Unidad 4: Métodos cualitativos

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

Grado en Ingeniería de la Ciberseguridad, curso 2022-2023

CONTENIDOS

1. Métodos cualitativos.
2. Niveles de madurez.
3. Mapas de calor y matrices de riesgo.
4. CORAS.
5. Magerit.

1. Métodos cualitativos

- Cuando se habla de métodos cualitativos para la evaluación del ciberriesgo, nos referimos a que la fase de análisis no es numérica ni basada en modelos formales, simulaciones o experimentos.
- Por el contrario, se emplean métodos y herramientas tradicionales de la investigación cualitativa.

1. Métodos cualitativos

Auto-evaluación de madurez	Entrevistas individuales	Grupos de discusión
Paneles de expertos externos	Talleres de calibración	Observación participante

1. Métodos cualitativos

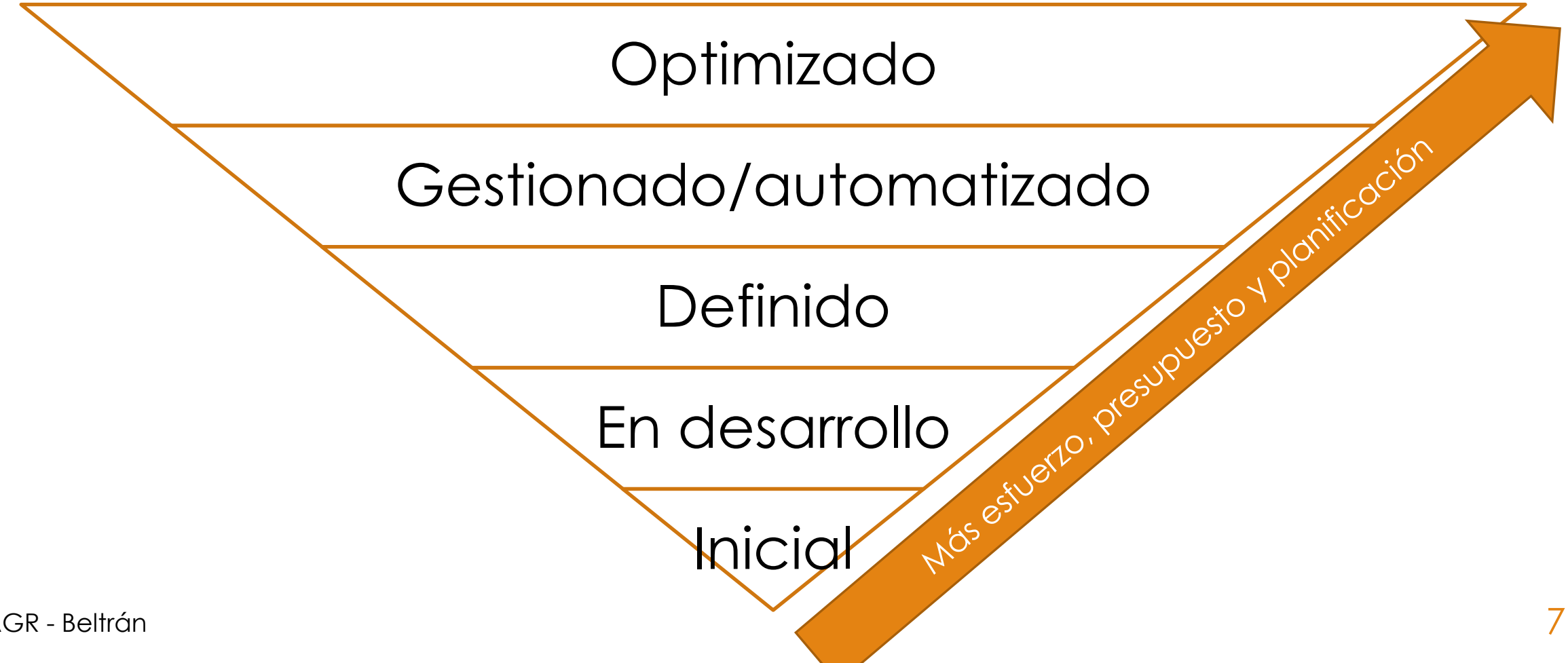
Herramientas que suelen ser útiles:

Cuestionarios	Listas de comprobación	Matrices, tablas, mapas	Método Delphi
Catálogos, listados, glosarios	Árboles y diagramas de amenaza/ataque	Diagramas UML	Esquemas XML

2. Niveles de madurez

- Ya hemos estudiado este concepto al final de la unidad anterior.
- No se trata de procesos de evaluación de riesgo pero sí que pueden ayudar a realizarlos.
- Además, son herramientas muy útiles para la gestión del riesgo, ya que permiten realizar mejora continua.
  - Se pueden fijar objetivos para ir subiendo el nivel de madurez.

2. Niveles de madurez



2. Niveles de madurez

- Ventajas de trabajar con niveles de madurez:
  - Miden cómo se ajusta a la organización a un estándar o marco de trabajo propuesto por expertos y teniendo en cuenta mejores prácticas, experiencias positivas del pasado, etc.
  - Se adaptan a diferentes tipos de organizaciones (tamaño, presupuesto, sector de actividad).
  - Ayudan a realizar benchmarking y comparativas objetivas.
  - Son una herramienta ideal para definir planes y programas siguiendo ciclos PDCA.
  - Son una buena base para realizar comunicación interna y externa.

2. Niveles de madurez

- Vamos a estudiar dos ejemplos que son muy utilizados, ambos estadounidenses.
  - El Cybersecurity Framework (CSF) del NIST para IT (y OT, pero no es específico).
    - Publicado en 2014, con actualizaciones prácticamente anuales desde el 2017.
    - Muy relacionado con las propuestas del NIST 800-53.
  - El C2M2 para OT.
    - Publicado en 2012, con actualizaciones en 2014 y 2019.

