Unidad 1: El concepto de ciberriesgo
BLOQUE I – Introducción al ciberriesgo

Grado en Ingeniería de la Ciberseguridad, curso 2022-2023

CONTENIDOS

1. Definición de riesgo.
2. Particularidades del ciberriesgo.
3. Conceptos básicos relacionados.
4. Tendencias actuales y evolución.
5. Relación con otras asignaturas del plan de estudios.

1. Definición de riesgo

- Según la RAE el riesgo es la contingencia o proximidad de un daño.
  - La palabra "contingencia" se refiere al primer elemento esencial del riesgo, la probabilidad.
  - La palabra "daño" está relacionada con el segundo elemento clave, el impacto.

1. Definición de riesgo

- El concepto de riesgo suele llevar implícito alguno de estos aspectos:
  - Posibilidad de pérdida o daño.
  - Impacto negativo potencial.
  - Probabilidad de un evento no deseado.
- Desde 1988, las organizaciones sin ánimo de lucro, las agencias gubernamentales y las empresas han intentado preocuparse por el riesgo corporativo de una manera rigurosa y sistemática.
  - En este caso se suele entender como riesgo la probabilidad de que los resultados reales no coincidan con los esperados.

1. Definición de riesgo

- Se pueden distinguir distintos tipos de riesgo:
  - Los riesgos de un proyecto, que afectan a la planificación o a los recursos humanos/materiales.
    - Mala ponderación de la dificultad de una tarea, bajas por enfermedad, retrasos de los proveedores.
  - Los riesgos de un producto, que afectan a la calidad o al rendimiento del resultado producido.
    - Falos en la maquinaria, turnos de personal con falta de experiencia, actualización de un producto o servicio.
  - Los riesgos del negocio son aquellos que afectan a la organización y al cumplimiento de sus objetivos estratégicos o de regulaciones y leyes.
    - Cambios en las preferencias de los clientes, crisis de los mercados, tecnología obsoleta, nuevas obligaciones legales.
  - Los riesgos financieros, cuando la empresa no cuenta con liquidez suficiente para llevar a cabo sus operaciones.
    - Retrasos en los cobros a los clientes, incremento de intereses.

1. Definición de riesgo

- En general todos estos riesgos, exceptuando los de proyecto, se denominan también riesgos corporativos, y hablaremos de ellos en la unidad 2 de la asignatura.
- No hay que centrarse exclusivamente en los riesgos que provocan pérdidas financieras directas.
  - Pueden ser igual de importantes o incluso más, los riesgos que provocan incumplimiento de plazos, de objetivos, de regulación.

1. Definición del riesgo

- La pregunta en la actualidad no es si puede pasar algo o no, la pregunta es ¿cuándo me va a pasar, cuánto me va a costar, cómo me puedo preparar?
  - El riesgo se puede definir como un estado de incertidumbre en el que algunos escenarios posibles implican resultados no deseados (una pérdida económica, una catástrofe).

