GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

Esquema Nacional de Seguridad Industrial

ENSI_IMC_01- Metodología de evaluación de Indicadores para Mejora de la Ciberresiliencia (IMC)

certsi_

CERT DE SEGURIDAD E INDUSTRIA

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

NOVIEMBRE 2016

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 para sistemas de control industrial, es ayudar a todas las partes interesadas en 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 especialmente diseñada para los sistemas de control industrial.

En este documento se ha adoptado la definición de Sistema de Control Industrial de acuerdo a la *International Society of Automation* (ISA) que entiendes por tales un amplio conjunto de componentes y sistemas que incluye, aunque no está limitado a:

- Sistemas SCADA (*Supervisory Control And Data Acquistion*). 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 todas las empresas del sector industrial como una herramienta que les permita analizar sus capacidades.

1.3. Partes interesadas

Las partes interesadas de una organización son 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, con sus propios intereses. El modelo que se presenta en el documento 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. ACERCA DEL ENSI

La promulgación de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas (Ley PIC), puso de manifiesto la importancia de la seguridad de las Infraestructuras Críticas dentro de la Seguridad del Estado. Por su parte, la Estrategia de Seguridad Nacional [1] de 2013 reconoce, por primera vez, las ciberamenazas como uno de los riesgos y amenazas a la seguridad nacional. Complementando la anterior, la Estrategia de Ciberseguridad Nacional [2] de 2013 completa la apuesta por la protección de los sistemas de control industrial como elemento clave en un enfoque integral de la ciberseguridad

En este contexto, el Instituto Nacional de Ciberseguridad (INCIBE), del Ministerio de Energía, Turismo y Agenda Digital, y el Centro Nacional de Infraestructuras Críticas del Ministerio del Interior, de la mano del acuerdo suscrito en 2012 y renovado en 2015 entre la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD) y la Secretaría de Estado de la Seguridad (SES), promueven el Esquema Nacional de Seguridad Industrial (ENSI), como instrumento para mejorar la seguridad de las infraestructuras críticas industriales y con una vocación global en tanto que es aplicable en sistemas de control industrial de cualquier organización.

Para ello, favorecer el tratamiento homogéneo de la seguridad y extender su aplicación a toda la cadena de valor de las organizaciones industriales, reconociendo el papel de proveedores y clientes, son las claves para dibujar el panorama completo al que responde el ENSI, que podría conformar la base para nuevas iniciativas que permitieran al ENSI ampliarse e incluir la seguridad desde un punto de vista más integral.

El ENSI se concreta en cuatro elementos esenciales que se configuran para atender a las necesidades específicas de su ámbito de aplicación:

- ARLI-SI: Metodología de Análisis de Riesgos Ligero de Seguridad Integral como punto de partida y piedra angular del proceso de mejora de la seguridad. Con entidad propia, dentro de esta metodología, ARLI-CIB permite un acercamiento específico, y también ligero, al Análisis de Riesgos de Ciberseguridad en sistemas de control industrial.
- IMC: Indicadores para la Mejora de Ciberresiliencia, como instrumento de diagnóstico y medición de la capacidad para soportar y sobreponerse a desastres y perturbaciones procedentes del ámbito digital.
- C4V: Modelo de Construcción de Capacidades en Ciberseguridad de la Cadena de Valor como elemento imperante en la operativa y actividad de la prestación de servicio del operador: proveedores y clientes.
- SA: Sistema de Acreditación en Ciberseguridad, garantía de la aplicación de unas medidas de seguridad mínimas equivalentes en todas las arquitecturas que prestan servicios equiparables o semejantes.

La aproximación práctica y ligera predomina en todos los elementos del ENSI y dibuja un marco completo para la mejora de la ciberseguridad en sistemas de control industrial.

Aquí, las diferentes guías y documentos de articulación, siempre alineados con todo lo establecido para los Planes de Seguridad del Operador, Planes de Protección Específicos y Planes Estratégicos Sectoriales, aportarán las instrucciones, criterios y herramientas para facilitar su aplicación por parte de los diferentes agentes.

3. MODELO DE INDICADORES PARA MEJORA DE LA CIBERRESILIENCIA

3.1. Definición de ciberresiliencia

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

3.2. Marco Conceptual

Para la construcción del Modelo, se propone un marco de trabajo en el que estructurar las métricas e indicadores de ciberresiliencia que serán definidas posteriormente para poder medir el estado de ciberresiliencia con el objetivo de proporcionar una visión lo más completa posible de la ciberresiliencia basada en dichas métricas.