2. Niveles de madurez

	Niveles de madurez	Dominios evaluados	Procesos y capacidades	Controles y mejores prácticas
NIST CSF	4	23	108	240
C2M2	3	10	38	210

Ambos son auto-evaluados

2. Niveles de madurez

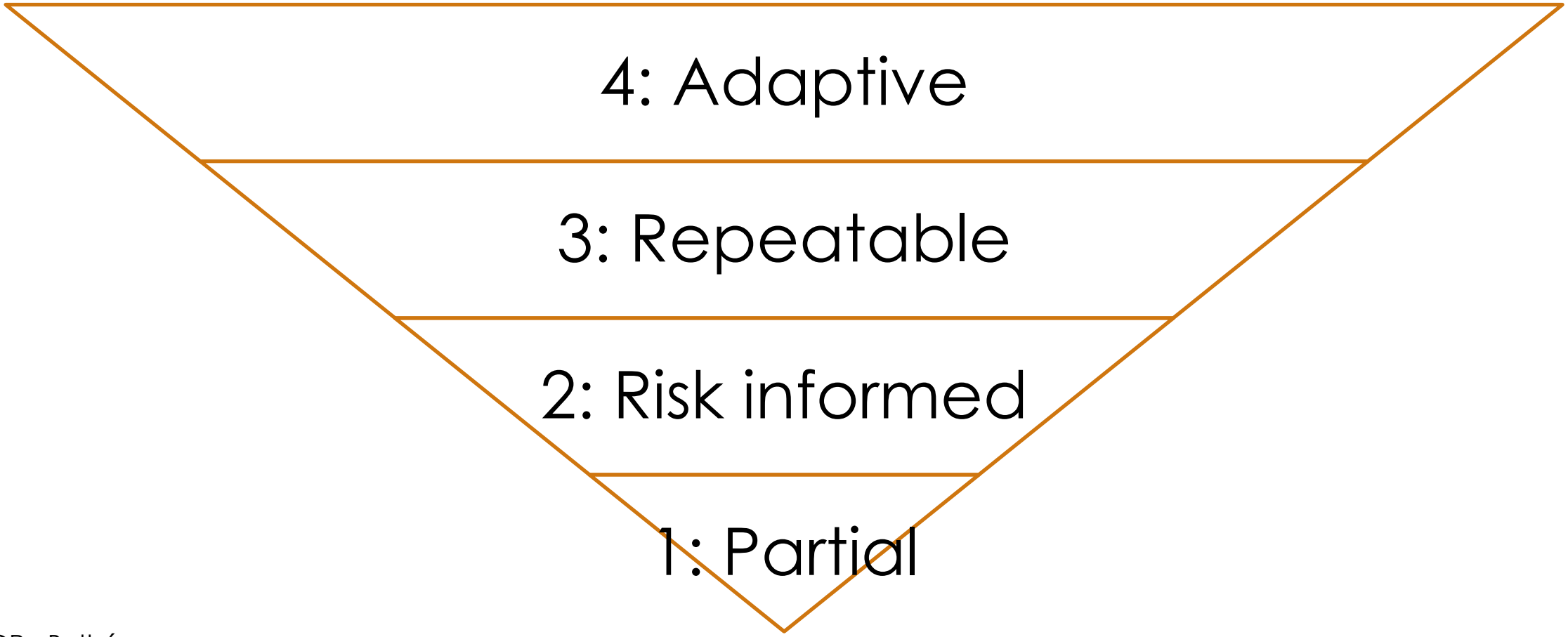
- NIST CSF

https://www.nist.gov/cyberframework/framework

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

https://www.nist.gov/cyberframework/framework

2. Niveles de madurez



2. Niveles de madurez

- Los criterios para puntuar en cada uno de estos cuatro niveles están especificados en la documentación.
- Por ejemplo, para Tier 1 (Partial).

Risk Management Process – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.

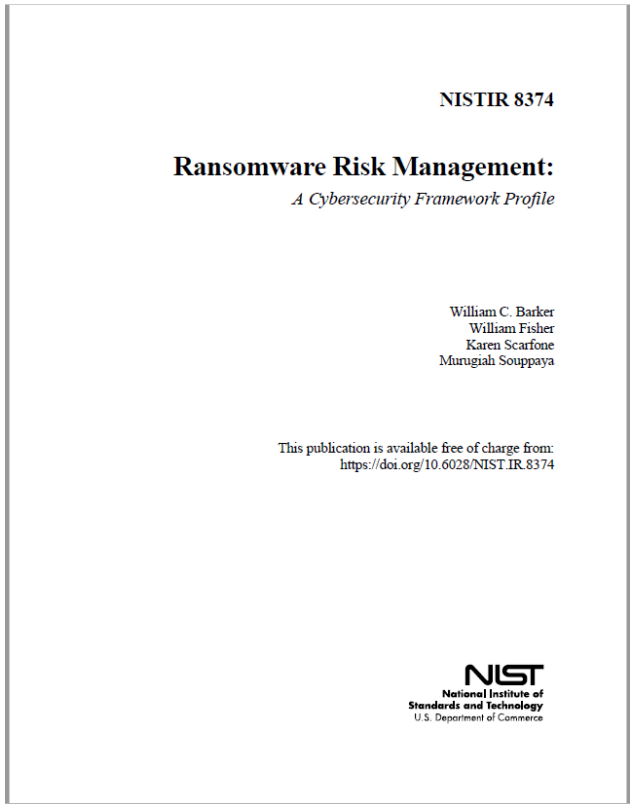
Integrated Risk Management Program – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.

External Participation – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.

2. Niveles de madurez

- Este framework está muy extendido y hay muchas iniciativas interesantes a su alrededor (herramientas interactivas, compartición de inteligencia, etc.).
- Para ayudar a utilizar el framework, el NIST va publicando "profiles", es decir, niveles de madurez objetivo que serían razonables para diferentes tipos de organizaciones con diferentes características.
- Uno de los últimos es el profile para protegerse frente al Ransomware.