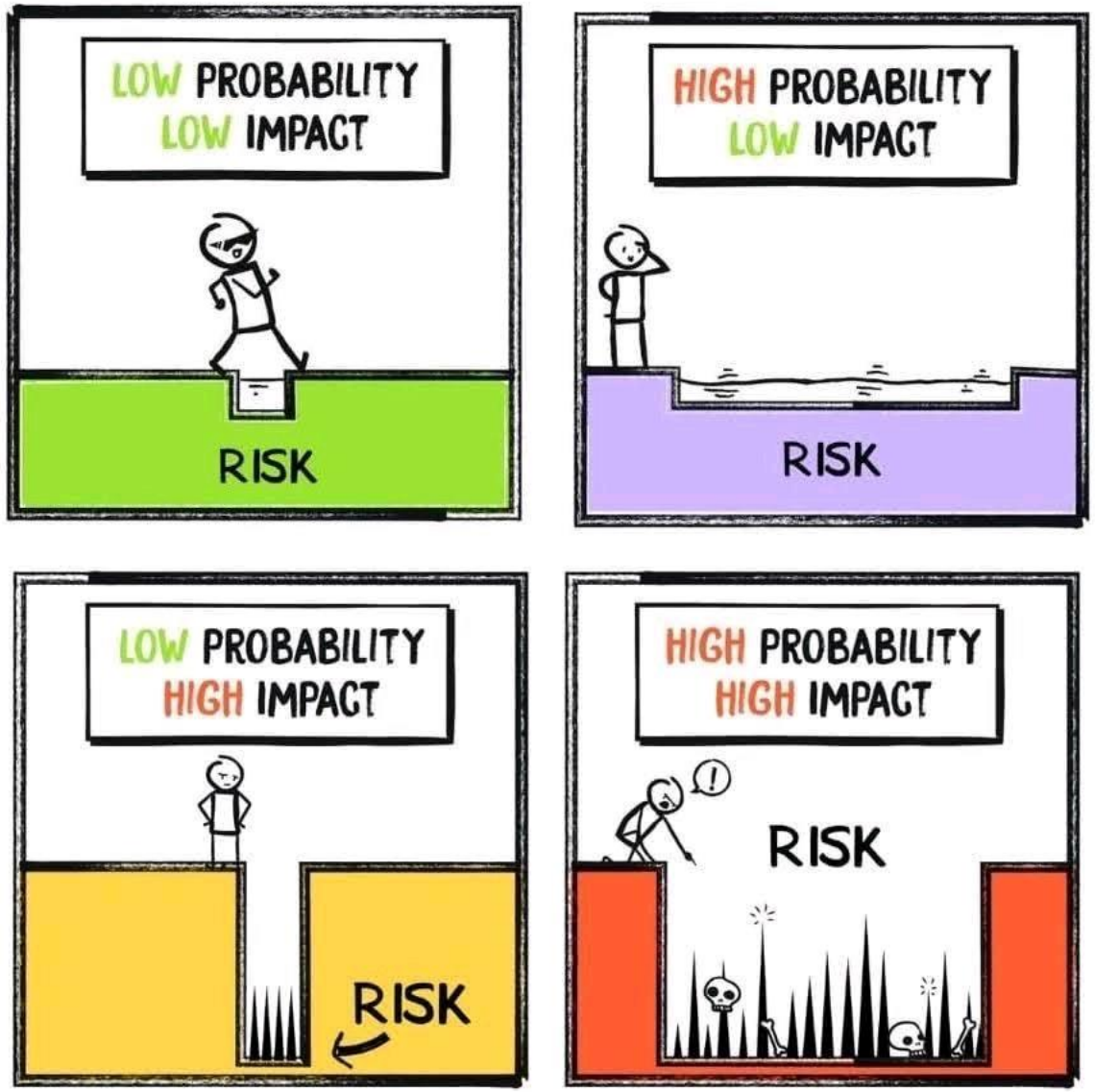
1. Definición del riesgo

- El riesgo en sí mismo no es negativo.
  - Incluso se puede ver como una oportunidad.
- Lo que sí es negativo es que el riesgo esté mal gestionado, mal interpretado, mal cuantificado, oculto o incomprendido.

