apenas contribuye a la materialización de la amenaza	14% - 0%

2. Medida de la probabilidad

Enfoque bayesiano



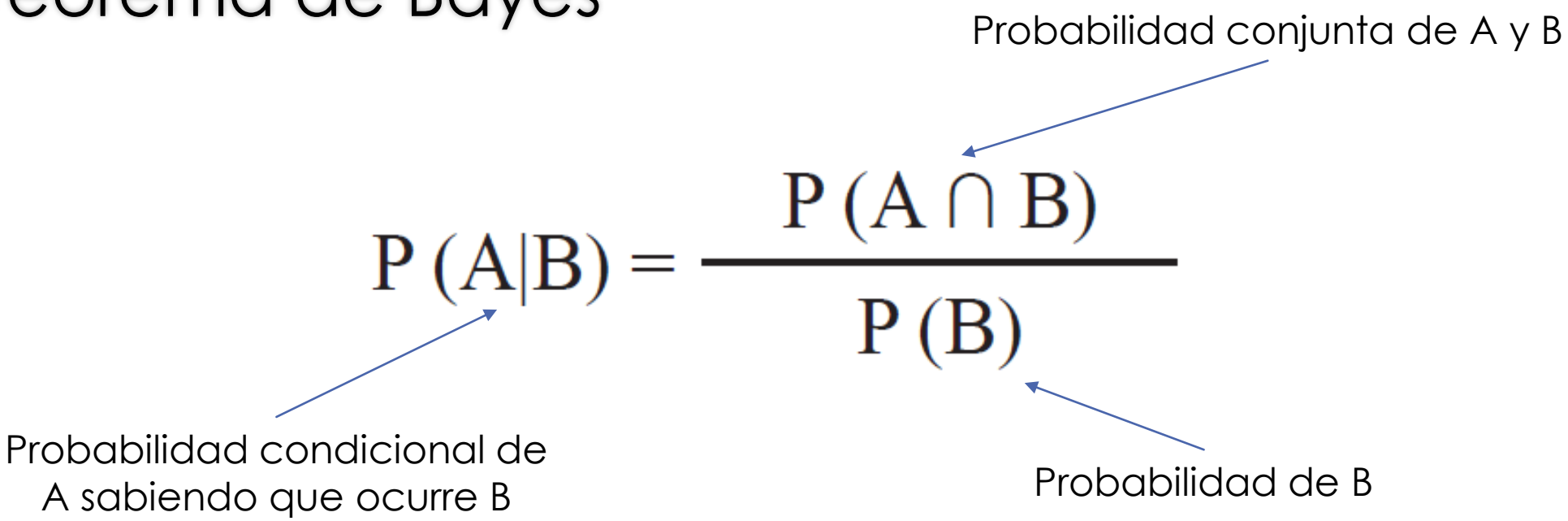
2. Medida de la probabilidad

- Enfoques indirectos

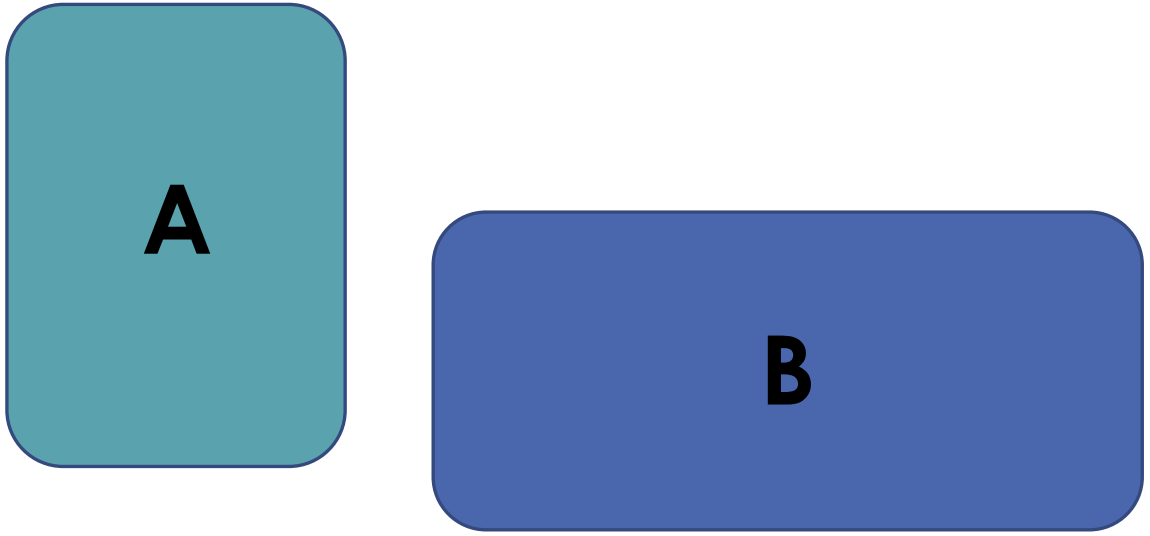
Teorema de Bayes	Distribución Beta

2. Medida de la probabilidad

- Teorema de Bayes

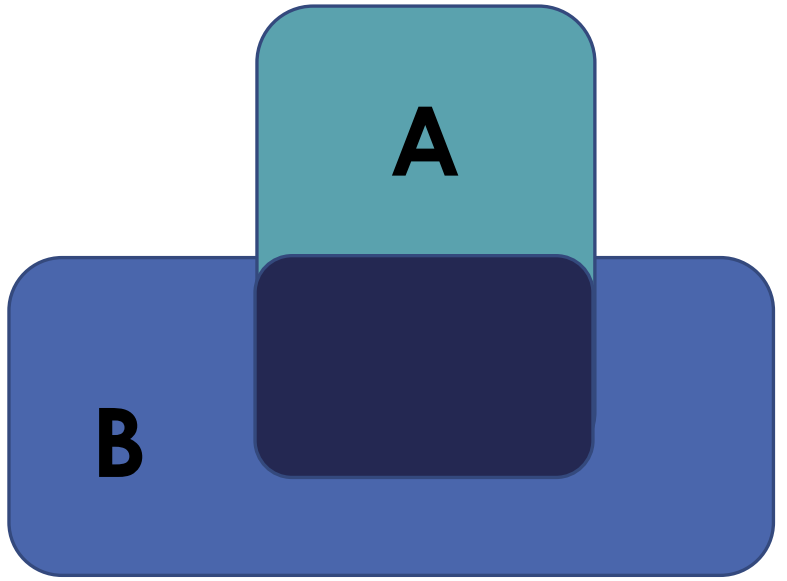


2. Medida de la probabilidad



$$P(A \cap B) = 0$$

Sucesos excluyentes



Sucesos dependientes
o independientes

2. Medida de la probabilidad

Sucesos independientes:

$$P(A \cap B) = P(A)P(B)$$

$$P(A|B) = P(A)$$

$$P(B|A) = P(B)$$

2. Medida de la probabilidad

- En ciber se observan sucesos dependientes que nos permiten aplicar el teorema de Bayes en diferentes situaciones.
- Por ejemplo, supongamos que estamos analizando un escenario que tiene que ver con incidentes en los que un servidor o dispositivo corporativo termine minando criptomoneda para un tercero.
  - Lo que degrada su rendimiento debido al alto consumo de recursos que esto implica.

2. Medida de la probabilidad

- Medidas que podemos hacer (históricos y evidencias):

1. P(CM|MALW): Probabilidad de que, infectado por malware (MALW), un equipo acabe minando criptomoneda (CM) para un tercero. Este valor puede calcularse a partir de datos de informes sobre malware, podemos saber, por ejemplo, del año pasado, qué proporción de malware respecto del total tenía como objetivo el minado de criptomoneda. Supongamos que es un 33%.

2. P(CM|~MALW): Probabilidad de que, sin estar causado el incidente por un malware, un equipo acabe minando criptomoneda para un tercero. Igualmente, podemos recurrir a informes que analicen amenazas recientes y determinar que otros patrones de ataque, además del malware, se usan con este objetivo y en qué proporción. Se puede utilizar PowerShell, por ejemplo, pero es un patrón que se observa muy poco en relación con el malware tradicional. Supongamos que la probabilidad se estima como un 2%.

2. Medida de la probabilidad

3. P(MALW|IoC): Probabilidad de que, activado un indicador de compromiso (IoC) que implica exceso de consumo de recursos (CPU, memoria), sea por culpa de una infección por malware. En este caso podemos recurrir a nuestros *logs* y documentación sobre alertas cuando se han observado ciertos IoC para realizar el cálculo. En este caso se calcula una probabilidad de un 50%.