2. Niveles de madurez



NISTIR 8374

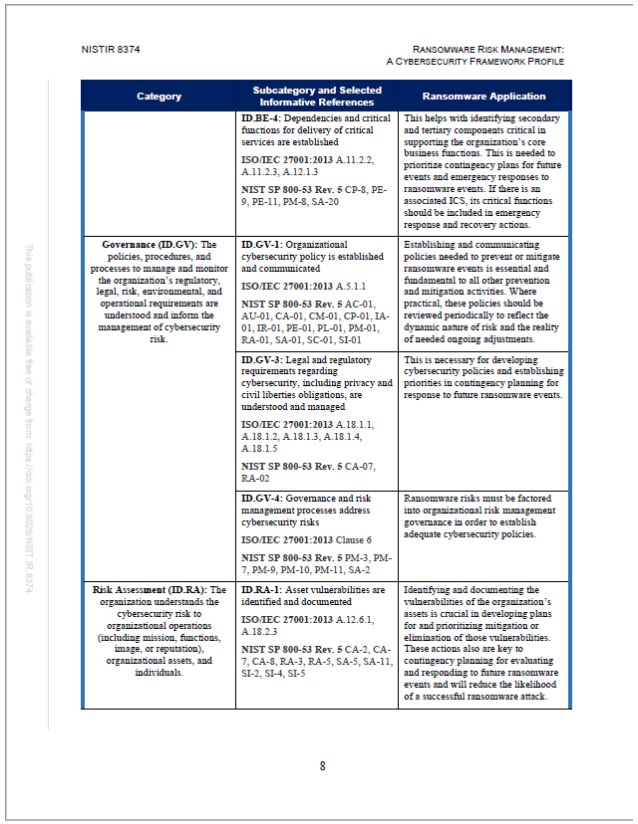
Ransomware Risk Management:

A Cybersecurity Framework Profile

William C. Barker
William Fisher
Karen Scarfone
Murugiah Souppaya

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

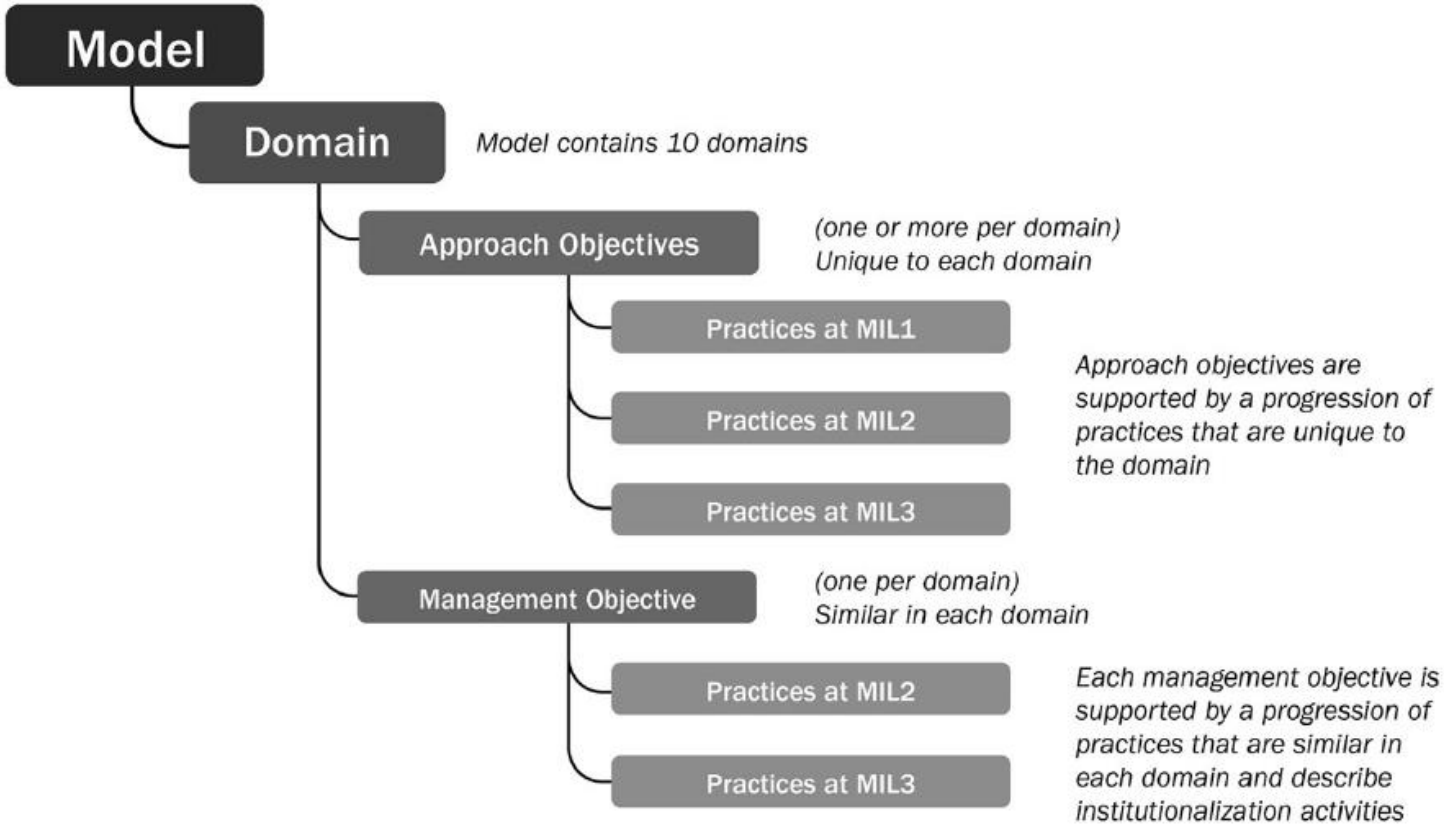


Category	Subcategory and Selected Informative References	Ransomware Application
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 5** CP-8, PE-9, PE-11, PM-8, SA-20	This helps with identifying secondary and tertiary components critical in supporting the organization's core business functions. This is needed to prioritize contingency plans for future events and emergency responses to ransomware events. If there is an associated ICS, its critical functions should be included in emergency response and recovery actions.
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 5** AC-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, PE-01, PL-01, PM-01, RA-01, SA-01, SC-01, SI-01	Establishing and communicating policies needed to prevent or mitigate ransomware events is essential and fundamental to all other prevention and mitigation activities. Where practical, these policies should be reviewed periodically to reflect the dynamic nature of risk and the reality of needed ongoing adjustments.
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 5** CA-07, RA-02	This is necessary for developing cybersecurity policies and establishing priorities in contingency planning for response to future ransomware events.
	ID.GV-4: Governance and risk management processes address cybersecurity risks **ISO/IEC 27001:2013** Clause 6 **NIST SP 800-53 Rev. 5** PM-3, PM-7, PM-9, PM-10, PM-11, SA-2	Ransomware risks must be factored into organizational risk management governance in order to establish adequate cybersecurity policies.
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 5** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	Identifying and documenting the vulnerabilities of the organization's assets is crucial in developing plans for and prioritizing mitigation or elimination of those vulnerabilities. These actions also are key to contingency planning for evaluating and responding to future ransomware events and will reduce the likelihood of a successful ransomware attack.