1. Definición de riesgo

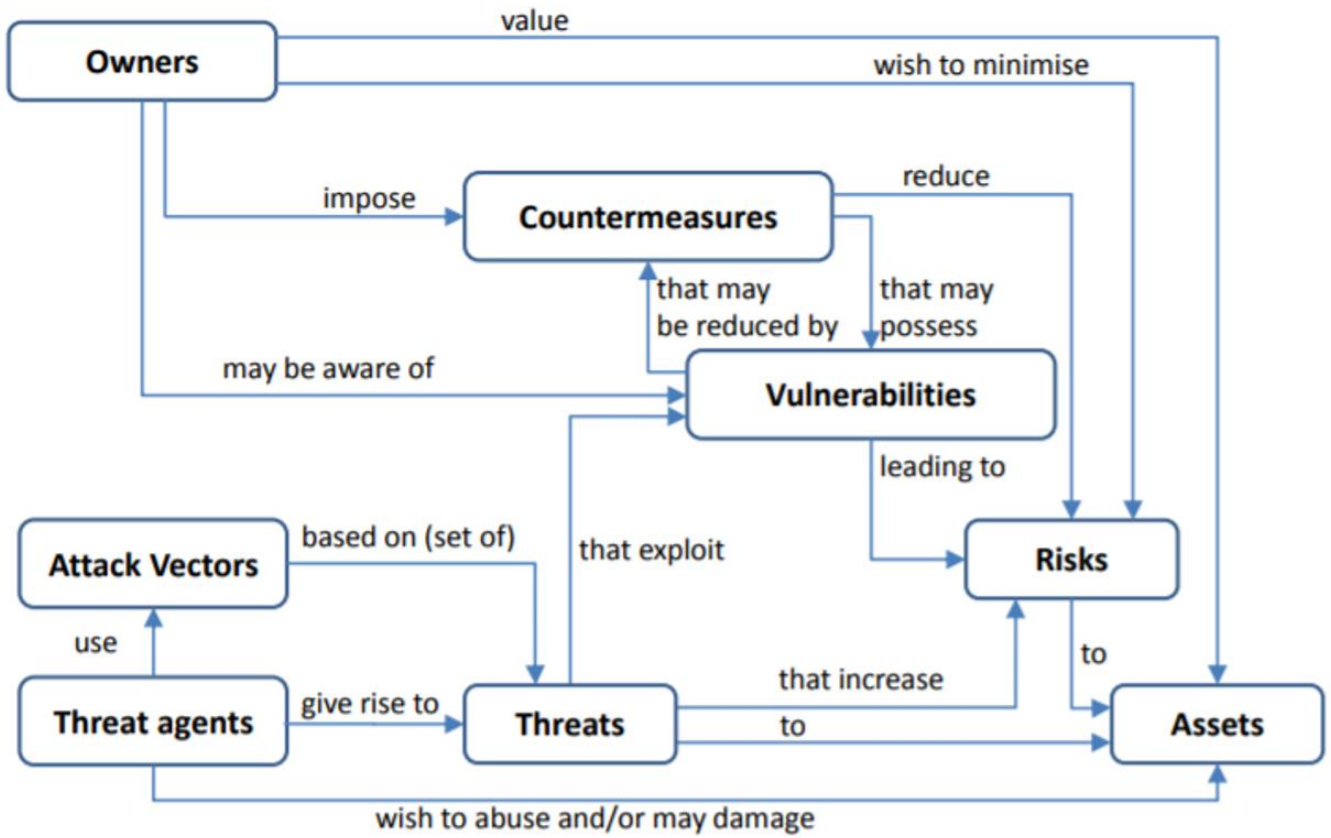
- En resumen, el riesgo es la probabilidad de que un determinado incidente no deseado ocurra y cause un impacto o pérdida en un activo.
  - El incidente reduce el valor de un activo o genera una pérdida relacionada con él.