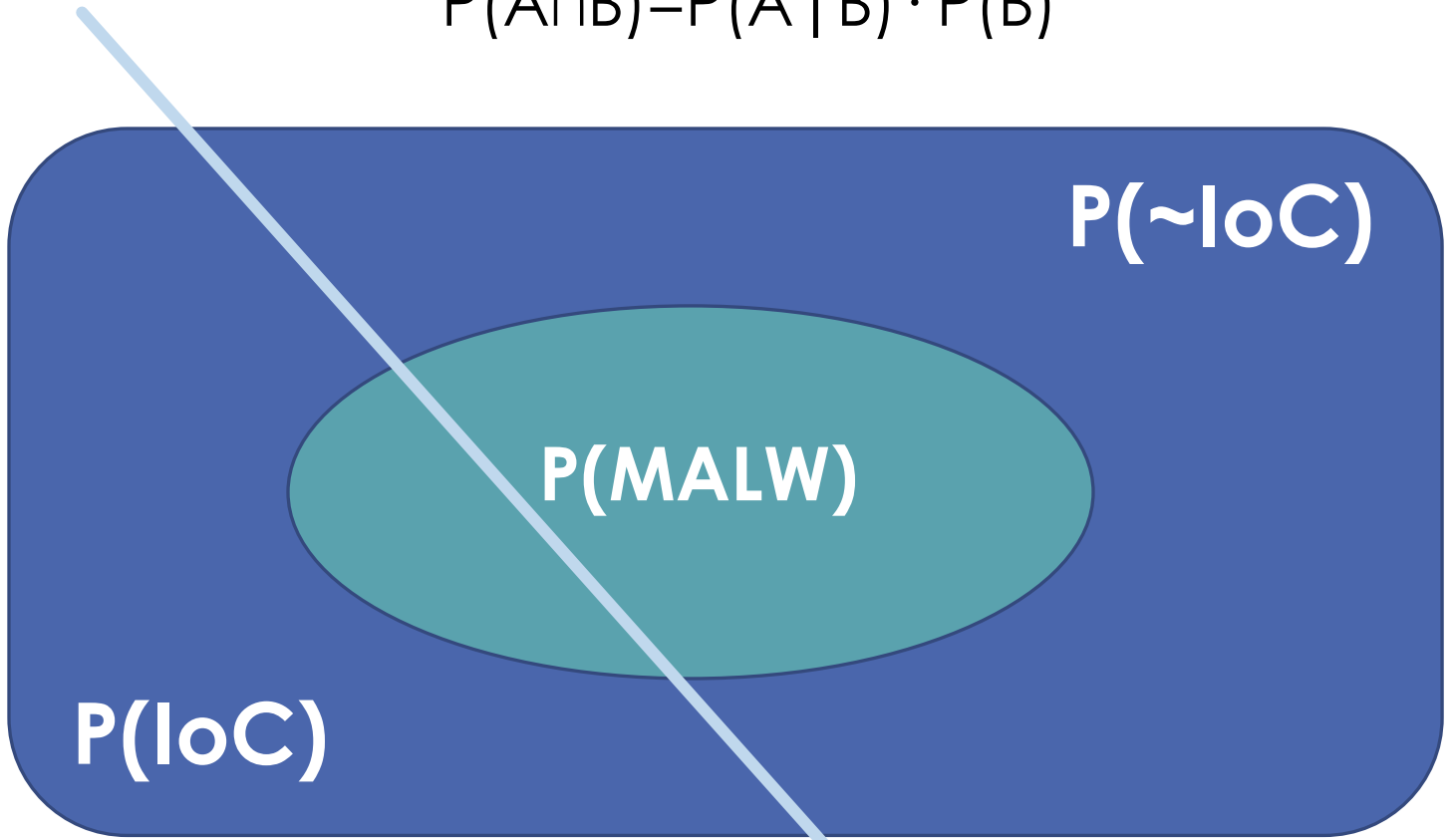
4. P(MALW|~IoC): Probabilidad de que, sin que se active un indicador de compromiso que implica exceso de consumo de recursos (CPU, memoria), tengamos una infección por malware. Si llevamos una buena documentación de respuesta a incidentes en la organización, podremos obtener este dato también con cierta facilidad. Tenemos una probabilidad del 30%.

5. P(IoC): Probabilidad de que se active el indicador de compromiso que nos dice que un equipo consume más recursos de los normales (CPU, memoria), por encima de un umbral sospechoso. Se puede medir como una frecuencia, en nuestro ejemplo, es de un 20% (por ejemplo, una vez cada cinco años).

