TLP:CLEAR

IMC_01 - Metodología de evaluación de Indicadores para Mejora de la Ciberresiliencia (IMC)

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Febrero 2023

IMC_01 - Metodología de evaluación versión 1.9

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. OBJETIVO Y ALCANCE DEL DOCUMENTO

1.1. Objetivo

El objetivo de la presente metodología de evaluación de Indicadores para la Mejora de la Ciberresiliencia (IMC) para sistemas de control industrial y sistemas TIC es ayudar a todas las partes interesadas en medir sus capacidades de ciberresiliencia y disponer de una metodología que permita conocer el grado de madurez de sus controles para anticipar, resistir, recuperarse y evolucionar frente a condiciones adversas, estrés o ataques contra los recursos cibernéticos de una organización.

1.2. Alcance

La metodología presentada en este documento está diseñada para evaluar la ciberresiliencia de organizaciones relativa a sus sistemas de control industrial y sistemas TIC.

En este documento se ha adoptado la definición de Sistema de Control Industrial (SCI) de acuerdo a la *International Society of Automation* (*ISA*) que entiende por tal un amplio conjunto de componentes y sistemas, incluyendo entre otros a:

- Sistemas SCADA (*Supervisory Control and Data Acquisition*). Utilizados en casos de amplia dispersión geográfica, cuando se necesitan supervisión y control centralizados.
- Sistemas de Control Distribuidos (*DCS – Distributed Control Systems*). Se trata de una arquitectura compuesta de subsistemas encargada de controlar procesos localizados.
- Controladores Lógicos Programables (PLC – *Programmable Logic Controllers*). Dispositivos informáticos equipados con memoria no volátil utilizados para controlar equipamientos y procesos.
- Sistemas de Seguridad Instrumentados (SIS – *Safety Instrumented Systems*). Controles *hardware* y *software* utilizados en procesos peligrosos para prevenir o mitigar consecuencias negativas.

El presente modelo está destinado a su uso en forma de consulta que puede lanzarse entre las organizaciones de cualquier sector esencial, y como herramienta de autoevaluación de las capacidades de ciberresiliencia para dichas organizaciones.

1.3. Partes interesadas

Las partes interesadas en la ciberresiliencia de una organización pueden ser cualquier individuo, grupo u organización que forme parte o se vea afectado por la misma, obteniendo algún beneficio o perjuicio, y cada una de ellas tiene sus propios intereses. El modelo que se presenta persigue dar respuesta a las diferentes necesidades de cada una de ellas conforme se recoge a continuación, considerando tanto las partes interesadas internas como externas más relevantes (Tabla 1).

Partes interesadas	Necesidad	Función del modelo
Internas		
Órganos de gobierno y gestión	Conocer el nivel de ciberresiliencia de los SCI	Mejora continua ciberresiliencia
Área de Operaciones	Mejorar el nivel de ciberresiliencia en los SCI	Mejora continua ciberresiliencia
Responsables de riesgos / Seguridad	Disponer de un modelo para medir el nivel de ciberresiliencia de los SCI	Mejora continua ciberresiliencia
Externas		
Accionistas	Conocer el nivel de ciberresiliencia de los SCI	Información sobre de ciberresiliencia
Socios / *partners*	Mejorar la continuidad del negocio a través de la ciberresiliencia de los socios o *partners*.	Información sobre las capacidades de ciberresiliencia de los socios o *partners*.

Tabla 1: Necesidades de las partes interesadas y utilidad del modelo

2. MODELO DE EVALUACION DE INDICADORES PARA MEJORA DE LA CIBERRESILENCIA (IMC)

2.1. Definición de ciberresilencia

Ciberresiliencia es la capacidad de un proceso, negocio, organización o nación de anticipar, resistir, recuperarse y evolucionar para mejorar sus capacidades frente a condiciones adversas, estrés o ataques a los recursos cibernéticos que necesita para funcionar.

2.2. Marco conceptual

Para la construcción del modelo de evaluación de IMC, se propone un marco conceptual en el que estructurar las métricas e indicadores para poder medir el estado de ciberresiliencia de una organización o de un sector. El objetivo es proporcionar una visión del estado de ciberresiliencia evaluado, lo más completa posible, basada en dichas métricas.