Este marco de trabajo está basado principalmente en el marco de indicadores de ciberresiliencia planteado por el MITRE [3] y adoptado por CERTSI en su iniciativa para la construcción de un marco integral de indicadores [4].

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

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 el podemos encontrar metas y gobernanza que establecerán las bases del resto de niveles.

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:

- **Objetivos generales**: Declaraciones más específicas de los resultados previstos, expresados con el fin de facilitar la evaluación.
- **Dominios funcionales**: Áreas en las que se puede 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 las funciones críticas.

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 el diseño de las funciones de negocio y a los recursos que los apoyan.
- **Métricas 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**: Representación estadística de los datos de una característica de ciberresiliencia relevante, con el fin de permitir comparaciones significativas. Representa el grado de satisfacción de las métricas de ciberresiliencia, por lo que se puede representar gráficamente con el fin de permitir comparaciones significativas (por ejemplo, representación estadística de los datos de un objetivo específico de ciberresiliencia).

A partir de este esquema conceptual, se ha diseñado un marco de trabajo formado por los siguientes elementos:

- Cuatro metas:
    - **Anticipar (A):** Mantener un estado de preparación informado, con el fin de evitar compromisos de funciones misión / empresa de los ciberataques.
    - **Resistir (T):** Continuar las funciones misión/empresariales esenciales a pesar de la ejecución con éxito de ciberataque.
    - **Recuperar (R):** Restaurar las funciones misión / negocio en la mayor medida posible con posterioridad a la ejecución con éxito de un ciberataque.
    - **Evolucionar (E):** Cambiar misiones funciones / de negocios y / o las capacidades cibernéticas de apoyo, a fin de minimizar los impactos negativos de los ciberataques reales o previstos.
- Catorce dominios funcionales agrupados por meta:
    - **Política de ciberseguridad:** Disponer de una política de ciberseguridad que establezca los requisitos de ciberresiliencia, contemple los riesgos de ciberseguridad, asigne responsabilidades y sea comunicada a toda la organización.
    - **Gestión de Activos:** Identificar, documentar y administrar los activos de la organización durante su ciclo de vida, para asegurar el mantenimiento de la productividad para soportar las funciones críticas.
    - **Gestión de Riesgos**: 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**: Promover el conocimiento y el desarrollo de habilidades y conocimientos de las personas en apoyo de sus funciones en la consecución y el mantenimiento de la ciberresiliencia operacional y la protección.
    - **Conocimiento de la Situación**: Descubrir y analizar activamente la información relacionada con posibles nuevas amenazas, así como con la estabilidad y seguridad operacional inmediata, y coordinar dicha información a través de toda la empresa para asegurarse de que todas las unidades organizativas están actuando bajo un cuadro de operaciones común.

- **Gestión de Controles**: Establecer, controlar, analizar y gestionar un sistema de control interno que asegure la eficacia y la eficiencia de las operaciones garantizando el éxito de la misión de los servicios críticos y los activos que los soportan.
- **Gestión de Vulnerabilidades**: Identificar, analizar y gestionar vulnerabilidades en los activos que apoyan la prestación del servicio esencial.
- **Monitorización Continua**: 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 riesgos de los activos de la organización y las funciones críticas que puedan afectar negativamente al funcionamiento y prestación de los mismos.
- **Gestión de Incidentes**: Establecer procesos para identificar y analizar los acontecimientos, detectar incidentes, y determinar y aplicar una adecuada respuesta organizativa.
- **Gestión de Continuidad del servicio**: Cómo la organización lleva a cabo la planificación de contingencias para garantizar la continuidad de las funciones críticas.
- **Gestión de Dependencias externas**: Establecer y gestionar un nivel adecuado de controles para asegurar la capacidad de recuperación de los servicios y bienes que dependen de las acciones de las entidades externas.
- **Gestión de la Configuración y el cambio**: Establecer procesos para mantener la integridad de todos los activos (tecnología, información, e instalaciones) necesarios para proporcionar las funciones críticas.
- **Mejora Continua**: Establecer procesos que garanticen la mejora continua de los procesos que dan soporte a las funciones críticas.
- **Comunicación**: 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 Figura 1