2. Medida de la probabilidad

Recuerda que con el teorema de Bayes sabemos que:

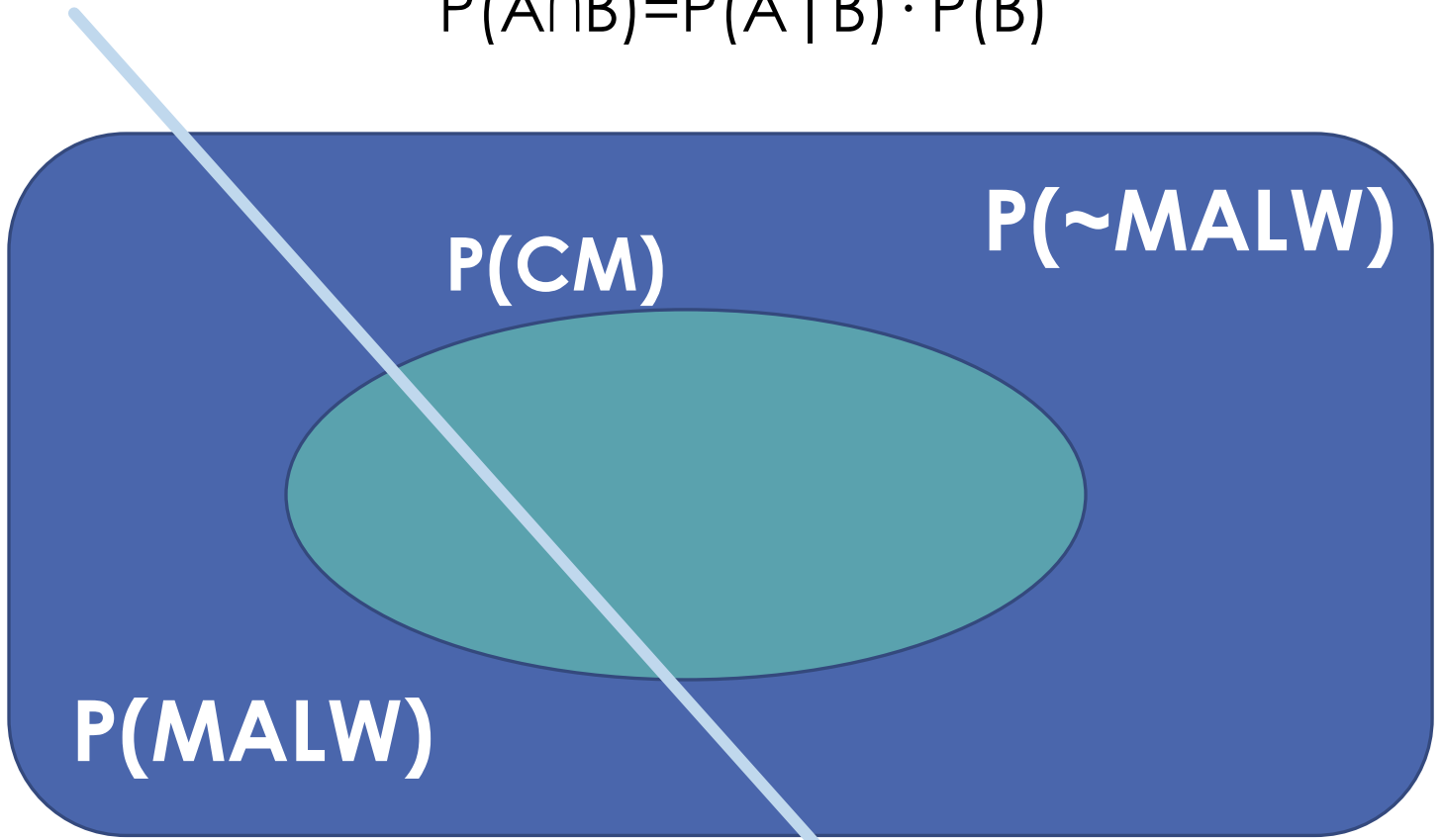
$$P(A \cap B) = P(A \mid B) \cdot P(B)$$



2. Medida de la probabilidad

Recuerda que con el teorema de Bayes sabemos que:

$$P(A \cap B) = P(A \mid B) \cdot P(B)$$



3. Medida del impacto

- ¿Podemos calcular con estos datos la probabilidad del incidente que nos interesa: terminar minando criptomoneda para un tercero malicioso?