https://csrc.nist.gov/publications/detail/nistir/8374/final

2. Niveles de madurez

- C2M2



https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

2. Niveles de madurez

C2M2 Domains

Asset, Change, and Configuration Management (ASSET)	**Risk Management** (RISK)
Cybersecurity Architecture (ARCHITECTURE)	**Situational Awareness** (SITUATION)
Cybersecurity Program Management (PROGRAM)	**Third-Party Risk Management** (THIRD-PARTIES)
Event and Incident Response, Continuity of Operations (RESPONSE)	**Threat and Vulnerability Management** (THREAT)
Identity and Access Management (ACCESS)	**Workforce Management** (WORKFORCE)

https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

2. Niveles de madurez

Level	Characteristics
MIL0	• Practices are not performed
MIL1	• Initial practices are performed but may be ad hoc
MIL2	Management characteristics: • Practices are documented • Adequate resources are provided to support the process Approach characteristic: • Practices are more complete or advanced than at MIL1
MIL3	Management characteristics: • Activities are guided by policies (or other organizational directives) • Personnel performing the practices have adequate skills and knowledge • Responsibility, accountability, and authority for performing the practices are assigned • The effectiveness of activities is evaluated and tracked Approach characteristic: • Practices are more complete or advanced than at MIL2

https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

2. Niveles de madurez

El propio marco te ayuda a evaluar tu nivel de madurez para cada control o mejor práctica en cada dominio:

2. Control Logical Access

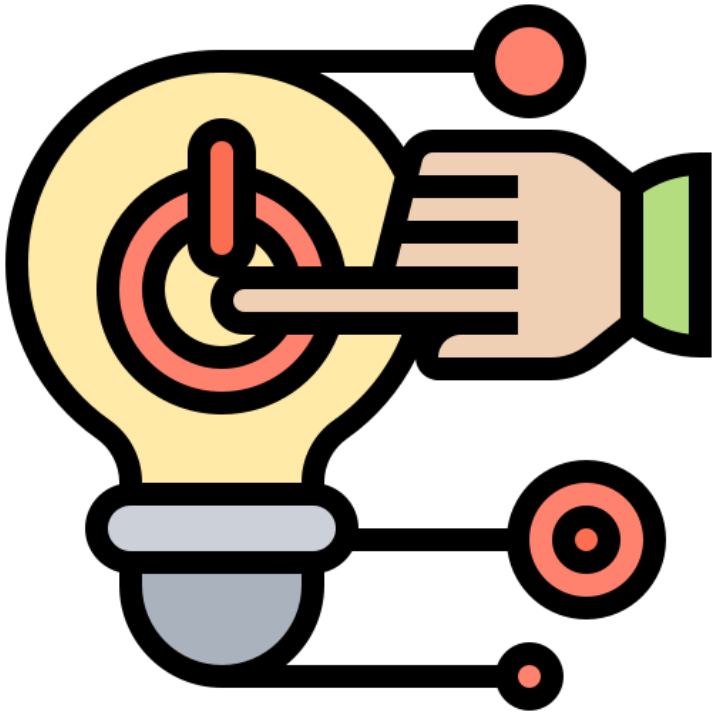
MIL1	a.	Logical access controls are implemented, at least in an ad hoc manner
	b.	Logical access is revoked when no longer needed, at least in an ad hoc manner
MIL2	c.	Logical access requirements are determined (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters)
	d.	Logical access requirements incorporate the principle of least privilege
	e.	Logical access requirements incorporate separation of duties
	f.	Logical access requests are reviewed and approved by the asset owner
	g.	Logical access that poses higher risk to the function receives additional scrutiny and monitoring
MIL3	h.	Logical access privileges are reviewed and updated to ensure conformance with access requirements periodically and according to defined triggers, such as changes to organizational structure, and after any temporary elevation of privileges
	i.	Anomalous access attempts are monitored as indicators of cybersecurity events

https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

2. Niveles de madurez

- En general, recuerda que cualquier estándar o marco de trabajo se puede convertir a un nivel de madurez si necesitas evaluar hasta qué punto se están cumpliendo sus exigencias o recomendaciones.