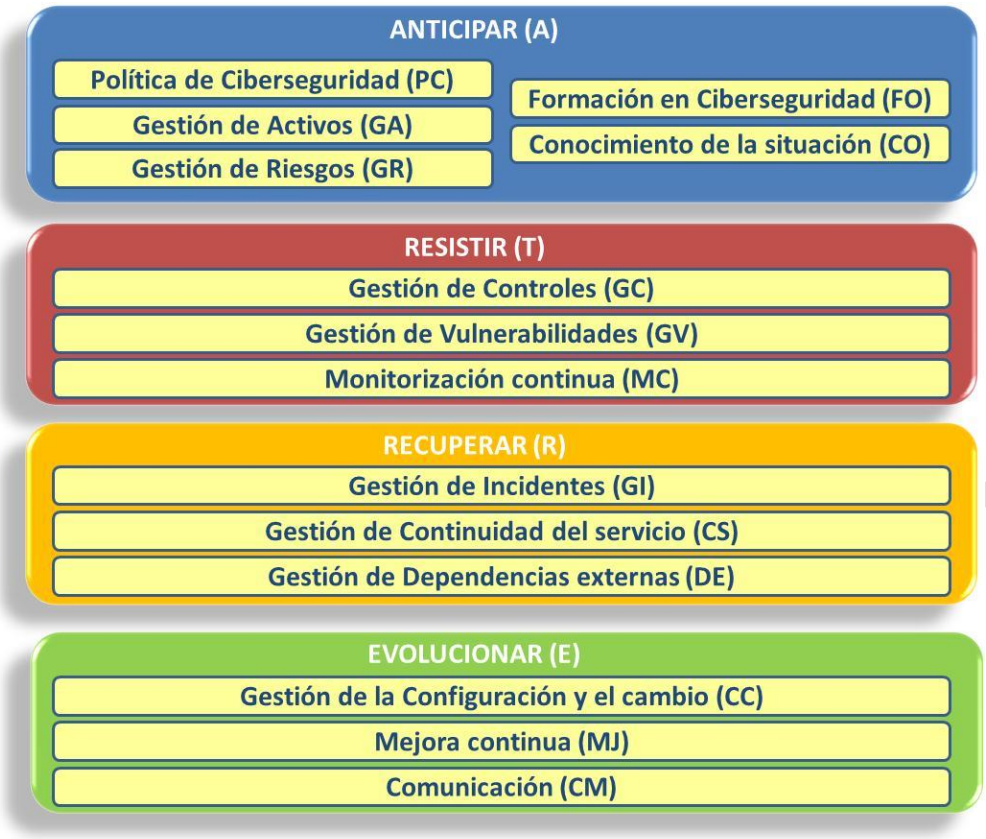

Figura 1. Marco de trabajo de ciberresiliencia

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 claves de rendimiento (KPI), y en la posible definición de KRI o KGI.

A partir de este modelo de fichas, se ha diseñado y seleccionado el conjunto de métricas e indicadores que se utilizarán para la evaluación de la ciberresiliencia. Estas métricas se pueden encontrar en la guía ENSI_IMC_02- Diccionario de indicadores para la Mejora de la Ciberresiliencia.

3.3. Componentes del Modelo

El Modelo de Indicadores de Ciberresiliencia está compuesto por los siguientes documentos

Documentación del Modelo IMC	
ENSI_IMC_01- Metodología de evaluación de Indicadores para la Mejora de la Ciberresiliencia	Documento que contiene el marco conceptual y la metodología para la realización de la evaluación de los Indicadores para la Mejora de la Ciberresiliencia.

ENSI_IMC_02- Diccionario de indicadores para la Mejora de la Ciberresiliencia	Documento compendio de cada una de las métricas utilizadas en la evaluación de los Indicadores para la Mejora de la Ciberresiliencia.

Tabla 2: Kit documental del Modelo de Evaluación de IMC.

3.4. Descripción de la Metodología de Análisis

El enfoque propuesto por el Modelo de Indicadores para la Mejora de la Ciberresiliencia desarrollado en esta guía pasa por los siguientes pasos:

- Delimitar el alcance del análisis
- Realizar una consulta de autoevaluación
- Aplicar una serie de medidas correctivas a aplicar dentro del alcance