P(MALW)	$P(IoC) \cdot P(MALW \mid IoC) + P(\sim IoC) \cdot P(MALW \mid \sim IoC) = 0,2 \cdot 0,5 + 0,8 \cdot 0,3$	0,34
P(CM)	$P(MALW) \cdot P(CM \mid MALW) + P(\sim MALW) \cdot P(CM \mid \sim MALW) = 0,34 \cdot 0,33 + 0,66 \cdot 0,02$	**0,1254**

2. Medida de la probabilidad

- Distribución Beta
  - Esta distribución es una distribución de probabilidad continua definida en el intervalo [0,1] con dos parámetros positivos, a y β.
    - Cuando estos dos parámetros tienen valor 1, la distribución Beta es la uniforme (la que asigna la misma probabilidad a todos los valores de la variable aleatoria).
  - Esta distribución estadística nos permite resolver problemas relativos a proporciones, que son muy habituales en los talleres de calibración.

2. Medida de la probabilidad

- Supongamos que la autoridad de control nos dice que el año pasado se notificaron 1.275 brechas de datos en España (históricos).
- Este dato nos puede ser útil para calcular la probabilidad de sufrir una brecha de datos si ese es el escenario que nos preocupa.
- Pero ¿1.275 brechas de datos en un año, qué probabilidad implica? Depende de la población total ¿cuántas organizaciones usamos para calcular la probabilidad? ¿cuál es el divisor, 1275/X, cómo decido el valor de X?
  - Porque ese valor condiciona completamente el valor de la probabilidad, no es lo mismo 1.275 brechas de datos en 2.000 organizaciones que en 2.000.000 de organizaciones.

2. Medida de la probabilidad

- Lo más obvio, sería buscar el número de organizaciones empresariales (supongamos que el informe se refiere a brechas en el sector privado) que existen en España y con eso calculo la probabilidad
  - 1.275 brechas notificadas/100.000 organizaciones=0,012.
  - Es decir, obtengo una probabilidad del 1.2% de brecha datos.

2. Medida de la probabilidad

- Supongamos ahora que investigamos más, buscamos organizaciones en el mismo sector que la nuestra (desarrollo de SW, por ejemplo) y de tamaño y facturación similar.
  - Encontramos 38 organizaciones, nos consta que sólo 1 de ellas ha tenido una brecha de datos en el último año de las que se recogen en el informe.
  - Eso sería una probabilidad de 1/38=0,026, es decir, de un 2.6%.

2. Medida de la probabilidad

- Pero todo depende del valor 38 que hemos decidido, puede que no estemos ajustando bien la proporción, una brecha de datos ¿entre cuántas empresas que debo tener en cuenta como población total, qué dato es útil para mi organización?
- Podemos hacer una estimación mejor, con mayor grado de certidumbre, usando una distribución Beta.
- ¿Con qué parámetros? Como no tengo conocimiento a priori, partimos de a y β con valor 1 (una distribución uniforme, todos los valores son igual de probables).

