Unidad 2: Niveles y enfoques para la gestión del ciberriesgo
BLOQUE I – Introducción al ciberriesgo

Grado en Ingeniería de la Ciberseguridad, curso 2022-2023

CONTENIDOS

1. Riesgo operativo vs riesgo estratégico.
2. Enterprise Risk Management (ERM).
3. Riesgos para la Seguridad Nacional.

1. Riesgo operativo vs riesgo estratégico

- El riesgo operativo se manifiesta de forma accidental, súbita o imprevista durante las operaciones de una organización.
- Por el contrario, el riesgo estratégico se manifiesta de forma continua en el tiempo, muchas veces de manera oculta o imperceptible, por lo que es más difícil de identificar.
- Los riesgos operativos pueden identificarse y analizarse, en mucho casos, de manera aislada o independiente.
- Mientras que los riesgos estratégicos suelen ser simultáneos y dependientes los unos de los otros.

1. Riesgo operativo vs riesgo estratégico

- El ciberriesgo puede darse en los dos niveles, el operativo y el estratégico.
  - Por ejemplo, el operativo puede estar relacionado con la mala configuración de un teléfono móvil personal que se usa para en el contexto profesional mientras que el estratégico puede estar relacionado con una mala definición de la política BYOD o por su inexistencia.

1. Riesgo operativo vs riesgo estratégico

- El ciberriesgo en el plano estratégico suele estar muy relacionado con el riesgo corporativo.

2. Enterprise Risk Management (ERM)

- Esta disciplina surge por la importancia del GRC (Governance, Risk y Compliance) corporativo: gobierno corporativo, gestión de riesgos corporativos y compliance global.
- También por la importancia que cobra en la actualidad la triada Environmental, Social and Governance (ESG).
- Desde la ley Sarbanes-Oxley de Estados Unidos y su versión japonesa, hasta las directivas europeas 4ª, 7ª y 8ª, Solvencia II, Basilea II y la Ley de Seguridad Financiera; existe un amplio marco regulatorio que exige la gestión adecuada del riesgo corporativo.

2. Enterprise Risk Management (ERM)

- Según el Comité de Basilea, se entiende por riesgo corporativo:

> La posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallos en los procesos internos, en la tecnología de información, en las competencias u honestidad de las personas o por la ocurrencia de eventos externos adversos; dichas fallos tienen su fuente, siguiendo el orden como han sido enunciados anteriormente, en los riesgos intrínsecos de los procesos internos, debido al diseño inapropiado de los procesos críticos, o como consecuencia de políticas y procedimientos inadecuados o inexistentes, que puedan generar deficiencias en las operaciones y servicios o la interrupción de los mismos

2. Enterprise Risk Management (ERM)

- El documento COSO ERM (2004) suele ser considerado como modelo conceptual común para el ERM y define la Gestión de Riesgos Corporativos (Enterprise Risk Management, ERM) como:

> "Un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionarlos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre la consecución de objetivos de la entidad"

2. Enterprise Risk Management (ERM)

- Actualmente la gestión de riesgos corporativos persigue :
  - Eficiencia y eficacia de las operaciones.
  - Fiabilidad de los sistemas de información y servicios contratados.
  - Cumplimiento de la ley y de las regulaciones y normativas específicas de cada sector, con especial atención a la protección de las personas (accionistas, clientes) y del medio ambiente.
- Contribuye a reducir la posibilidad de que haya fraudes, conflictos de interés, errores estratégicos y utilización de información privilegiada, por poner sólo algunos ejemplos.