LEVELS OF RISK



2. Particularidades del ciberriesgo

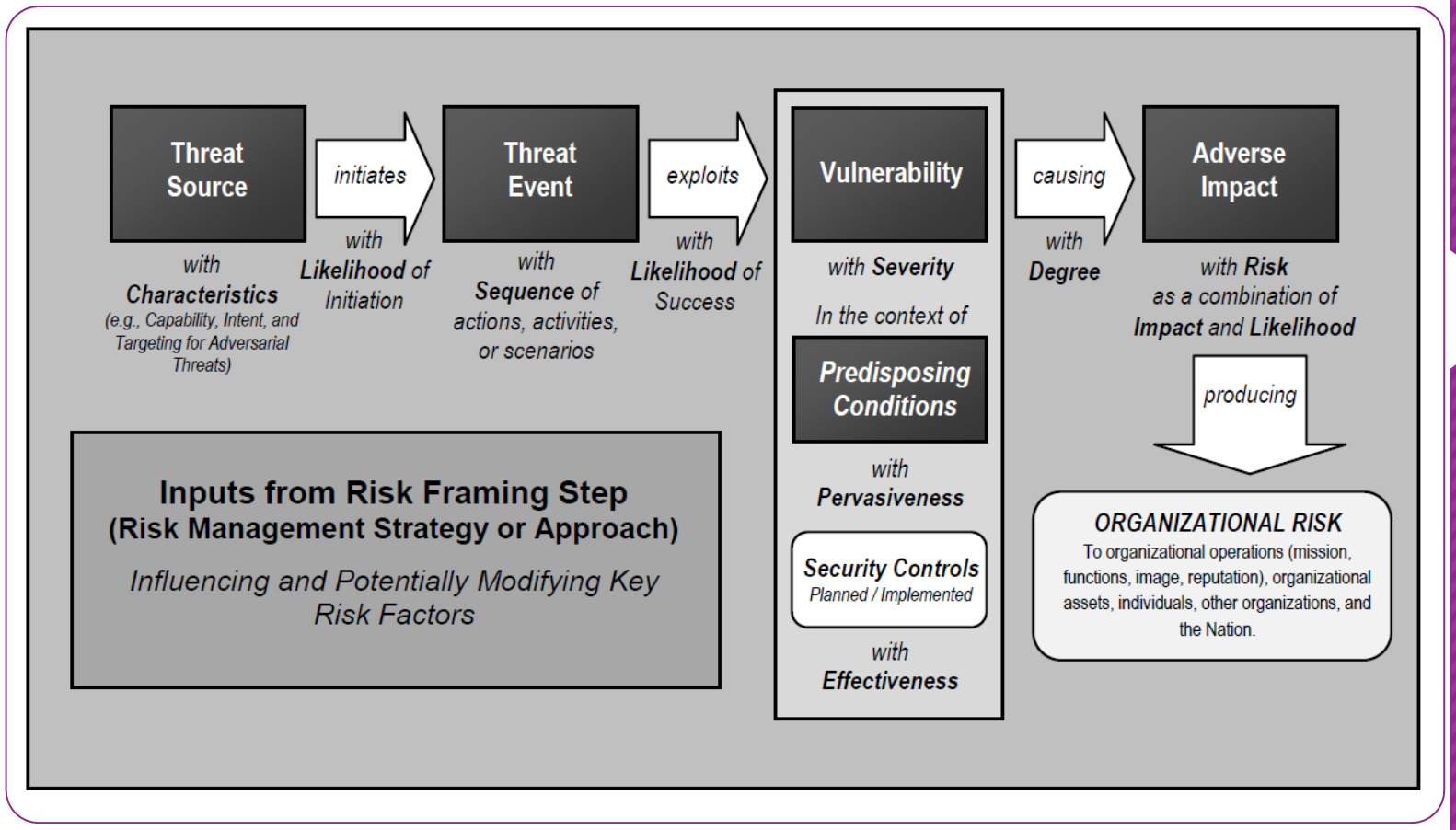
- El ciberriesgo es la probabilidad de que ocurra un incidente de ciberseguridad (provocado por diferentes tipos de agentes amenaza y como consecuencia de la existencia de diferentes tipos vulnerabilidades) que afecte al normal funcionamiento de los activos digitales y que pueda producir un determinado impacto a la propia organización o a un tercero.