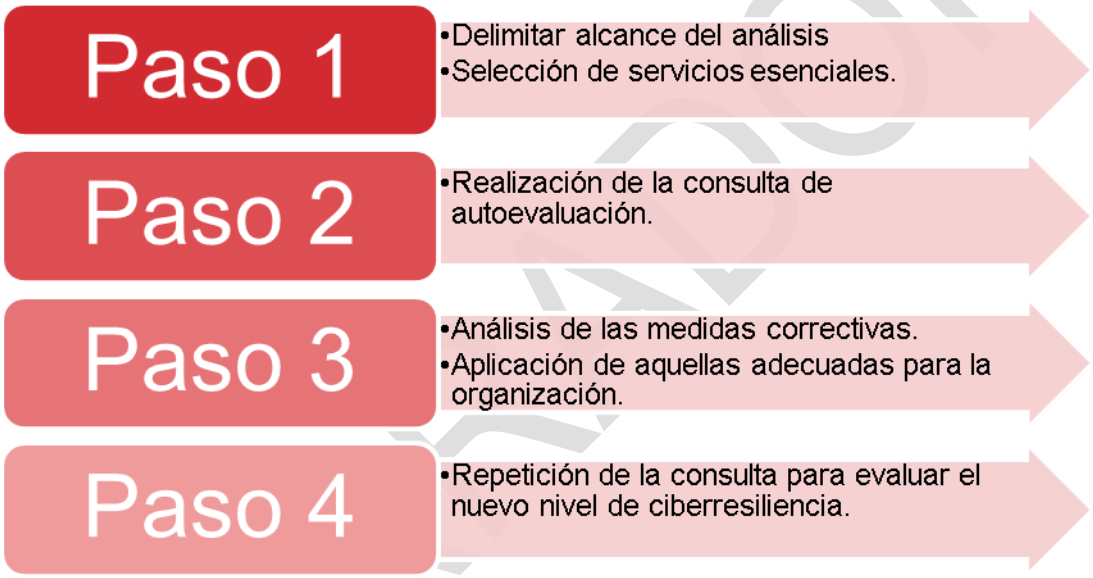

Figura 2: Enfoque general del Modelo de Evaluación de IMC.

Queda, por tanto, fuera del ámbito de este modelo, la aplicación de las medidas correctivas que deberá ser realizada por la organización objeto del estudio.

4. APLICACIÓN METODOLÓGICA DEL MODELO

Al objeto de facilitar la ejecución de la aplicación del modelo, se describen, a continuación, los pasos propuestos para este modelo:

4.1. Paso 1: Delimitación del alcance

El primer paso para la aplicación del modelo de medición de indicadores para la mejora de la ciberresiliencia consiste en determinar el alcance del estudio que se desea realizar. 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 críticas). Por tanto, cada organización que desee someterse a este modelo debe determinar cuál será el alcance de su consulta.

La elección del alcance de la consulta se realizará por parte del promotor de la consulta. Como indicación general, cada empresa deberá rellenar la consulta en relación a la provisión concreta de un servicio esencial cuya interrupción presumiblemente ocasione un gran impacto para la misma. 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 por el encuestado.

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

4.2. Paso 2: Realización de la consulta de autoevaluación

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

La consulta se realiza, por tanto, mediante una herramienta que dispone de las cuatro metas de la consulta: Anticipar, Resistir, Recuperar y Evolucionar. Para cada una de estas metas se realiza la medición de diferentes métricas. Cada una de estas métricas puede estar implementadas según un nivel de madurez. El nivel de madurez está adaptado a cada una de las métricas, siendo el correspondiente a una de ellas según se muestra en la Figura 3

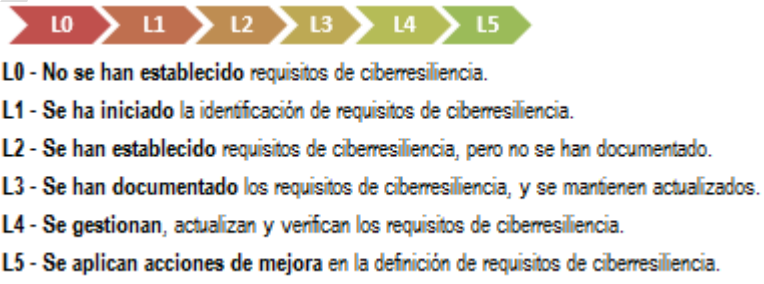

Figura 3: Niveles de madurez consulta IMC.

Una vez respondido el nivel de madurez correspondiente a cada una de las métricas, la herramienta ofrece el resultado obtenido para cada una de las metas en forma de diagrama de barras como se puede ver en la Figura 4