2. Medida de la probabilidad

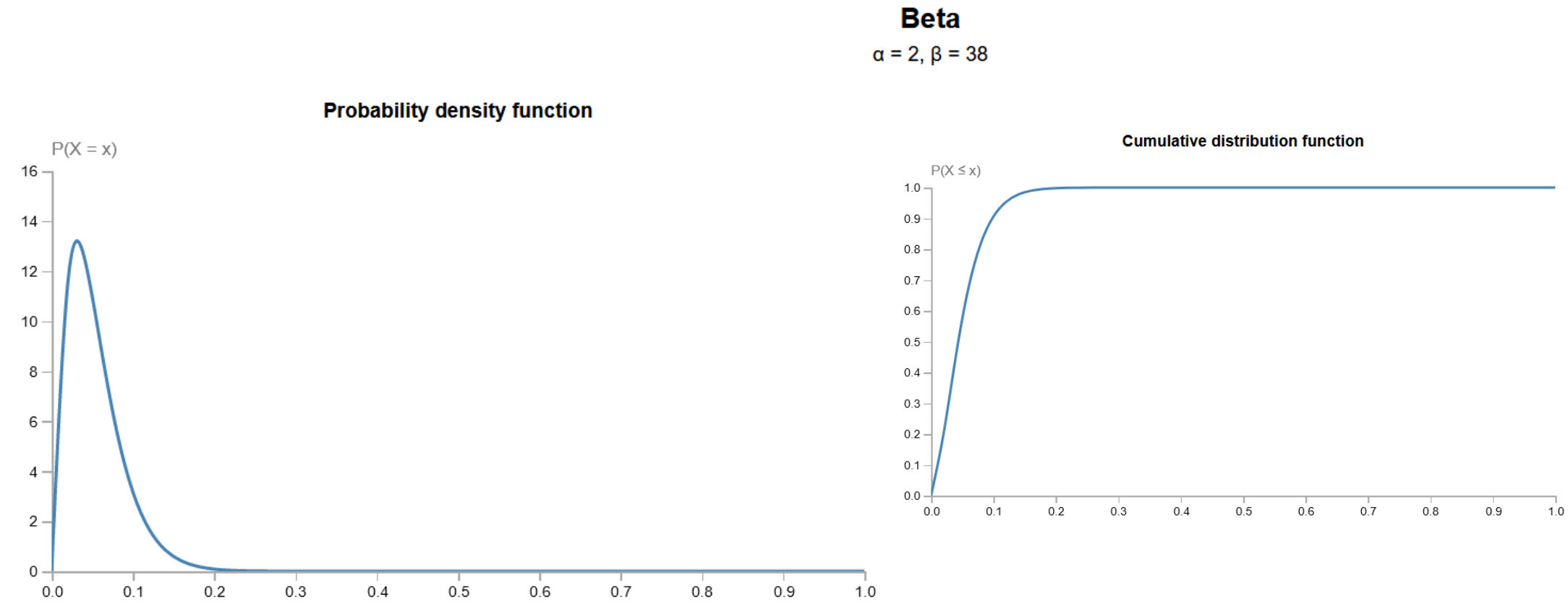
- A a le sumamos las organizaciones en las que ha habido brecha y a β le sumamos las organizaciones en las que no la ha habido de la muestra de 38 que estamos teniendo en cuenta.

$\alpha = 1 + 1$	2
$\beta = 1 + 37$	38

2. Medida de la probabilidad

- Ahora usamos la distribución Beta con estos valores de parámetros para estimar la probabilidad del escenario de brecha de datos.
- Tenemos, por ejemplo, que con un intervalo de confianza del 90% la probabilidad estará entre el 0.92% y el 11.60% (tenemos un valor mínimo y un valor máximo para la probabilidad del escenario).
- Y también tenemos el valor más probable, con la esperanza de la distribución, que en este ejemplo vale un 5%.
- Podemos usar cualquiera de estos tres valores o realizar un PERT como ya hemos hecho anteriormente.

2. Medida de la probabilidad



https://statdist.com/distributions/beta

3. Medida del impacto

- Las fuentes de conocimiento para realizar las estimaciones de impacto son las mismas que para las estimaciones de probabilidad.
  - Internas y externas.
  - Pasado, presente y futuro (históricos, evidencias y predicciones).
- Los impactos pueden estimarse mediante escalas cualitativas o de manera numérica.
  - Técnicos o económicos.

3. Medida del impacto

Pilar de la seguridad afectado	Medida de impacto técnico
Confidencialidad	Número de archivos exfiltrados, Número de contraseñas o secretos comprometidos, Número de clientes afectados
Integridad	Número de ítems modificados o eliminados sin permiso (archivos, mensajes, contraseñas, programas, configuraciones)
Disponibilidad	Tiempo de caída, Número de servicios o activos no accesibles.

3. Medida del impacto

Tipo de pérdida económica
Productividad
Extorsión
Respuesta y recuperación
Reputación y gestión de crisis
Multas, sanciones y reclamaciones