Relación entre amenaza, riesgo y vulnerabilidad según el ISO 15408:2005

2.Particularidades del ciberriesgo

2.Particularidades del ciberriesgo



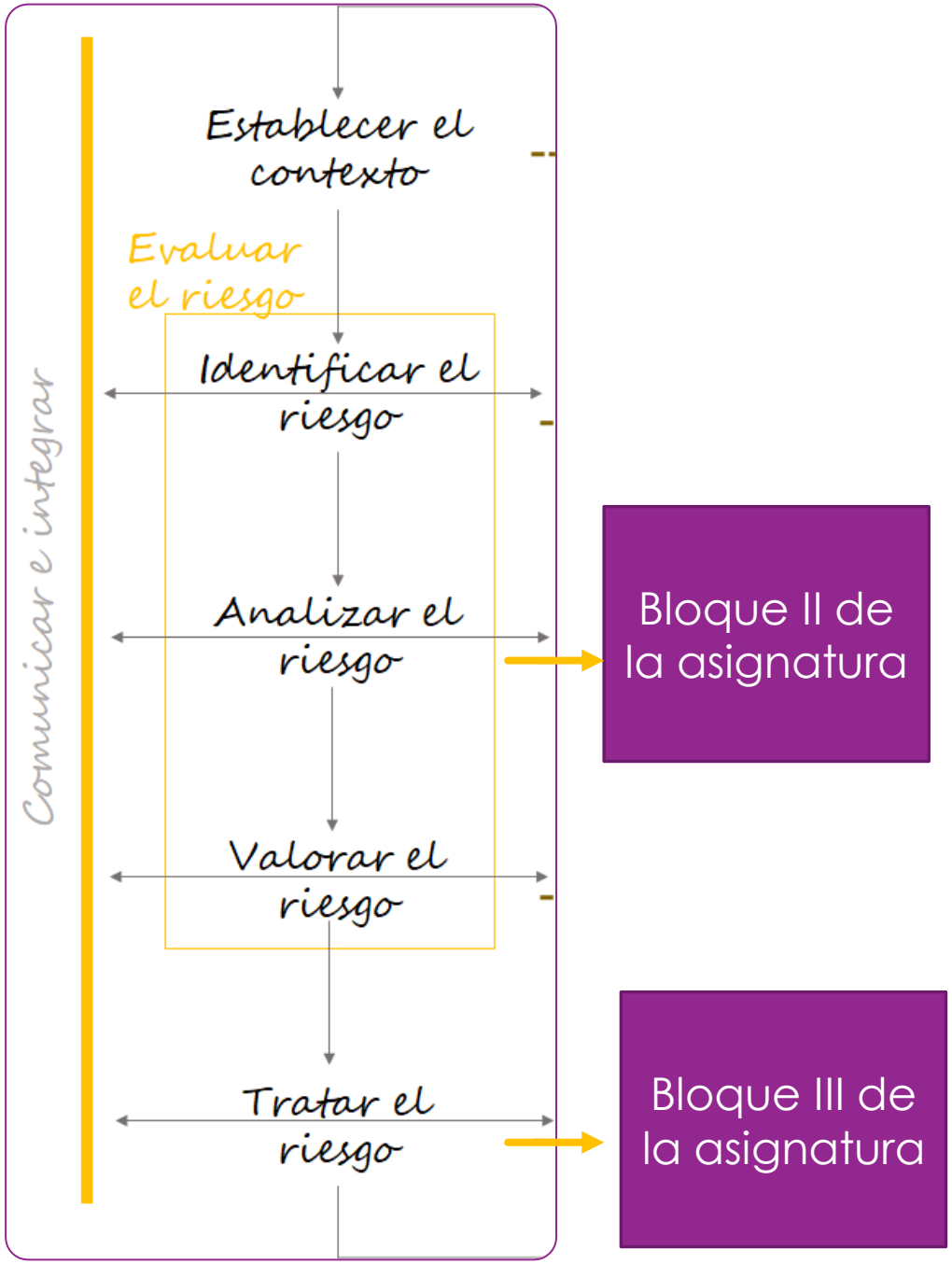
NIST Special Publication 800-30

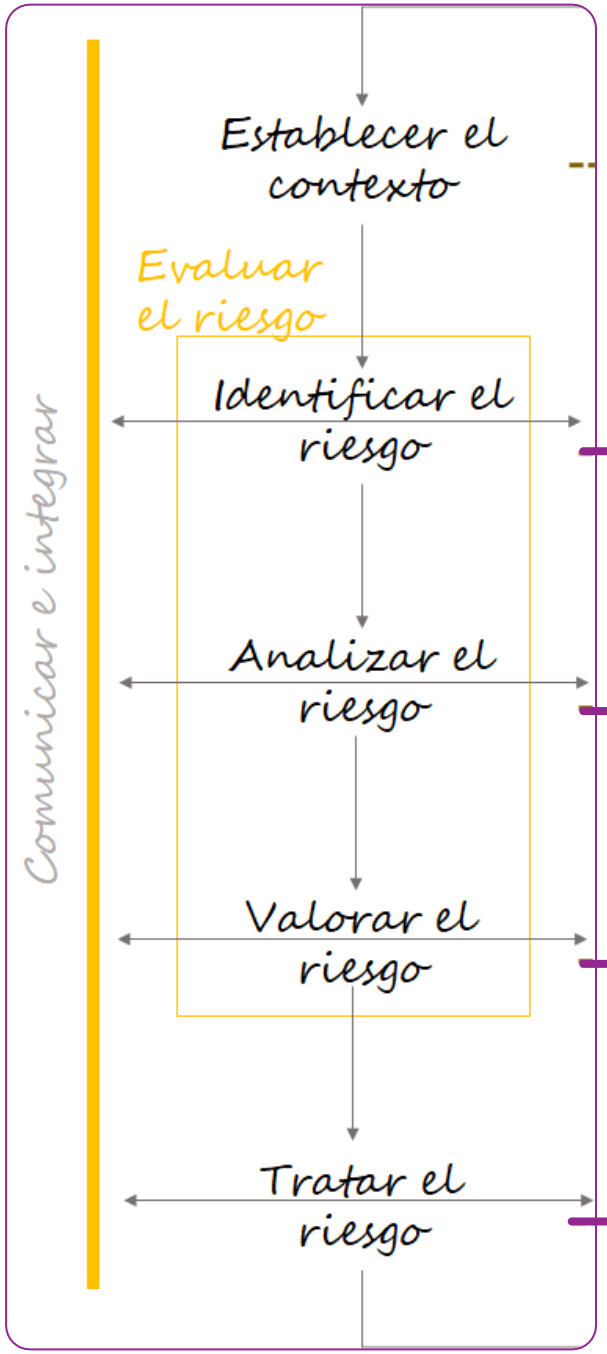
El adversario

2.Particularidades del ciberriesgo

3. Conceptos básicos relacionados

Proceso de evaluación y gestión del ciberriesgo





Entender las amenazas y los agentes detrás de ellas, sus potenciales objetivos, los incidentes que podrían provocar, explotando qué vulnerabilidades, etc.

Para los riesgos identificados, recoger toda la información disponible e intentar estimar, simular, medir, etc. probabilidad e impacto.

Combinar probabilidad e impacto para obtener algún tipo de valor o métrica. Priorizar.

Decidir estrategias (aceptación, evitación, mitigación, transferencia). Planificar.