Este marco conceptual está basado principalmente en el esquema de referencia de indicadores de ciberresiliencia planteado por el MITRE [1] y adoptado por INCIBE-CERT en su iniciativa para la construcción de un marco integral de indicadores [2], conforme con la Estrategia de Ciberseguridad Nacional [3-4] del Gobierno de España.

Siguiendo un modelo *GQM* (*Goal-Question-Metric*) se define un conjunto de metas de alto nivel, posteriormente se establecen una serie de objetivos tanto generales como específicos, y por último se definen las preguntas necesarias para contestar o conseguir dichos objetivos. Esta aproximación permite partir del nivel más alto (estratégico) e ir desarrollando nuevas métricas a partir de estas, sin perder de vista los objetivos operativos de las organizaciones para el mantenimiento de sus servicios esenciales.

Se establecen de esta forma tres niveles conceptuales:

En un **primer nivel** se encuentra el concepto de gobernanza, asociada al cumplimiento de metas de alto nivel. En él podemos encontrar metas que establecerán las bases del resto de niveles.

- ***Objetivos generales o metas:*** declaraciones específicas de los resultados previstos, expresados con el fin de facilitar la evaluación.

El **segundo nivel** está formado por una serie de grupos o dominios funcionales, cada uno de los cuales está asociado al cumplimiento de un objetivo general de ciberresiliencia.

- ***Dominios funcionales:*** áreas en las que se pueden agrupar los principales aspectos de ciberresiliencia de la organización, que contienen el conjunto de prácticas que la organización debe implantar para asegurar la protección y el mantenimiento de los servicios esenciales.

El **nivel más bajo** y «tangible» del marco está formado por las métricas de ciberresiliencia, cada una de las cuales está asociada a la medición de un objetivo específico más concreto:

- ***Objetivos específicos****:* formas de lograr uno o más objetivos generales de ciberresiliencia, que se aplican a la arquitectura o al diseño de las funciones de negocio y a los recursos que los apoyan.

- ***Métrica de ciberresiliencia**:* variable a la que se le asigna un valor como resultado de la medición de un aspecto de la ciberresiliencia de la organización.

Asociados a estos tres niveles, se pueden definir indicadores de ciberresiliencia.

- ***Indicadores de ciberresiliencia**:* muestran el estado actual y el progreso a lo largo del tiempo de las metas, para facilitar la toma de decisiones.

2.3. Modelos de evaluación de IMC

A partir del marco conceptual, se ha diseñado un modelo de evaluación del nivel de ciberresiliencia de servicios esenciales. Dicho marco conceptual está formado por los siguientes elementos:

- Cuatro metas:
  - **Anticipar (A):** mantener un estado de preparación informado, con el fin de evitar que se vean comprometidos los servicios esenciales por los ciberataques.
  - **Resistir (T):** continuar con los servicios esenciales a pesar de la ejecución con éxito del ciberataque.
  - **Recuperar (R):** restaurar servicios esenciales en la mayor medida posible con posterioridad a la ejecución con éxito de un ciberataque.
  - **Evolucionar (E):** cambiar las funciones y las capacidades con el fin de rediseñar las estrategias, a fin de minimizar los impactos negativos de los ciberataques reales o previstos.
- Nueve dominios funcionales agrupados por meta:
  - **Política de ciberseguridad (PC):** disponer de una política que establezca los requisitos de ciberresiliencia, contemple los riesgos de ciberseguridad, asigne responsabilidades y sea comunicada a toda la organización.
  - **Gestión de riesgos (GR)**: identificar, analizar y mitigar los riesgos sobre los activos de la organización, que podrían afectar negativamente el funcionamiento y la prestación de servicios.
  - **Formación en ciberseguridad (FO)**: promover el conocimiento y el desarrollo de habilidades de las personas en apoyo de sus funciones, para la consecución y el mantenimiento de la ciberresiliencia operacional y la protección.
  - **Gestión de vulnerabilidades (GV)**: identificar, analizar y gestionar vulnerabilidades en los activos que apoyan la prestación de los servicios esenciales.
  - **Supervisión continua (SC)**: recoger, recopilar y distribuir información sobre el comportamiento y las actividades de los sistemas y las personas, para apoyar el proceso continuo de identificación y análisis de los riesgos de los activos de la organización y de los servicios esenciales que puedan afectar negativamente al funcionamiento y prestación de estos.