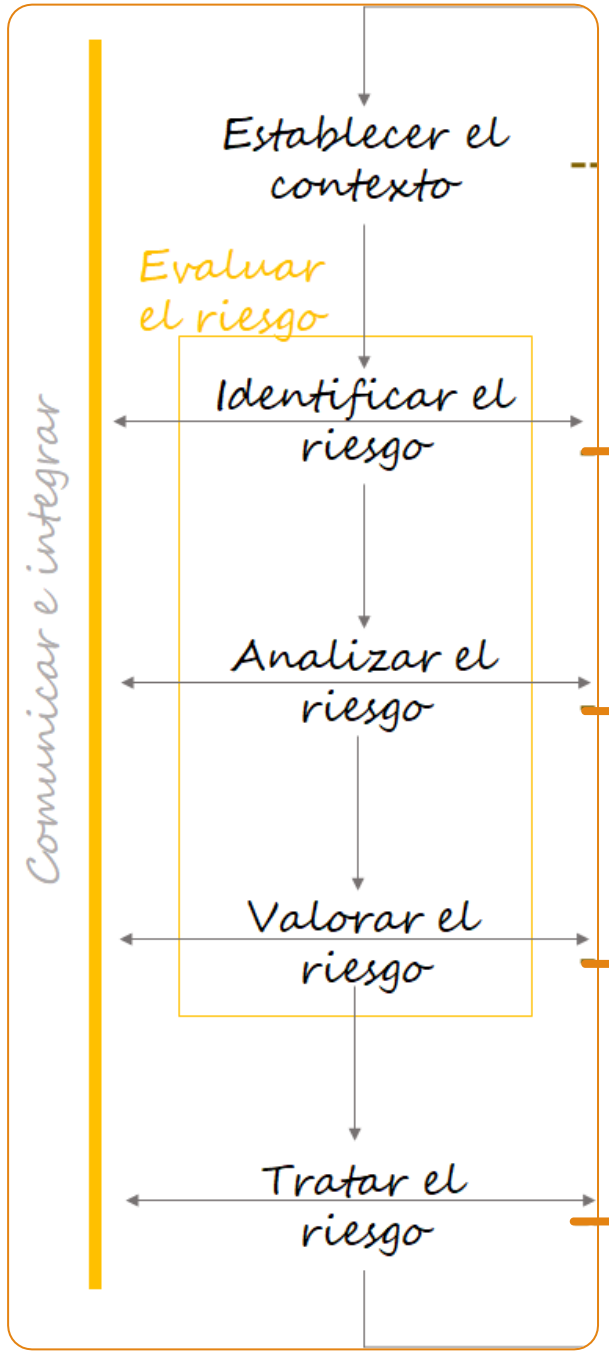
2. Niveles de madurez



CASO 1

3. Mapas de calor y matrices de riesgo

- Los niveles de madurez pueden ser muy útiles en la evaluación y gestión del riesgo.
- Pero, como ya hemos comentado, no es su objetivo evaluar directamente el ciberriesgo.
  - Simplemente, pueden ayudar a hacerlo.
- Tradicionalmente, para la evaluación se ha trabajado con las fases o etapas que ya hemos mencionado.



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. Mapas de calor y matrices de riesgo

- La mayor parte de las metodologías que hemos estudiado en la unidad anterior se basan en métodos cualitativos.
- Esto implica estimar probabilidades e impactos de manera subjetiva, no aplicando técnicas estadísticas o modelos formales.
  - Cuidado, no implica que el proceso sea menos valioso o útil, simplemente, hay que conocer las limitaciones que tiene hacerlo así.

3. Mapas de calor y matrices de riesgo

- Casi todas las metodologías cualitativas estiman probabilidad e impacto mediante escalas, tablas y matrices.
- Y las combinan de manera que llegan a valores cualitativos (riesgo bajo, medio, alto) o cuantitativos (sobre una puntuación máxima o en %).
- Se suele recurrir a representaciones gráficas de tipo matriz o mapa de calor.
- Veamos algunos ejemplos.

3. Mapas de calor y matrices de riesgo

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

NIST Special Publication 800-30

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

3. Mapas de calor y matrices de riesgo

Probabilidad	Descripción
Muy alta	Se espera que ocurra casi siempre.
Alta	Es muy probable que ocurra.
Media	Puede ocurrir en ocasiones.
Baja	No se espera que ocurra, es raro.
Muy baja	Es casi imposible que ocurra.

Estudiaremos en profundidad cómo hacer estas estimaciones un poco más adelante

Probabilidad	Descripción
5	Ocurre al menos 1 vez cada 2 años.
4	Ocurre como mucho 1 vez cada 5 años.
3	Ocurre como mucho 1 vez cada 10 años.
2	Ocurre como mucho 1 vez cada 25 años.
1	Ocurre como mucho 1 vez cada 50 años.

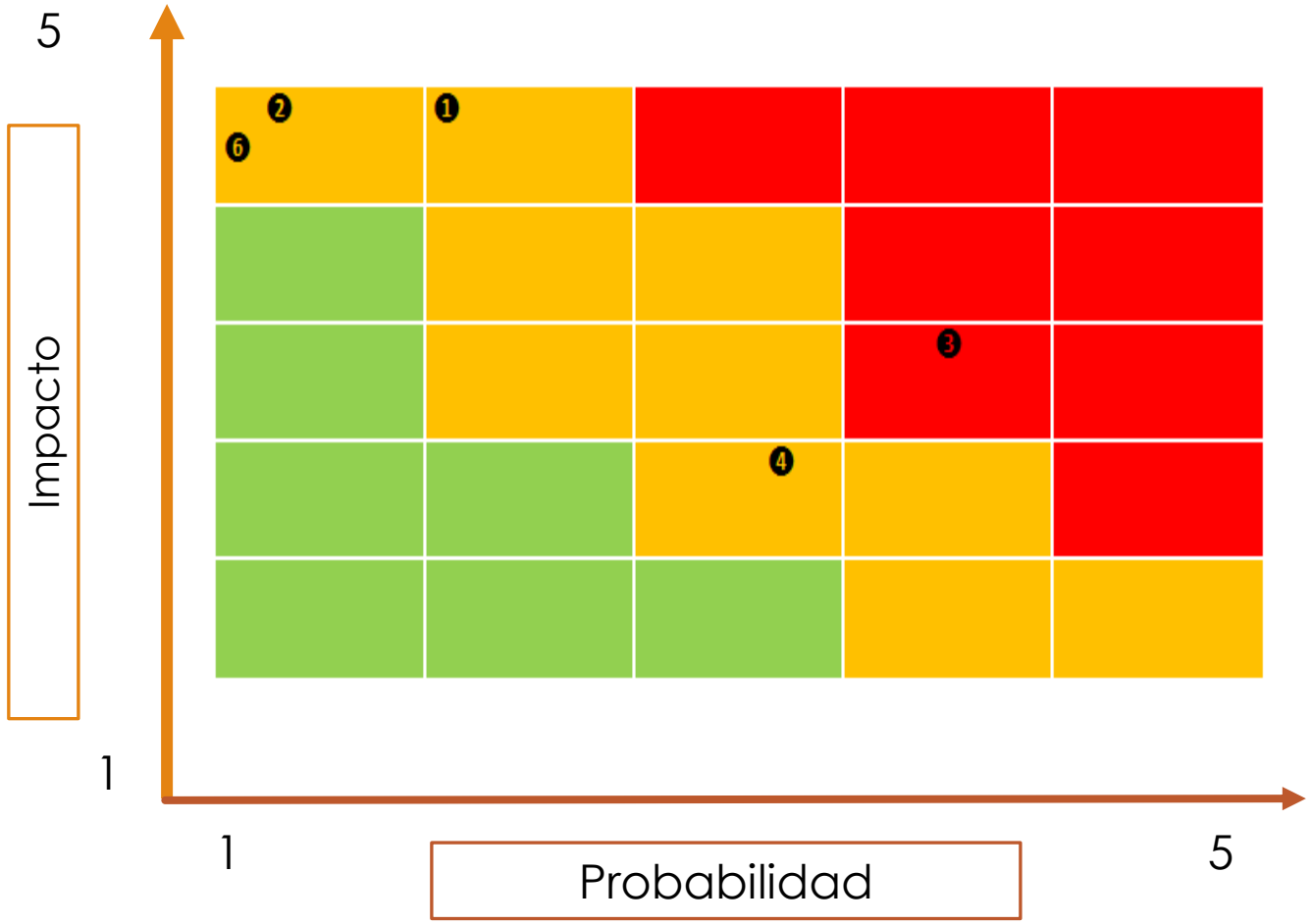
3. Mapas de calor y matrices de riesgo

Impacto	Descripción
Muy alto	Consecuencias catastróficas
Alto	Consecuencias graves
Medio	Consecuencias moderadas
Bajo	Consecuencias leves
Muy bajo	Consecuencias casi despreciables