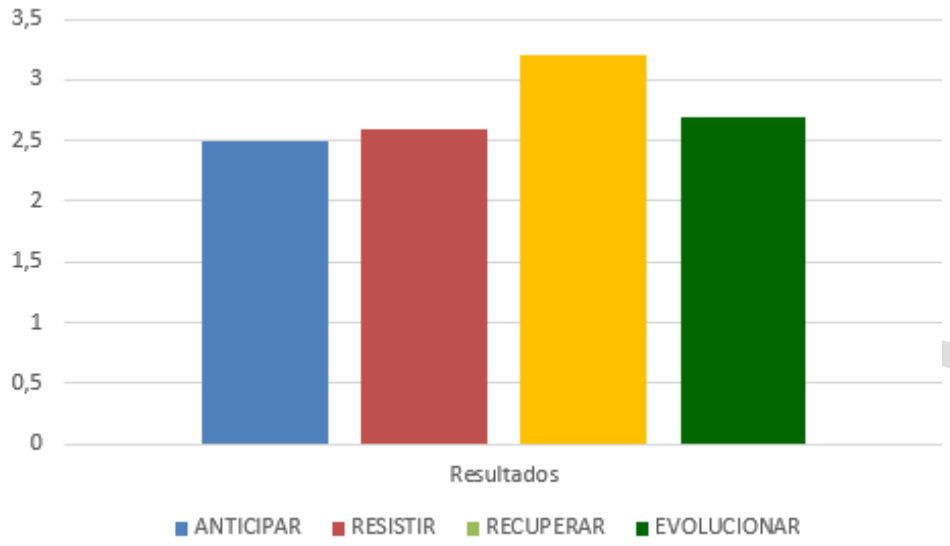

Figura 4: Ejemplo de resultados de la herramienta de consulta de IMC.

Para cada uno de los servicios esenciales identificados en el punto anterior se deberá rellenar una consulta, de forma que se pueda obtener el valor de ciberresiliencia de cada uno de los servicios esenciales.

4.3. Paso 3: Aplicación de medidas correctivas

El último paso una vez realizada la consulta de autoevaluación es la aplicación de medidas correctivas. En el documento del modelo ENSI_IMC_02- Diccionario de indicadores para la Mejora de la Ciberresiliencia se podrán consultar aquellas medidas correctivas para aquellas 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 anticipar:

Indicador	**Valores positivos**	Valores tendentes a L5 indican que existe un proceso mejorado para estimar el número de horas entre la fecha de detección de una vulnerabilidad que afecte a una función crítica y la fecha de mitigación de la misma.
	Acciones correctivas	- Revisar y mejorar la implantación del procedimiento de gestión de vulnerabilidades.

Figura 5: Ejemplo de medidas correctivas.

El estudio de la idoneidad de la aplicación de las medidas correctivas propuestas u otras más idóneas para la organización que realiza la consulta, así como el propio proceso de implantación de las mismas queda fuera del alcance de este modelo. .

4.4. Periodicidad e importancia de la consulta

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 e intentar evolucionar para mejorar aquellos aspectos que sea posible incrementando de esa forma la ciberresiliencia de aquellos servicios considerados esenciales.

5. ACRÓNIMOS

ARLI: Análisis de Riesgos Ligero.

C4V: Construcción de Capacidades de Ciberseguridad de la Cadena de Valor.

CERT: *Computer Emergency Response Team*.

CERTSI: CERT de Seguridad e Industria.

CIS: *Center for Internet Security.*

CNPIC: Centro Nacional para la Protección de las Infraestructuras Críticas.

ENISA: *European Network and Information Security Agency*.

IEC: *International Elecrotechnical Commission*.

IMC: Indicadores para la Mejora de la Ciberresiliencia

INCIBE: Instituto Nacional de Ciberseguridad.

ISA: *International Society for Automation*.

NIST: *National Institute of Standards and Technology*.

OC: Operador Crítico.

PES: Plan Estratégico Sectorial.

PIC: Protección de Infraestructuras Críticas.

PPO: Plan de Protección del Operador.

SCI: Sistemas de Control Industrial.

SEE: Secretaría de Estado de Energía.

SES: Secretaría de Estado de Seguridad.

SESIAD: Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

6. REFERENCIAS

[1] Gobierno de España, “ESTRATEGIA DE SEGURIDAD NACIONAL,” 2013. [Online]. Available: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf.

[2] Gobierno de España, “ESTRATEGIA NACIONAL DE CIBERSEGURIDAD,” 2013. [Online]. Available: http://www.dsn.gob.es/es/file/146/download?token=Kl839vHG.

[3] R. v. S. a. E. Berghout., The Goal/question/metric Method: A practical guide for quality improvement of software development., McGraw-Hill, 1999.

[4] CERTSI, “CIBER-RESILIENCIA: Aproximación a un marco de medición.,” [Online]. Available: https://www.certsi.es/sites/default/files/contenidos/estudios/doc/int_ciber_resiliencia_marco_medicion.pdf.

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

certsi_

CERT DE SEGURIDAD E INDUSTRIA