2. Enterprise Risk Management (ERM)

Minimizar amenazas

Maximizar oportunidades

Crear valor

2. Enterprise Risk Management (ERM)

Externos

- Económicos
- Medioambientales
- Políticos
- Legales
- Mercado
- Sociales

Internos

- Procesos
- Personas
- Sistemas

El nivel de análisis y gestión suele ser el estratégico

2. Enterprise Risk Management (ERM)

Externos

- Económicos
- Medioambientales
- Políticos
- Legales
- Mercado
- Sociales

Macroeconomía, política fiscal, desempleo y política laboral

Fuentes de energía y eficiencia energética, calentamiento global

Grupos de presión y lobbies, terrorismo

Contratos, patentes y propiedad intelectual, protección de datos personales

Competencia, barreras de entrada, variabilidad de demanda y precios

Criminalidad, migración, demografía, hábitos de vida

2. Enterprise Risk Management (ERM)

Internos

- Procesos
- Personas
- Sistemas

Contrataciones, onboarding y offboarding, formación

Liquidez, crédito e inversiones, fijación de precios

Seguridad física

Ciberseguridad

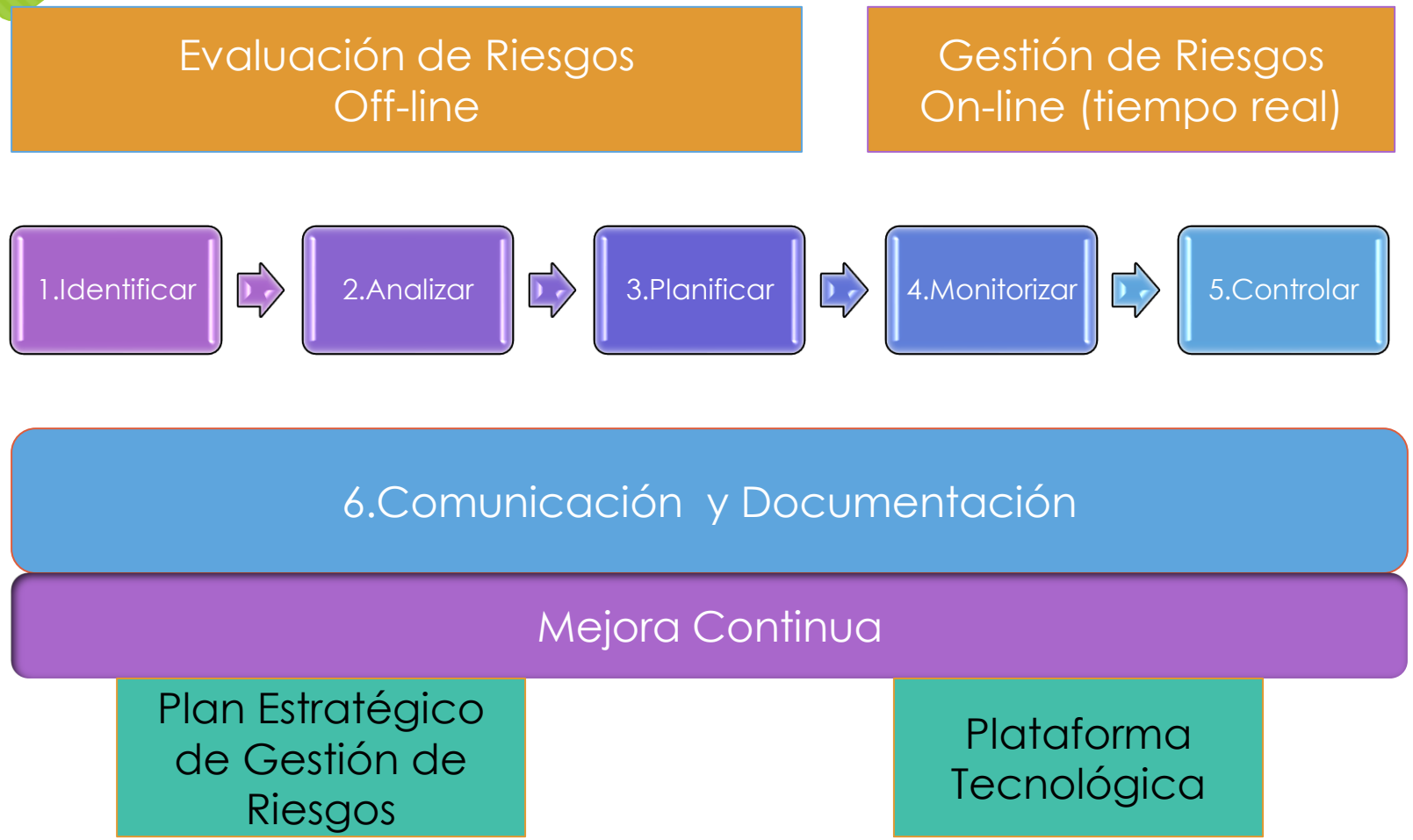
Outsourcing y dependencias de terceros

Obsolescencia tecnológica, gestión de la innovación

2. Enterprise Risk Management (ERM)

Riesgos que necesitan Mitigación	Riesgos que necesitan Investigación	Riesgos que necesitan Monitorización
Planes de actuación correctivos	Planes de actuación preventivos	Planes de actuación detectivos
Evitación o minimización	Transferencia o compartición	Aceptación