3. Conceptos básicos relacionados

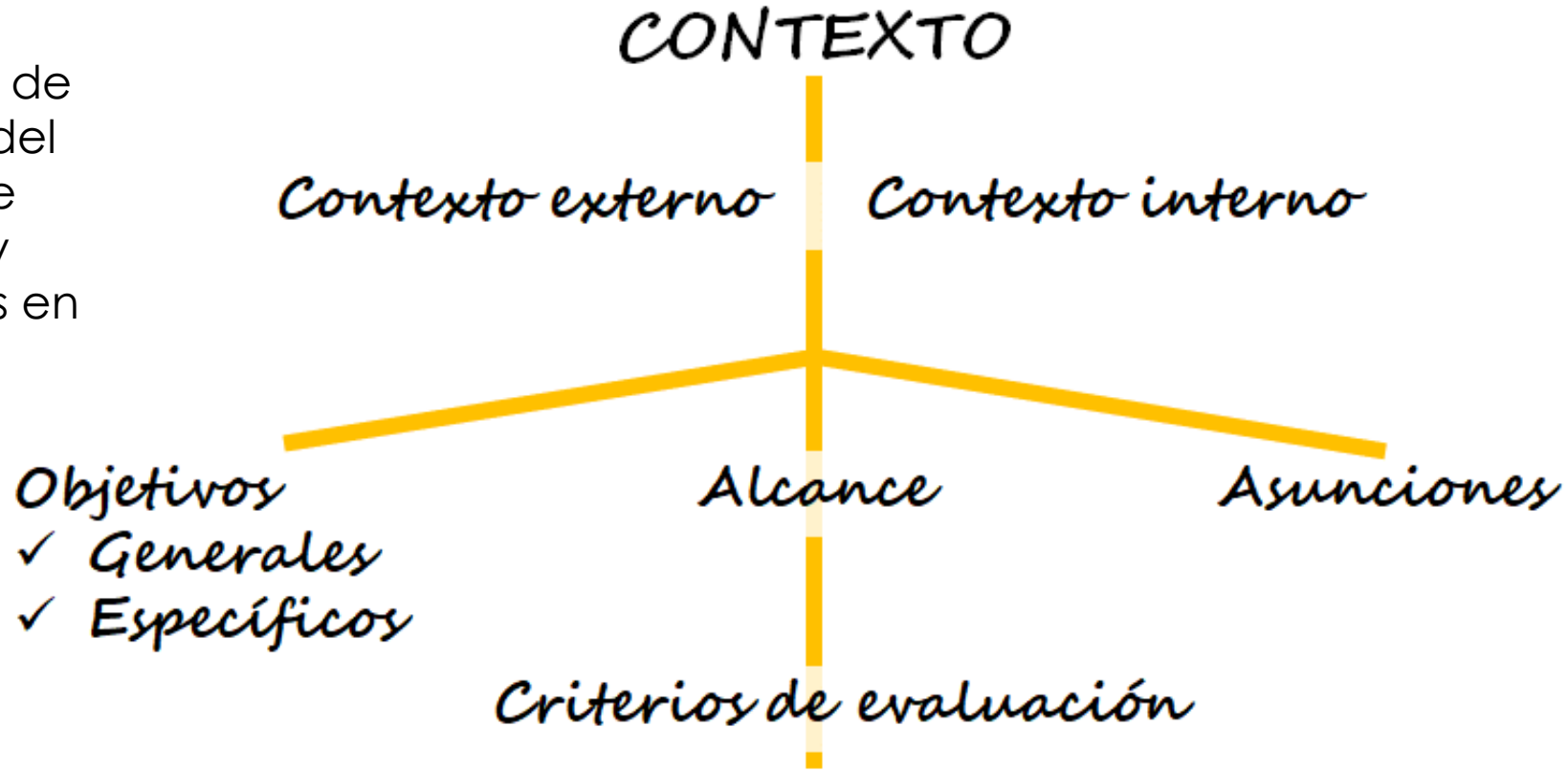
- **Establecer el contexto**
  - Vamos a profundizar un poco en esta fase de momento.
  - El contexto tiene dos ámbitos que hay que investigar:
    - Contexto externo: Información relacionada con el entorno societario, político, legal, regulatorio, tecnológico, etc. en el que la organización se desenvuelve. También con los agentes externos (clientes, proveedores, competencia, inversores) con los que la organización se relaciona.
    - Contexto interno: Objetivos de la organización, estructura organizativa, cultura corporativa, apetito por el riesgo. Procesos, personas y sistemas.

3. Conceptos básicos relacionados

- En esta fase hay que definir también sin ambigüedades los objetivos y alcance de la gestión del ciberriesgo.
  - ¿Qué se pretende conseguir? ¿Qué resultados se esperan? ¿Qué entregables hay que producir? Se deben definir objetivos generales y específicos.
  - ¿Qué procesos, personas y sistemas van a verse involucrados en el proceso? ¿Cuáles serán objeto de análisis?
- También hay que explicitar asunciones, limitaciones.
- Y definir criterios de evaluación e indicadores/métricas.

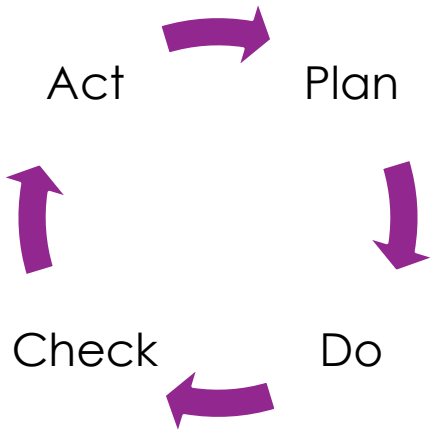
3. Conceptos básicos relacionados

Este debe ser el punto de partida de cualquier proceso de análisis y gestión del riesgo, conviene invertir tiempo y recursos suficientes en hacerlo bien.



3. Conceptos básicos relacionados

- A pesar de cómo suelen dibujarse estos diagramas, el proceso no suele ser lineal.
- Ni se realiza una única vez, los riesgos cambian, hay que repetirlo periódicamente, es un ciclo.
  - El periodo adecuado dependerá de la organización y de su contexto, así como de los objetivos que tenga.
- El proceso de gestión del riesgo debe mejorar de manera continua.
- E intentar anticiparse a lo que viene en el futuro.



3. Conceptos básicos relacionados

- **Apetito por el riesgo**
  - Es el tipo y la cantidad de riesgo que una organización está dispuesta a aceptar o asumir para poder alcanzar sus objetivos estratégicos.
  - Afecta a todos los tipos de riesgo, pero en el caso del ciberriesgo suele costar decidir cuál es, ya que su evaluación no suele estar clara para el comité de dirección como la del riesgo financiero, por ejemplo.
  - Se relaciona con el conceto de **tolerancia al riesgo**, que es límite máximo de riesgo a la que la organización puede estar expuesta.