- **Gestión de incidentes (GI)**: establecer procesos para identificar y analizar los acontecimientos, detectar incidentes, y determinar y aplicar una adecuada respuesta organizativa.
- **Gestión de continuidad del servicio (CS)**: establecer cómo la organización lleva a cabo la planificación de actividades para garantizar la continuidad de los servicios esenciales en caso de incidente o desastre.
- **Gestión de la configuración y de los cambios (CC)**: establecer procesos para mantener la integridad de todos los activos (tecnología, información e instalaciones) necesarios para proporcionar los servicios esenciales.
- **Comunicación (CM)**: establecer procesos que garanticen la comunicación entre responsables involucrados en la operación de los servicios esenciales, tanto internos como externos a la organización.

La agrupación de los dominios dentro de las metas se puede ver en la siguiente figura:

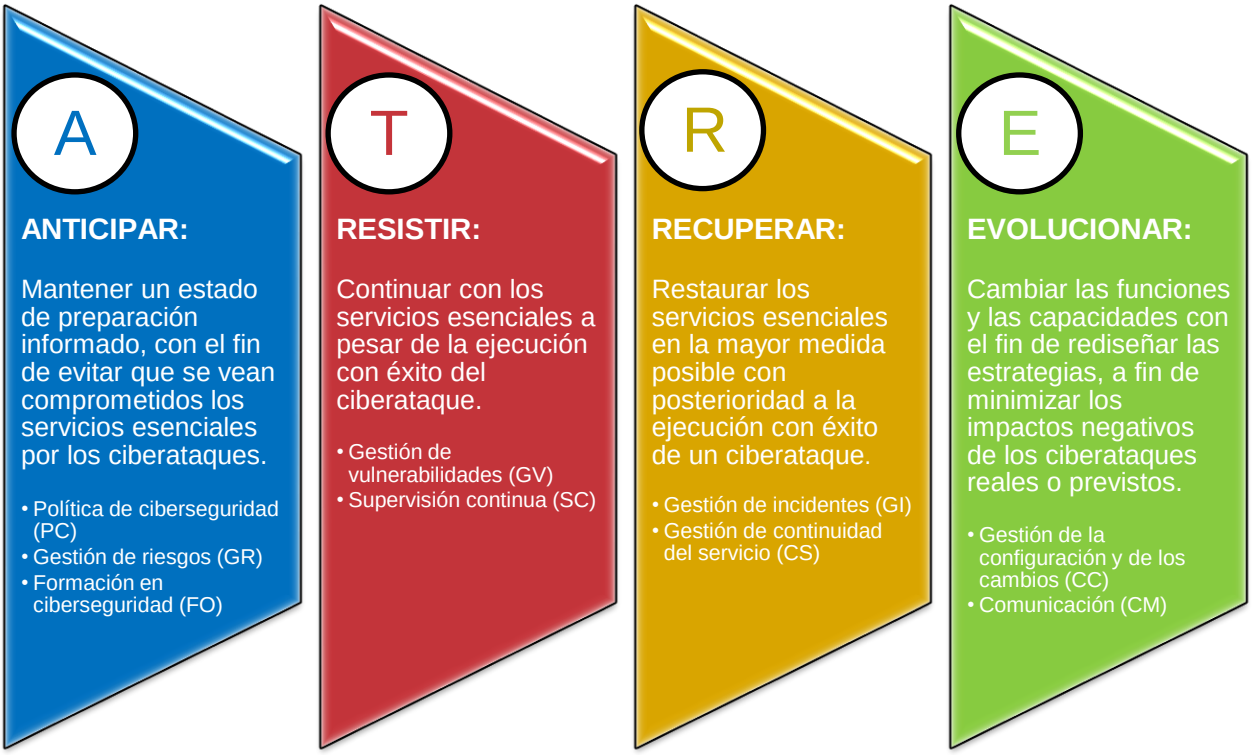

Figura 1: Marco de trabajo de ciberresiliencia

Para alimentar este marco de trabajo, se han definido:

- Un conjunto de métricas de ciberresiliencia agrupadas por dominio funcional.
- Un conjunto de indicadores de ciberresiliencia, basados principalmente en indicadores clave de rendimiento o *KPI* y en la posible definición de indicadores clave de riesgo o *KRI*.
- Este modelo de metas, dominios, métricas e indicadores que se utilizarán para la evaluación de la ciberresiliencia conforman el Modelo de evaluación del IMC.