2. Enterprise Risk Management (ERM)



2. Enterprise Risk Management (ERM)

Descripción del marco interno	Establecimiento de objetivos	Selección de plataforma tecnológica	Definición de responsabilidades
Inventario de riesgos	Matriz de riesgos	Planes de actuación	Planes de contingencia
Políticas y procedimientos de control	Plan de comunicación	Listado de documentación (entregables)	Mecanismos de supervisión y evaluación del plan
	Calendario de ejecución	Presupuesto	

2. Enterprise Risk Management (ERM)

- **Descripción del marco interno (I)**
  - Es necesario comenzar el plan analizando la empresa y organización.
  - Se pueden emplear las herramientas típicas:
    - Análisis DAFO, plan de negocio, plan de marketing, plan financiero.
  - También sería recomendable un análisis en profundidad de:
    - Recursos.
      - Personas y sistemas.
    - Procesos.
    - Sistemas de gestión del cambio.

2. Enterprise Risk Management (ERM)

- **Descripción del marco interno (II)**
  - A continuación en este primer apartado del plan se debe plasmar la filosofía de gestión de riesgos de la organización.
    - Eso influirá decisivamente en su riesgo aceptado.
      - Volumen de riesgo, a un nivel amplio, que una entidad está dispuesta a aceptar en su búsqueda de valor.
      - Refleja la filosofía de gestión de riesgo de la entidad e impacta a su vez en su cultura y estilo operativo.
  - Factores que deben tenerse en cuenta son la supervisión ejercida por el consejo de administración, la integridad, valores éticos y competencia del personal y la forma en que la dirección asigna la autoridad y responsabilidad y organiza y desarrolla a sus empleados.

2. Enterprise Risk Management (ERM)

- **Establecimiento de objetivos**
  - Cada organización se enfrenta a un conjunto de riesgos procedentes de fuentes externas e internas y una condición previa para su evaluación y solución es fijar los objetivos de la organización, que tienen que estar alineados con el riesgo aceptado por la entidad.

Estratégicos	Operativos	Información	Cumplimiento

2. Enterprise Risk Management (ERM)

- **Selección de la plataforma tecnológica (I)**
  - Casi todos los planes estratégicos de gestión de riesgos se apoyan en una o varias herramientas tecnológicas.
  - Las más habituales son:
    - Bases de datos de riesgos/documentales, herramientas BPM (Bussiness Process Managament), herramientas ZLE (Zero Latency Enterprise).
  - Pero ya existen una gran cantidad de herramientas software de gestión de riesgo disponibles en el mercado.

2. Enterprise Risk Management (ERM)

Selección de la plataforma tecnológica (II)

- Sea cual sea la plataforma escogida, las ventajas de automatizar los procesos de ERM con una herramienta software son:
  - Se "institucionaliza" el Proceso de Gestión de Riesgos.
  - Se asegura que no hay riesgos importantes que se "cuelen" por la organización.
  - Se asigna la propiedad de los riesgos a la persona, área o departamento al que pertenece. Sin ambigüedades.
  - Se comunican los eventos de riesgo en tiempo real.
  - Se pueden tomar las decisiones clave de riesgo más rápido.
  - Se mejora la eficiencia de la recogida, análisis y comunicación de la información de riesgo.
  - Se manejan datos más precisos, consolidados.
  - Se evitan los riesgos de perpetuar los errores provocados por el uso de técnicas "artesanales", hojas de cálculo, etc.

2. Enterprise Risk Management (ERM)

- **Definición de responsabilidades**
  - Por norma general:
    - La Dirección debe garantizar que existe un plan de gestión de riesgos.
      - Responsabilidad distribuida o dirección específica dentro de la organización (CRO).
  - Pero, ¿quién elabora el plan y se encarga de su puesta en marcha, mantenimiento, auditoría y mejora continua?.
    - Comisión de Gestión de Riesgos.
      - Elaboración del plan estratégico.
    - Subcomisión o persona individual encargados de la auditoría interna.
      - Posibilidad /necesidad de realizar auditoría externa.
  - Toda la organización debe estar involucrada en la ejecución del plan.