Estudiaremos en profundidad cómo hacer estas estimaciones de impacto un poco más adelante

Impacto	Descripción
4	Se filtran datos de más de 10.000 usuarios
3	Se filtran datos de entre 1000 y 10.000 usuarios
2	Se filtran datos de entre 100 y 1000 usuarios
1	Se filtran datos de <100 usuarios

3. Mapas de calor y matrices de riesgo



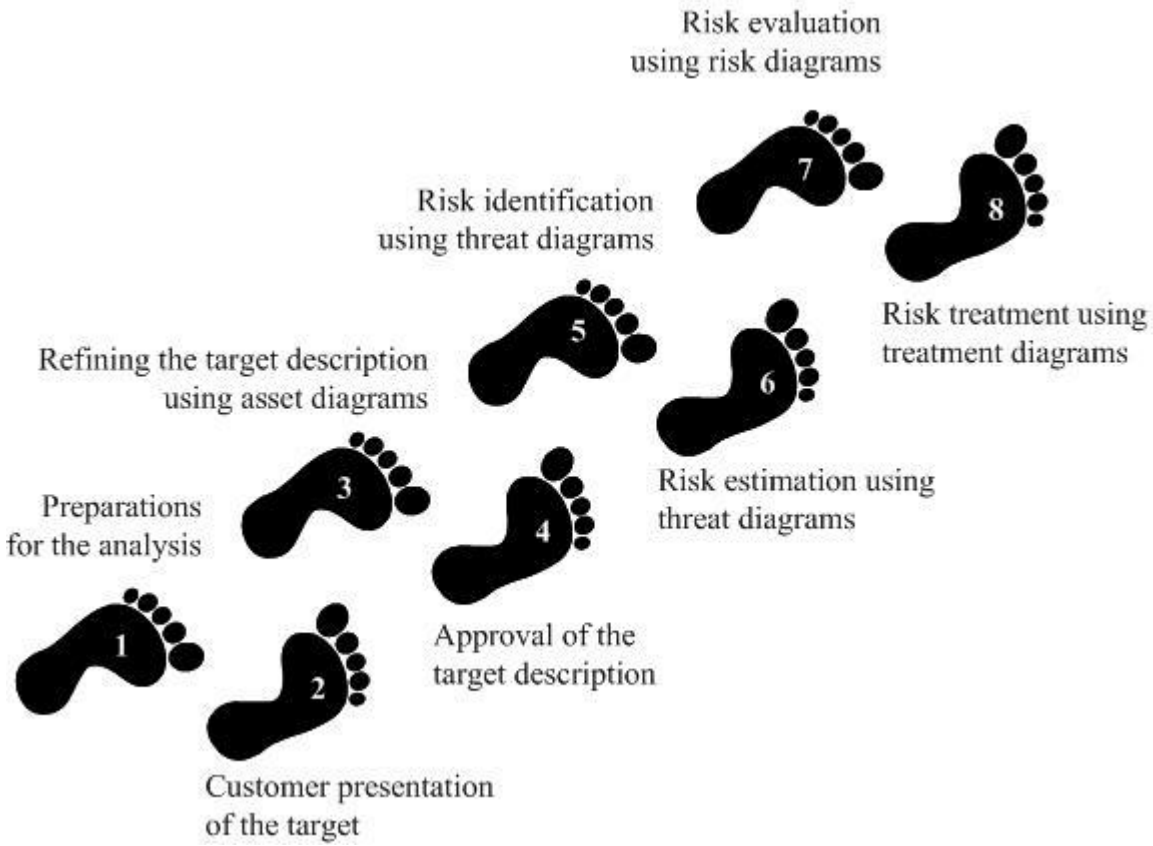
4. CORAS

- CORAS es una metodología de gestión de riesgos que surge de un proyecto financiado por la Unión Europea que finaliza en el año 2003.
- Es desarrollada por un grupo de investigadores noruego.
  - Mantenida y actualizada por la comunidad como proyecto open source.
- Se basa en los estándares de la ISO (27002 y 31000, sobre todo).
- Pero intenta ser mucho más asequible, proponiendo unos pasos concretos y aportando herramientas para llevarlos a cabo.
  - Muy utilizada por pequeñas y medianas empresas europeas.

4. CORAS

- Esta metodología permite modelar la relación existente entre agentes, activos, amenazas, escenarios de amenazas, incidentes, vulnerabilidades y riesgos.
  - Para ello utiliza el lenguaje UML (Unified Modeling Language).
- En la documentación asociada a la metodología CORAS, se habla siempre de dos partes implicadas: el cliente y el analista de riesgos.
  - La comunicación entre ambas partes es fundamental. De hecho, CORAS propone hasta un total de cuatro etapas que ayudan a establecerla de manera adecuada.

4. CORAS



http://coras.sourceforge.net/index.html

4. CORAS

1. Preparación para el análisis: Se conoce al cliente, se comprenden sus necesidades, se analiza su situación y la información disponible, y se definen responsabilidades.
2. Presentación por parte del cliente del objetivo del proyecto: Se define con cierto detalle el contexto, los agentes involucrados, los objetivos y el alcance del proyecto. Para ello el analista de riesgos lleva a cabo entrevistas con el cliente, se realiza una introducción de CORAS como metodología y se establece una nomenclatura común entre todas las partes involucradas.

4. CORAS

3. Redefinición del objetivo mediante diagramas de activos: Se genera una representación gráfica del proyecto mediante UML y la biblioteca de iconos de CORAS. Se identifican los activos y su criticidad. Y se realiza una identificación de los riesgos intentando contestar a estas preguntas:

¿Quién puede provocar los riesgos?	¿Cómo? ¿Qué activo ser vería involucrado? ¿Qué incidente se provocaría?	¿Qué lo hace posible? ¿Qué vulnerabilidad se explotaría?