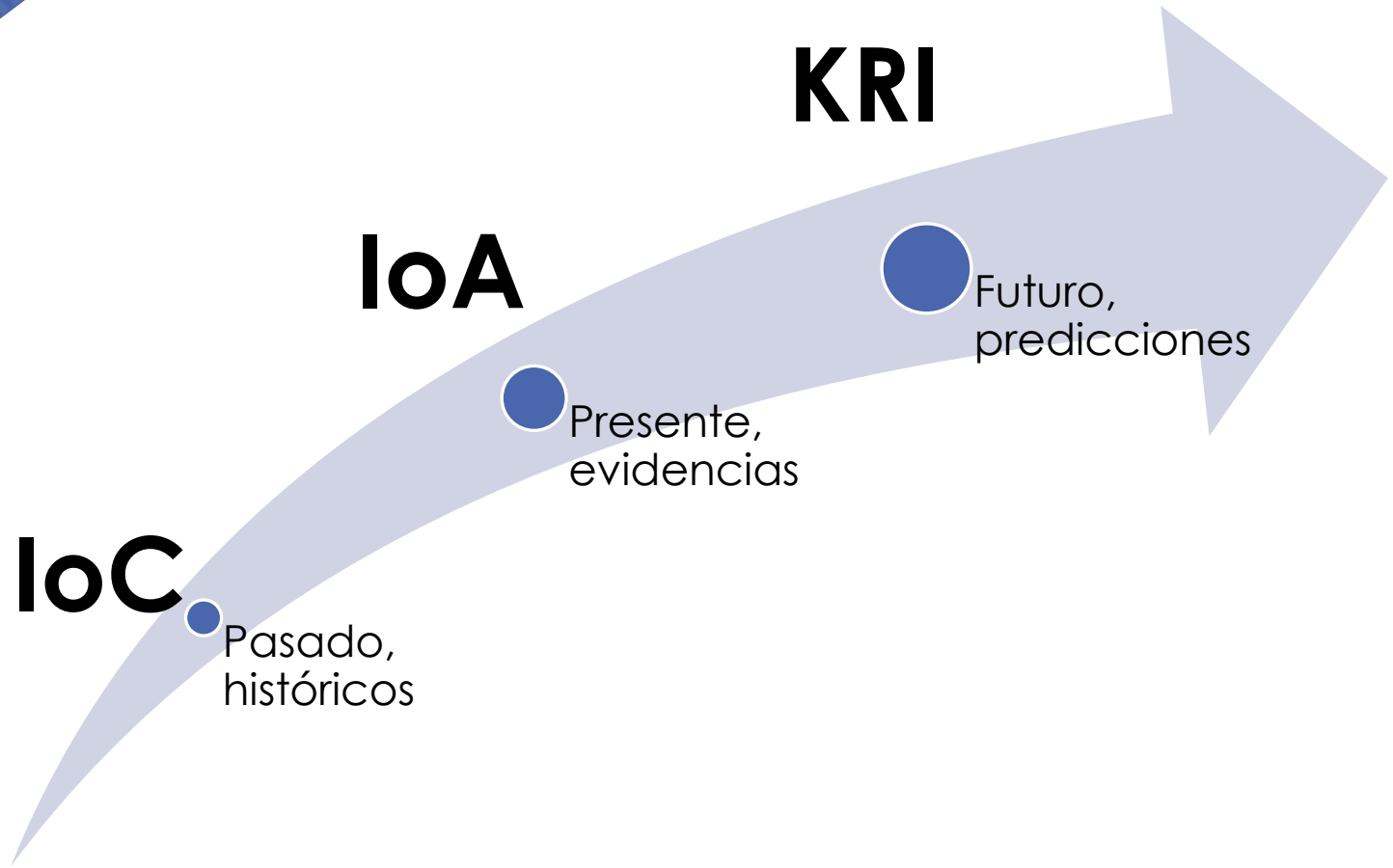
PRÁCTICA 1

- Vais a completar el trabajo hecho en las dos sesiones anteriores.
  - Trabajando con mayor profundidad las estimaciones de probabilidades e impactos y trabajando con diferentes enfoques.
  - Combinando los resultados obtenidos con CORAS y con FAIR (método cualitativo y método cuantitativo).

4. KRIs y otras métricas

- Los KRI o Key Risk Indicators son indicadores del riesgo.
- Los KPI (Key Performance Indicators) son típicos en la gestión de equipos, proyectos y organizaciones.
  - Se basan en datos históricos, el rendimiento en el pasado.
- Los KRI, menos conocidos, deberían ser predictivos, de manera que nos avisen de un potencial cambio de tendencia en relación con un riesgo.
  - No confundir con los IoC (Indicator of Compromise) o IoA (Indicator of Attack), que sí que tienen que ver con el pasado o el presente.