2. Enterprise Risk Management (ERM)

- **Plan de Comunicación**
  - "Lo que no se comunica, no existe".
    - Y toda la organización debe estar involucrada en la gestión de riesgos.
  - El Plan de Comunicación asociado a la gestión de riesgos tiene que establecer con todo detalle la estrategia de comunicación y la metodología comunicativa que se deben emplear para hacer llegar al personal y a la dirección de la entidad la información que les concierne acerca de la gestión de riesgos.
  - Esto es comunicación interna, pero también puede ser necesaria comunicación externa para convencer a los Grupos de Interés relacionados de la eficacia y/o necesidad de la gestión de riesgos.

2. Enterprise Risk Management (ERM)

- **Mecanismos de supervisión y evaluación del plan**
  - Mediante auditoría interna y/o externa.
  - Algunos aspectos:
    - ¿Se ha cuantificado correctamente el riesgo aceptable de la organización?
    - ¿Cuánto tiempo transcurre desde que se identifica un riesgo hasta que se documenta?
    - ¿Cuánto tiempo tarda la información acerca de un riesgo en llegar a la persona o personas relacionadas con su plan de actuación y/o contingencia?
    - ¿Llega esta información con el suficiente detalle y fidelidad?
    - ¿Son adecuados los planes de actuación y contingencia?
    - ¿Se traducen estos planes en políticas y procedimientos realizables?
    - ¿Se realiza mejora continua del proceso de gestión de riesgos?

2. Enterprise Risk Management (ERM)

- ¿Existe alguna metodología que ayude a realizar todo este proceso?
  - El estándar ISO 31000 puede servir como base.
  - Muchas organizaciones se basan de una manera u otra en el modelo de COSO.
  - COSO (Committee of Sponsoring Organizations of the Tradeway Commission) es una organización compuesta por organismos privados, establecida en los EEUU, cuya misión es proporcionar un modelo común para la gobernanza corporativa, la ética empresarial, el control interno, el control del fraude, la presentación de informes financieros.
  - Y ERM.
  - Actualmente se usa el marco integrado COSO ERM 2017.

2. Enterprise Risk Management (ERM)

https://www.coso.org/Pages/guidance.aspx

2. Enterprise Risk Management (ERM)

COSO ERM 2017: https://www.coso.org/Pages/guidance.aspx

2. Enterprise Risk Management (ERM)

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

COSO ERM 2017: https://www.coso.org/Pages/guidance.aspx

2. Enterprise Risk Management (ERM)

Enfoques complementarios

Six Sigma

Balanced Scorecard

2. Enterprise Risk Management (ERM)

- **Six Sigma**
  - Se trata de una metodología de mejora de procesos basada en la reducción de la variabilidad de los mismos (sigma).
    - La idea es reducir o eliminar los defectos en la entrega de un producto o servicio al cliente.
    - La meta de Six Sigma es llegar a un máximo de 3.4 defectos por millón de eventos u oportunidades (99.999966% de eficiencia), entendiéndose como defecto cualquier evento en que un producto o servicio no logra cumplir los requerimientos del cliente.
  - Six Sigma utiliza para ello herramientas estadísticas para la caracterización y el estudio de los procesos.
  - Se basa en cinco etapas: Definir el problema o el defecto, Medir y recopilar datos, Analizar datos, Mejorar y Controlar.

2. Enterprise Risk Management (ERM)

- Six Sigma y ERM comparten algunos aspectos:
  - Se centran en aportar valor a los clientes, inversores, empleados, etc.
  - Dependen en gran medida de los procesos y sistemas.
  - Tienen que lidiar con las incertidumbres.
- Pero lo hacen dese diferentes perspectivas:
  - Six Sigma, desde la perspectiva de las operaciones y la producción.
  - ERM desde la perspectiva de la gestión del riesgo.
- Además, ERM no suele pararse a valorar si las consecuencias de los riesgos corporativos van minimizándose con el tiempo.

2. Enterprise Risk Management (ERM)

- **Balanced Scorecard**
  - También llamado Cuadro de Mando Integral (CMI), se trata de una herramienta de administración de empresas que muestra en tiempo real el grado de consecución de los resultados definidos por el plan estratégico.
    - También es una herramienta que ayuda a la compañía a expresar los objetivos a diferentes niveles y las iniciativas y planes necesarios para cumplirlos.
  - El CMI sugiere que veamos a la organización desde cuatro perspectivas, cada una de las cuales debe responder a una pregunta determinada:
    - Desarrollo y Aprendizaje (Learning and Growth): ¿Podemos continuar mejorando y creando valor?
    - Interna del Negocio (Internal Business): ¿En qué debemos destacar?
    - Del cliente (Customer): ¿Cómo nos ven los clientes?
    - Financiera (Financial): ¿Cómo nos ven los accionistas e inversores?