2.4. Documentos de modelo

El Modelo de evaluación de Indicadores para la Mejora de la Ciberresiliencia está compuesto por los siguientes documentos:

Documentación del Modelo IMC	
IMC_01 - Metodología de evaluación de Indicadores para la Mejora de la Ciberresiliencia	Este documento contiene el marco conceptual y la metodología para la realización de la evaluación de los Indicadores para la Mejora de la Ciberresiliencia.
IMC_02 - Diccionario de Indicadores para la Mejora de la Ciberresiliencia	Compendio de cada una de las métricas utilizadas en la evaluación de los Indicadores para la Mejora de la Ciberresiliencia.
IMC_03 – Formulario para la medición de la Ciberresiliencia	Plantilla para la evaluación de Indicadores para la Mejora de la Ciberresiliencia.

Tabla 2: Kit documental del Modelo de evaluación de IMC

2.5. Metodología de evaluación de IMC

La metodología de evaluación de Indicadores para la Mejora de la Ciberresiliencia que debe aplicar cada empresa u organización participante en alguna consulta se desarrolla en las siguientes etapas:

- Delimitar el alcance del análisis.
- Realizar una autoevaluación.
- Aplicar una serie de medidas correctivas dentro del alcance.
- Repetir la autoevaluación para analizar la efectividad de las medidas.

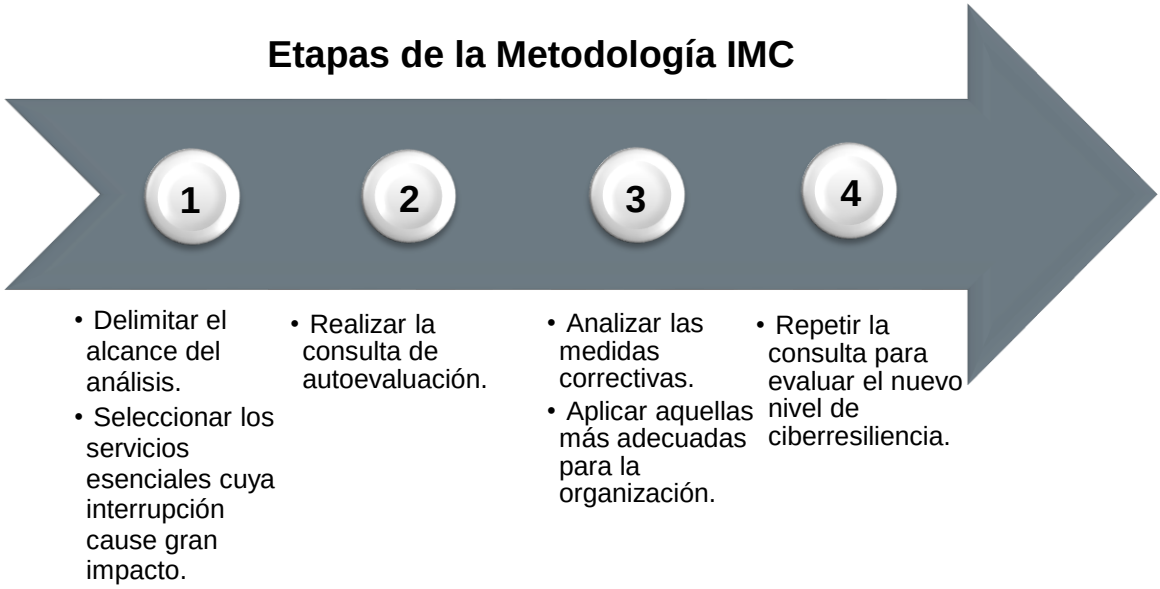

Figura 2: Enfoque general de la Metodología de evaluación de IMC

Queda fuera del ámbito de esta Metodología la aplicación de las medidas correctivas que deberá ser realizada por la organización objeto del estudio.

3. APLICACION DE METODOLOGIA DEL MODELO

Al objeto de facilitar la ejecución de la aplicación del Modelo, se describen a continuación las etapas propuestas:

3.1. Etapa 1: Delimitación del alcance

El primer paso para la aplicación del Modelo de evaluación de Indicadores para la Mejora de la Ciberresiliencia consiste en determinar el servicio esencial que se desea evaluar. Dentro de este contexto, se define el alcance en relación a la provisión concreta de un **servicio esencial cuya interrupción presumiblemente ocasione un gran impacto** en la organización (o en la sociedad española en caso de tratarse de infraestructuras que soportan servicios esenciales). Por tanto, cada organización que desee someterse a una autoevaluación basada en este modelo debe determinar cuál será el alcance.