3. Conceptos básicos relacionados

- **Riesgo inherente y riesgo residual**
  - Esta distinción suele hacerse para diferenciar entre el riesgo al que está expuesto la organización antes de gestionarlo de ninguna manera (el inherente) y el riesgo al que está expuesta tras aplicar alguna estrategia de gestión y desplegar controles, contramedidas, etc. (el residual o mitigado).
  - Obviamente, si las cosas se hacen bien, tras un ciclo de análisis y gestión el riesgo residual debería ser menor que el inherente.

3. Conceptos básicos relacionados

- **Resiliencia**
  - El concepto de *trustworthiness* tiene cada vez más importancia y una relación muy estrecha con la gestión de riesgos.

Privacy	*Reliability*	*Resilience*	*Safety*	*Security*

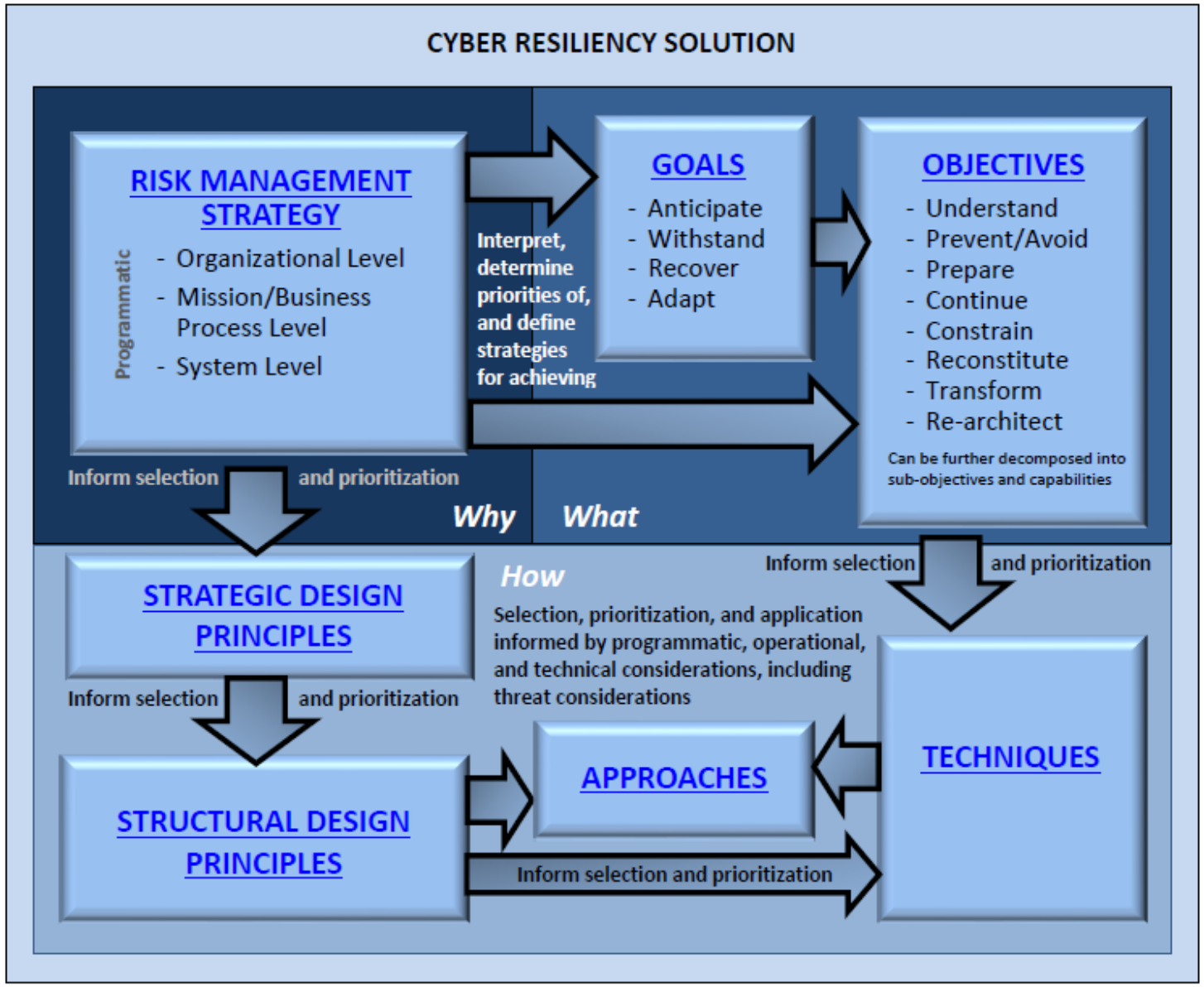
3. Conceptos básicos relacionados

- La resiliencia es el conjunto de procesos que permite a las organizaciones sobreponerse a incidentes o circunstancias desfavorables.
  - Implica capacidad de anticipación y de adaptación positiva.
- En relación con la ciberseguridad y el ciberriesgo, es la capacidad de responder adecuadamente a todo tipo de amenazas (internas o externas, de diferentes grados de sofisticación) de manera que se puedan cumplir los objetivos estratégicos de la organización a pesar de que se produzcan incidentes.