2. Enterprise Risk Management (ERM)

- Balanced Scorecard y ERM pueden relacionarse.
  - El CMI ayuda a la compañía a saber en qué situación está y si está cumpliendo o no sus objetivos.
  - Por otro lado, las estrategias ERM permiten determinar los riesgos que afectan negativamente al cumplimiento de los objetivos estratégicos.
    - Y también permiten gestionarlos mediante planes de actuación específicos.
  - Por lo tanto se trata de dos herramientas que se centran en la estrategia de la compañía para cumplir sus objetivos y que deben ser del todo complementarias.
    - Se pueden incluir fácilmente en el CMI, objetivos, planes de actuación y estrategias relacionadas con ERM.
    - O se puede crear un cuadro de mando específico para la gestión de riesgos.

3. Riesgos para la Seguridad Nacional

- Los riesgos para la Seguridad Nacional están relacionados con las amenazas a la libertad, los derechos y bienestar de los ciudadanos de un estado, a sus principios y valores constitucionales o democráticos y en general, a la seguridad internacional y al cumplimiento de los compromisos asumidos con otros estados.

3. Riesgos para la Seguridad Nacional

- La Seguridad Nacional debe ser objeto de una Política de Estado y en cada país se desarrolla con una estrategia diferente.
  - Que se traduce en una estructura institucional y en un marco regulatorio diferente.
- La Política de Seguridad Nacional se encarga de identificar los riesgos y de definir líneas de acción para gestionarlos optimizando los recursos existentes.

3. Riesgos para la Seguridad Nacional

- En el caso de España, el Sistema de Seguridad Nacional es el conjunto de órganos, organismos, recursos y procedimientos que permite a los órganos competentes en materia de Seguridad Nacional ejercer sus funciones.
- La Ley de Seguridad Nacional regula los principios básicos, órganos superiores y autoridades y los componentes fundamentales de la Seguridad Nacional; el Sistema de Seguridad Nacional, su dirección, organización y coordinación; la gestión de crisis y la contribución de recursos a la Seguridad Nacional.

3. Riesgos para la Seguridad Nacional

BOLETÍN OFICIAL DEL ESTADO

Núm. 233 Martes 29 de septiembre de 2015 Sec. I. Pág. 87106

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

10389 *Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.*

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

Índice

PREÁMBULO

I

La seguridad constituye la base sobre la cual una sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos, y garantizar la estabilidad y buen funcionamiento de sus instituciones.

La legislación española así lo reconoce e interpreta, y contiene instrumentos normativos que, partiendo del marco diseñado por la Constitución, regulan los aspectos fundamentales que han venido permitiendo a los poderes públicos cumplir con sus obligaciones en esta materia.

http://www.boe.es/boe/dias/2015/09/29/pdfs/BOE-A-2015-10389.pdf

Sistema de Seguridad Nacional

LEYENDA

- Comités de apoyo existentes
- Comités de apoyo de nueva creación

DSN Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno
Secretaría Técnica y Órgano de Trabajo Permanente del Consejo de Seguridad Nacional

3. Riesgos para la Seguridad Nacional

- El último documento publicado es la Estrategia de Seguridad Nacional 2021.