4. CORAS

4. Aprobación del objetivo: Con estos primeros diagramas, el analista debe obtener la aprobación del cliente. Es el momento de solucionar malentendidos, de corregir el inventario de activos, de discutir acerca de la identificación de riesgos realizada, etc. antes de avanzar más en el proyecto. Se deciden además los criterios con los que el analista trabajará en los siguientes pasos de la metodología (probabilidad e impacto).

4. CORAS

Consequence	Description
Catastrophic	Catastrophic accident
Major	Abrupt manoeuvre required
Moderate	Recovery from large reduction in separation
Minor	Increasing workload of ATCOs or pilots
Insignificant	No hazardous effect on operations

Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen. Risk analysis of changing and evolving systems using CORAS. Foundations of Security Analysis and Design VI (FOSAD'11), number 6858 in Lecture Notes in Computer Science, pages 231-274, Springer 2011.

Ejemplos de escalas para los impactos

Consequence	Description
Catastrophic	Loss of data that can be utilised in terror
Major	Data loss of legal implications
Moderate	Distortion of air company competition
Minor	Loss of aircraft information data (apart from aircraft position data)
Insignificant	Loss of publicly available data

4. CORAS

Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen. Risk analysis of changing and evolving systems using CORAS. Foundations of Security Analysis and Design VI (FOSAD'11), number 6858 in Lecture Notes in Computer Science, pages 231-274, Springer 2011.

Likelihood	Description
Certain	A very high number of similar occurrences already on record; has occurred a very high number of times at the same location/time
Likely	A significant number of similar occurrences already on record; has occurred a significant number of times at the same location
Possible	Several similar occurrences on record; has occurred more than once at the same location
Unlikely	Only very few similar incidents on record when considering a large traffic volume or no records on a small traffic volume
Rare	Has never occurred yet throughout the total lifetime of the system

Ejemplo de escala para las probabilidades

4. CORAS

Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen. Risk analysis of changing and evolving systems using CORAS. Foundations of Security Analysis and Design VI (FOSAD'11), number 6858 in Lecture Notes in Computer Science, pages 231-274, Springer 2011.

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare					
	Unlikely					
	Possible					
	Likely					
	Certain					

4. CORAS

5. Identificación de riesgos mediante diagramas de amenazas: Se avanza en el análisis de los riesgos realizando un proceso de modelado de amenazas (se emplean procesos de brainstorming en grupo). CORAS propone su propia metodología, con sus iconos y diagramas, así como con una clasificación que distingue entre amenazas humanas accidentales o deliberadas y amenazas no humanas.

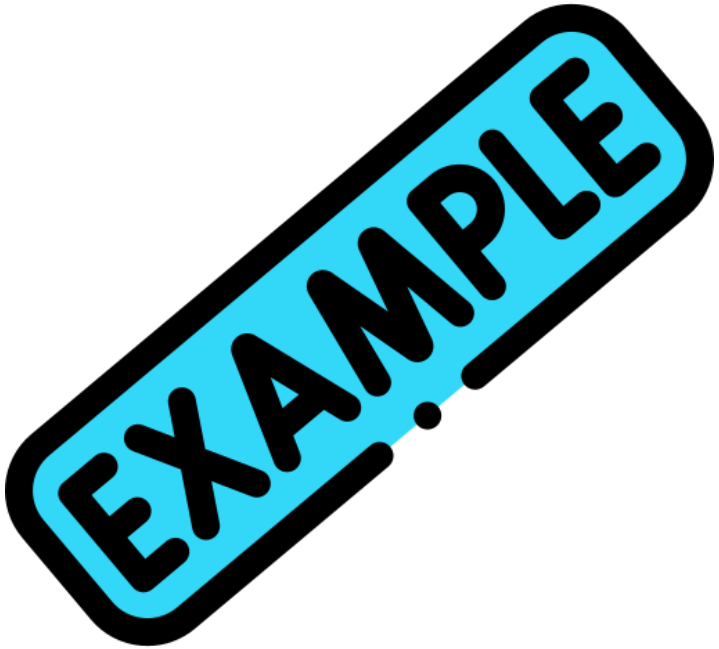
4. CORAS

6. Estimación o valoración del riesgo: Se asignan a los diagramas producidos valores para la probabilidad y el impacto según las decisiones que se hayan tomado en el paso 4. De nuevo se trabaja en equipo y con brainstorming. CORAS recomienda que la probabilidad se asocie a la frecuencia de ocurrencia y que el impacto se asocie al volumen de activos afectado, a su criticidad, etc. (impactos técnicos).

4. CORAS

7. Evaluación del riesgo: Se muestran los resultados de la fase anterior al cliente y se comienza a trabajar en decidir qué es aceptable y qué no lo es. Se genera la matriz de riesgos y se colorean las diferentes zonas en función de las estrategias de gestión que el cliente decide.
8. Gestión o tratamiento del riesgo: Se trabaja específicamente en la gestión del riesgo decidida en la fase anterior. Hay unos diagramas específicos que ayudan a visualizar las acciones y actividades que se planifican para la gestión de cada riesgo.