Como indicación general, se debe rellenar el formulario en relación a la provisión concreta de, al menos, un servicio esencial cuya interrupción presumiblemente ocasione un gran impacto. La consulta se podrá responder para más de un servicio esencial, obteniéndose de esa forma un valor de ciberresiliencia para cada uno de los servicios considerados esenciales.

Realizar un análisis amplio que incluya varios servicios permitirá a los interesados localizar sinergias que permitan de una forma global la mejora de la ciberresiliencia de la organización.

3.2. Etapa 2: Realización de la consulta de autoevaluación

Una vez identificado el servicio esencial objeto del análisis, se cumplimentará el formulario de autoevaluación, valorando las métricas seleccionadas en función de su grado de desarrollo.

El formulario presenta un apartado para cada meta: Anticipar, Resistir, Recuperar y Evolucionar. Para cada una de ellas la empresa debe realizar la medición de las diferentes métricas. Cada una de estas métricas puede estar implementada en la empresa con un nivel de madurez que se ha de indicar en el formulario. El nivel de madurez está adaptado a cada una de las métricas, siendo el correspondiente a una de ellas el que se muestra en el ejemplo de la Figura 3:

L0 - No se han establecido requisitos de ciberresiliencia.
L1 - Se ha iniciado la identificación de requisitos de ciberresiliencia.
L2 - Se han establecido requisitos de ciberresiliencia, pero no se han documentado.
L3 - Se han documentado los requisitos de ciberresiliencia y se mantienen actualizados.
L4 - Se gestionan, actualizan y verifican los requisitos de ciberresiliencia.
L5 - Se aplican acciones de mejora en la definición de requisitos de ciberresiliencia.

Figura 3: Niveles de madurez consulta IMC

Una vez seleccionado el nivel de madurez correspondiente a cada una de las métricas, se podrá calcular, asignando un valor a cada nivel y agregando los resultados de todas las métricas de cada meta, el resultado obtenido para cada una de ellas. El ejemplo (Figura 4) muestra cómo se podrían representar estos resultados en forma de diagrama de barras.

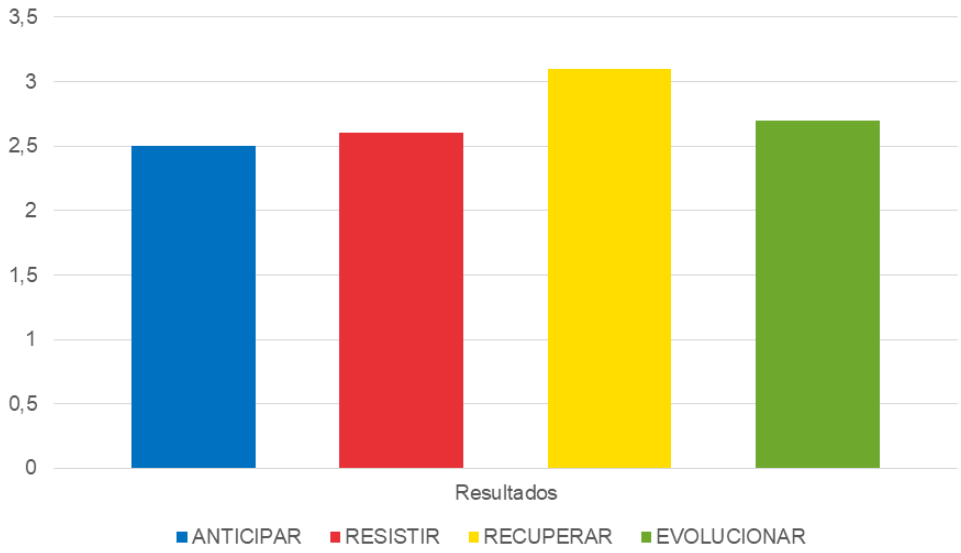

Figura 4: Ejemplo de resultado de la consulta de IMC

Opcionalmente, para el resto de los servicios esenciales identificados en el punto anterior se puede rellenar otro formulario, de esta forma se obtendrá el valor de ciberresiliencia de cada servicio esencial identificado cuyo deterioro o fallo pueda causar un gran impacto.