https://www.dsn.gob.es/sites/dsn/files/ESN2021.pdf

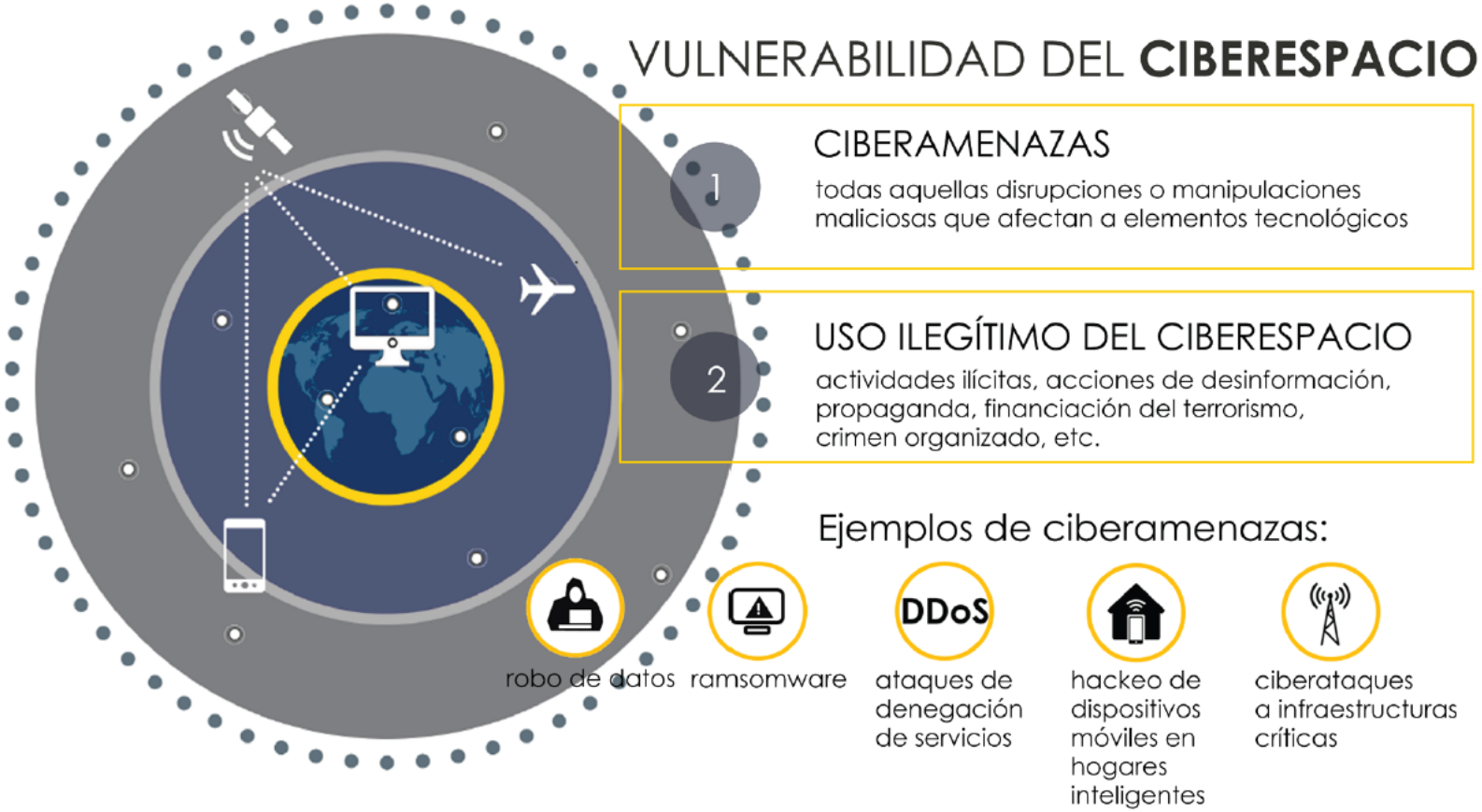
Según este documento que define la Estrategia:


Tensión estrategica y regional
Terrorismo y radicalización violenta
Epidemias y pandemias
Amenazas a las Infraestructuras Críticas
Emergencias y catástrofes
Espionaje e injerencias desde el exterior
Campañas de desinformación
Vulnerabilidad del ciberespacio
Vulnerabilidad del espacio marítimo
Vulnerabilidad aeroespacial
Inestabilidad económica y financiera
Crimen organizado y delincuencia grave
Flujos migratorios irregulares
Vulnerabilidad energética
Proliferación de armas de destrucción masiva
Efectos del cambio climático y de la degradación del medio natural
El tamaño del círculo da indicación del grado de correspondencia de cada riesgo y amenaza con la dimensión tecnológica y con las estrategias híbridas
Riesgos y amenazas interconectados
Predominio del vector tecnológico
Estrategias híbridas

3. Riesgos para la Seguridad Nacional

- En relación con lo que estudiamos en esta asignatura:
  - Se considera el ciberespacio como un espacio común global más.
  - Todas las amenazas (terrorismo, crimen organizado, etc.) pueden materializarse contra activos ciber o empleando medios ciber.
  - Las amenazas contra las infraestructuras críticas son cada vez más ciber.

3. Riesgos para la Seguridad Nacional



3. Riesgos para la Seguridad Nacional

Para leer e investigar…

1. COSO ERM 2017 – "Enterprise Risk Management Integrating with Strategy and Performance" Executive Summary (2017).
2. "COSO in the Cyber Age: Report Offers Guidance on Using Frameworks to Assess Cyber Risks" (2015).
3. "Estrategia de Seguridad Nacional" (2021).

Referencias

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