NIST Special Publication 800-160

GOAL	DESCRIPTION
ANTICIPATE	Maintain a state of informed preparedness for adversity.
	Discussion: Adversity refers to adverse conditions, stresses, attacks, or compromises on cyber resources. Adverse conditions can include natural disasters and structural failures (e.g., power failures). Stresses can include unexpectedly high-performance loads. Adversity can be caused or taken advantage of by an APT actor. Informed preparedness involves contingency planning, including plans for mitigating and investigating threat events as well as for responding to discoveries of vulnerabilities or supply chain compromises. Cyber threat intelligence (CTI) provides vital information for informed preparedness.
WITHSTAND	Continue essential mission or business functions despite adversity.
	Discussion: Detection is not required for this goal to be meaningful and achievable. An APT actor's activities may be undetected, or they may be detected but incorrectly attributed to user error or other stresses. The identification of essential organizational missions or business functions is necessary to achieve this goal. In addition, supporting processes, systems, services, networks, and infrastructures must also be identified. The criticality of resources and capabilities of essential functions can vary over time.
RECOVER	Restore mission or business functions during and after adversity.
	Discussion: The restoration of functions and data can be incremental. A key challenge is determining how much trust can be placed in restored functions and data as restoration progresses. Other threat events or conditions in the operational or technical environment can interfere with recovery, and an APT actor may seek to take advantage of confusion about recovery processes to establish a new foothold in the organization's systems.
ADAPT	Modify mission or business functions and/or supporting capabilities in response to predicted changes in the technical, operational, or threat environments.
	Discussion: Change can occur at different scales and over different time frames, so tactical and strategic adaption may be needed. Modification can be applied to processes and procedures as well as technology. Changes in the technical environment can include emerging technologies (e.g., artificial intelligence, 5th generation mobile network [5G], Internet of Things) and the retirement of obsolete products. Changes in the operational environment of the organization can result from regulatory or policy changes, as well as the introduction of new business processes or workflows. Analyses of such changes and of interactions between changes can reveal how these could modify the attack surface or introduce fragility.

NIST Special Publication 800-160



4. Tendencias actuales y evolución

4. Tendencias actuales y evolución

- Incorporar el riesgo asociado a los nuevos paradigmas (cloud, IoT, edge, 5G) y a los nuevos usos de la tecnología.
  - Incorporar en la gestión a las "terceras partes".
- Mejorar las técnicas de cuantificación (objetivas, automatizadas, etc.) aprovechando los avances en mecanismos de analítica avanzada, sistemas expertos, aprendizaje automático, inteligencia artificial, etc.

4. Tendencias actuales y evolución

- Emplear enfoques colaborativos, tanto dentro de las organizaciones como entre organizaciones.
- Gestionar el riesgo de manera dinámica y conseguir seguridad adaptativa, risk-based, inteligente.
  - Resiliencia.
- Emplear nuevas estrategias de gestión más allá de la mitigación clásica.
- Tener en cuenta la relación del ciberriesgo con otros riesgos (agregación, amenazas híbridas, efectos cascada).
- Mejorar los procesos de toma de decisiones.

5. Relación con otras asignaturas del plan de estudios

- Governance, Risk & Compliance (GRC)
  - El gobierno de la seguridad, la gestión de riesgos y el cumplimiento son tres aspectos de la gestión de la ciberseguridad que a menudo tratan sobre las mismas áreas y procesos desde diferentes perspectivas.
  - En el Grado cursáis al mismo tiempo que ésta la asignatura de Regulación y Gobernanza ya que están muy relacionadas.

5. Relación con otras asignaturas del plan de estudios

- El instrumento de control para el GRC es además la función de Auditoría, asignatura que habéis cursado durante el primer cuatrimestre.
- Las asignaturas del itinerario ofensivo del grado (Técnicas de Hacking, Malware y amenazas dirigidas, Pentesting) os proporcionan la base para comprender las amenazas y para identificar los escenarios de ciberriesgo, así cómo para cuantificar probabilidades e impactos.

5. Relación con otras asignaturas del plan de estudios

- Las asignaturas del itinerario defensivo del grado (Criptografía, Seguridad en redes, Seguridad en Bases de datos) os proporcionan la base para la gestión del riesgo mediante estrategias de mitigación.
- Por último, las asignaturas como Dimensiones y modelo de la Seguridad o Principios jurídicos, os proporcionan un contexto en temas relacionados con la Seguridad Nacional o la Privacidad, por mencionar sólo un par de ejemplos.

Para leer e investigar…

- "The Global Risks Report 2022", WEF.
- "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach", NIST SP 800-160 Vol. 2 Rev. 1 (Diciembre 2021).

Referencias

- Fotografías
  - https://unsplash.com
- Iconos
  - https://www.flaticon.es/
- Figuras sobre riesgo:
  - "Dirección de seguridad y gestión del ciberriesgo" Fernando Sevillano y Marta Beltrán. Colección Ciberseguridad, editorial RaMa. 2021.