3.3. Etapa 3: Aplicación de medidas correctivas

Una vez realizada la consulta de autoevaluación, aplicaremos las medidas correctivas. En el documento del modelo IMC_02- Diccionario de Indicadores para la Mejora de la Ciberresiliencia se pueden consultar acciones correctivas para las métricas cuya evaluación no haya sido lo suficientemente satisfactoria, como se puede ver en el siguiente ejemplo, correspondiente a una de las métricas de la meta Resistir:

ANÁLISIS		
Medida Objetivo	L5	
Indicador	**Valores positivos**	Valores tendentes a L5 indican que la organización mantiene un repositorio actualizado de todas las vulnerabilidades conocidas, almacenando información de las mismas y su resolución.
	Acciones correctivas	Establecer un repositorio de vulnerabilidades con información del ciclo de vida de las mismas. Dicho repositorio debe contener información básica como: • Identificador único para referencia interna de la vulnerabilidad en la organización. • Descripción de la vulnerabilidad. • Fecha de ingreso en el repositorio. • Referencias a la fuente de la vulnerabilidad. • Importancia de la vulnerabilidad para la organización (crítica, moderada, etc.). • Personas o equipos asignados para analizarla y solucionarla. • Registro de las acciones de resolución tomadas para disminuir o eliminar la vulnerabilidad.

Figura 5: Ejemplo de acciones correctivas

El estudio de la idoneidad de la aplicación de las medidas correctivas propuestas u otras más adecuadas para la organización que participe en una consulta, así como el propio proceso de implantación de las mismas, quedan fuera del alcance de este modelo.

3.4. Etapa 4: Repetir la consulta periódicamente

La evaluación de la ciberresiliencia es un proceso que permite a los interesados conocer la capacidad de anticipar, resistir, recuperarse y evolucionar frente a incidentes de origen cibernético. Es importante realizar este análisis de forma periódica para valorar la eficacia de las medidas y así intentar mejorar aquellos aspectos que sea posible, incrementando de esa forma la ciberresiliencia de aquellos servicios considerados esenciales.

4. ACRÓNIMOS

- INCIBE-CERT: Centro de Respuesta a Incidentes de Seguridad de referencia para ciudadanos y entidades de derecho privado en España, operado por INCIBE.
- CNPIC: Centro Nacional de Protección de Infraestructuras Críticas.
- *GQM*: *Goal-Question-Metric*.
- IMC: Indicadores para la Mejora de la Ciberresiliencia.
- INCIBE: Instituto Nacional de Ciberseguridad.
- *KPI*: *Key Performance Indicator*.
- *KRI*: *Key Risk Indicator*.
- *ISA: International Society for Automation*.
- SCI: Sistemas de Control Industrial.
- TIC: Tecnologías de la información y comunicación.

5. REFERENCIAS

Referencia	Título, autor y enlace web
[Ref.- 1]	MITRE (2018), Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring. https://www.mitre.org/news-insights/publication/cyber-resiliency-metrics-measures-effectiveness-and-scoring
[Ref.- 2]	INCIBE_CERT (2014), CIBER-RESILIENCIA: Aproximación a un marco de medición. https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/int_ciber_resiliencia_marco_medicion.pdf
[Ref.- 3]	España (2019), ESTRATEGIA NACIONAL DE CIBERSEGURIDAD. https://www.boe.es/buscar/act.php?id=BOE-A-2019-6347
[Ref.- 4]	España (2021), ESTRATEGIA DE SEGURIDAD NACIONAL. https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021
[Ref.- 5]	NIST (2022). SP 800-53A, Assesing Security and Privacy Controls in Information Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

Otros documentos de interés	Título, autor y enlace web
[Doc.- 1]	MITRE (2023). MITRE Launches Cyber Resiliency Engineering Framework Navigator. https://www.mitre.org/news-insights/news-release/mitre-launches-cyber-resiliency-engineering-framework-navigator
[Doc.- 2]	MITRE. (s.f). Navigator. https://crefnavigator.mitre.org/navigator
[Doc.- 3]	NIST (2021). SP 800-160 Vol. 2 Rev. 1. Developing Cyber-Resilient System: A System Security Engineering Approach. https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final