4. KRIs y otras métricas



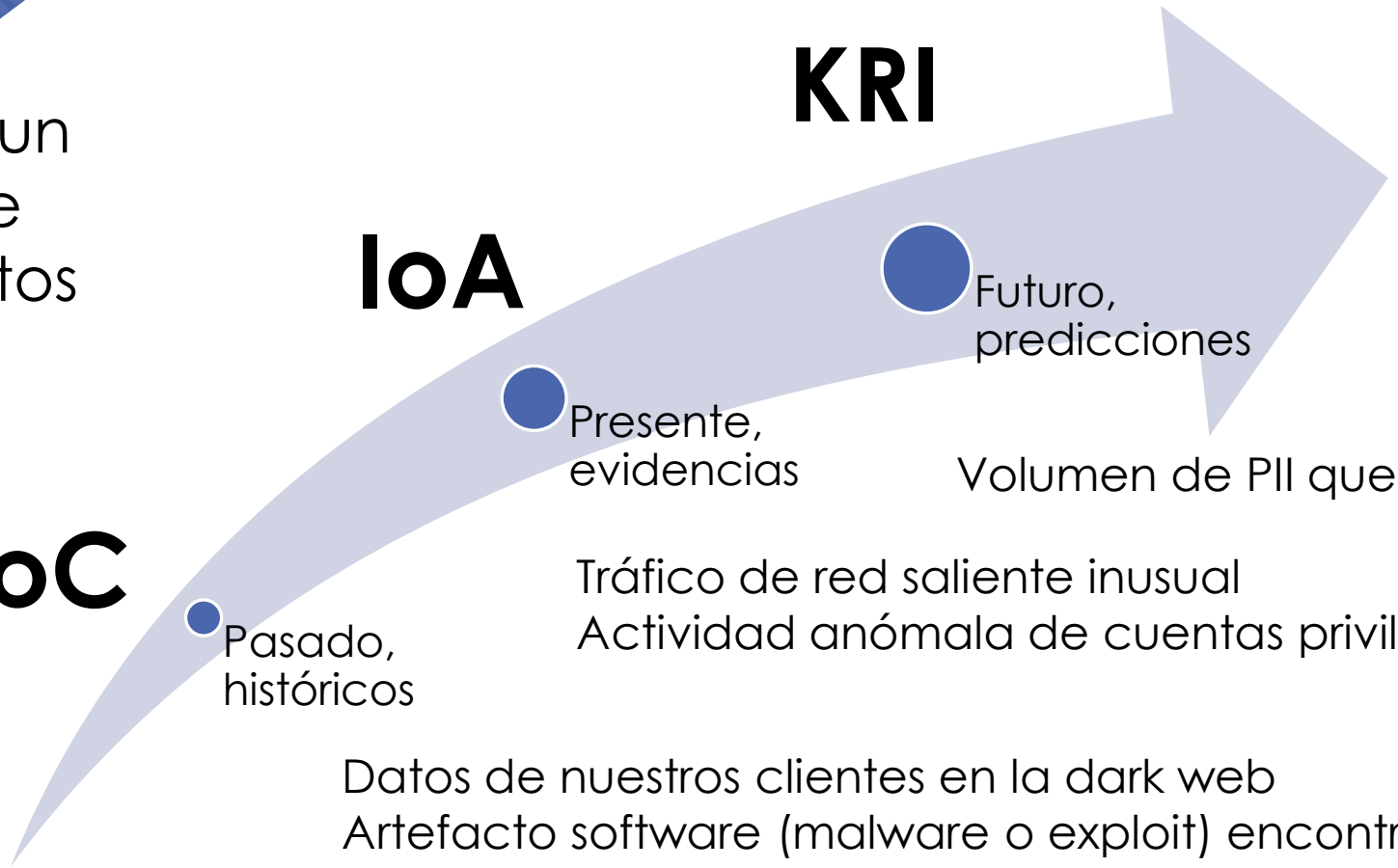
Paper Miguel Calvo y Marta Beltrán

4. KRIs y otras métricas

- Todas estas métricas, que permiten monitorizar el riesgo de una manera o de otra, son difíciles de definir.
  - Tienen que ver con los procesos de análisis y gestión del riesgo porque permiten monitorizar los riesgos.
  - Pero no evalúan o cuantifican el riesgo directamente, cuidado, el objetivo en este caso es diferente.
- Se pretende manejar sistemas de alerta temprana, tener la capacidad de reaccionar lo antes posible.

4. KRIs y otras métricas

Ejemplo para un escenario de brecha de datos



Volumen de PII que se maneja sin cifrar

Tráfico de red saliente inusual
Actividad anómala de cuentas privilegiadas

Datos de nuestros clientes en la dark web
Artefacto software (malware o exploit) encontrado en nuestra red

Para leer e investigar…

- ISO 27004 “Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluationTechnologies” (2016).

Referencias

- Fotografías
  - https://unsplash.com
- Iconos
  - https://www.flaticon.es/