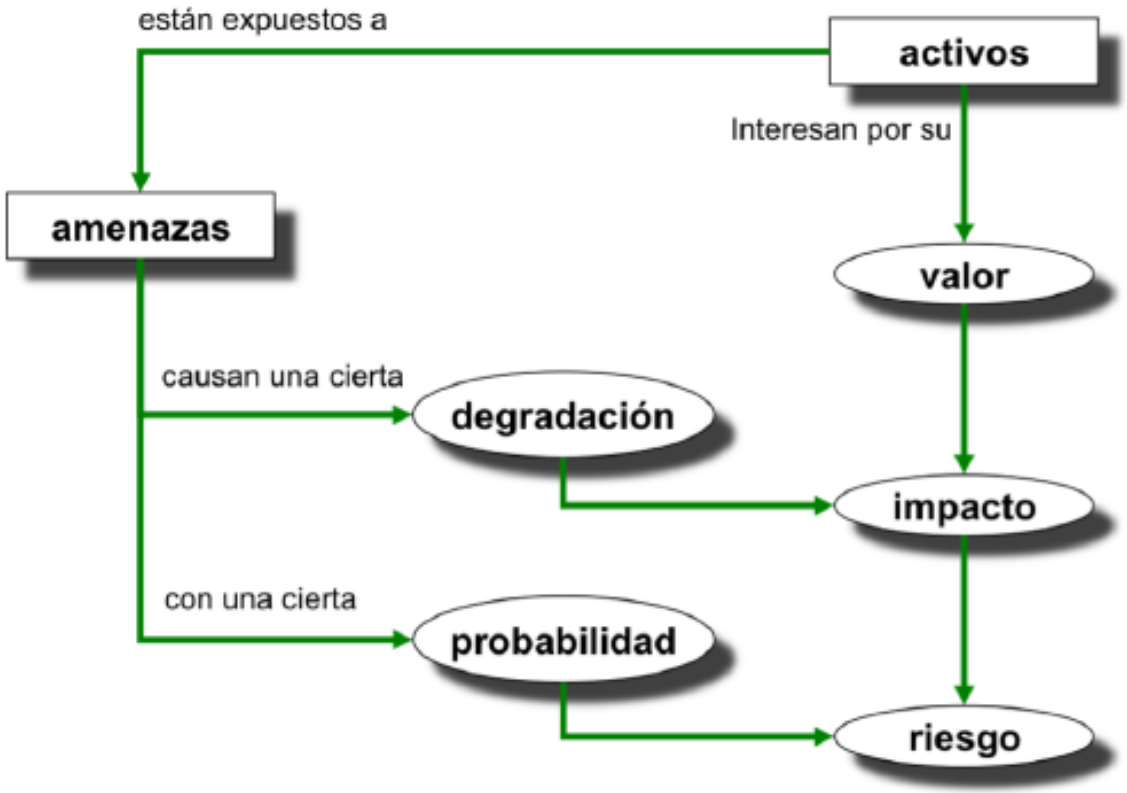
4. CORAS



5. Magerit

- Es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información promovida por el Gobierno de España.
  - Actualmente está en su versión 3 (la primera se publicó en 1997).
  - Está internacionalmente reconocida, detallada en tres libros.
- Es la metodología recomendada por el Esquema Nacional de Seguridad (ENS), la ley NIS o la lay PIC (Protección de infraestructuras críticas), entre otros.
- Tiene el soporte de la herramienta PILAR del CCN-CERT.

5. Magerit



MAGERIT v3 (libro 1)

5. Magerit

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Tabla 1. Degradación del valor

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Tabla 2. Probabilidad de ocurrencia

5. Magerit

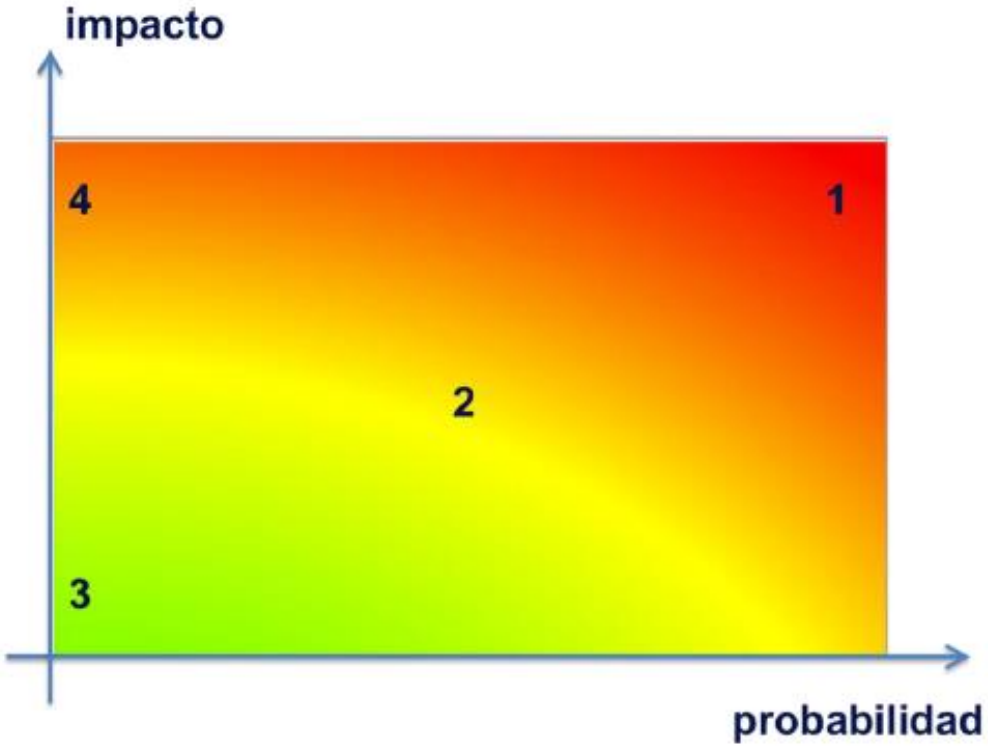
efecto	tipo
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Tabla 3. Tipos de salvaguardas

factor	nivel	significado
0%	**L0**	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	**L5**	optimizado

Tabla 4. Eficacia y madurez de las salvaguardas

5. Magerit



5. Magerit

MAR – Método de Análisis de Riesgos

- MAR.1 – Caracterización de los activos
  - MAR.11 – Identificación de los activos
  - MAR.12 – Dependencias entre activos
  - MAR.13 – Valoración de los activos
- MAR.2 – Caracterización de las amenazas
  - MAR.21 – Identificación de las amenazas
  - MAR.22 – Valoración de las amenazas
- MAR.3 – Caracterización de las salvaguardas
  - MAR.31 – Identificación de las salvaguardas pertinentes
  - MAR.32 – Valoración de las salvaguardas
- MAR.4 – Estimación del estado de riesgo
  - MAR.41 – Estimación del impacto
  - MAR.42 – Estimación del riesgo

MAGERIT v3 (libro 1)

MAGERIT v3 (libro 2): Proporciona un catálogo muy exhaustivo de elementos como activos, amenazas y salvaguardas

Índice

MAGERIT v3 (libro 3): Proporciona una explicación de las técnicas que pueden ser útiles para llevar a cabo el proceso

Índice

PRÁCTICA 1

- Vais a realizar vuestro primer proceso de evaluación del ciberriesgo, empleando para ello métodos cualitativos y los datos de nuestra startup particular.
  - Para ello utilizaréis CORAS.

Para leer e investigar…

1. Libros de la metodología Magerit version 3.
2. Solución PILAR del CCN-CERT: https://pilar.ccn-cert.cni.es/index.php/pilar/que-es-pilar

Referencias

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