TLP:WHITE

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

Esquema Nacional de Seguridad Industrial

ENSI_POL_01- Política General: Objetivos y Actores

certsi_

CERT DE SEGURIDAD E INDUSTRIA

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

NOVIEMBRE 2016

1. OBJETO DEL DOCUMENTO

Este documento establece la Política del Esquema Nacional de Seguridad Industrial (ENSI).

Como tal, establece los aspectos básicos del ENSI, su motivación y los elementos que lo componen. Para ello, desarrolla:

- Situación contextual que promueve la creación del ENSI, reflejando la necesidad de su creación y del apoyo normativo que lo sustenta.
- Objetivos que se persiguen con el ENSI junto a los principios que han estado presentes en todas las etapas de su creación.
- Identificación de actores y partes interesadas que están llamados a participar en el ENSI.
- Los diferentes elementos a través de los que se desarrolla el ENSI.
- Una aproximación metodológica de aplicación.

2. ANTECEDENTES Y CONTEXTO

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.

En esta Ley los conceptos de Infraestructura Crítica y de Servicio Esencial quedaron definidos de la siguiente manera:

- ***Infraestructuras críticas:*** *las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.*
- ***Servicio esencial:*** *el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.*

Adicionalmente, en la mencionada Ley se establece la creación del Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), y le atribuye la capacidad de impulsar las políticas de seguridad del Gobierno sobre los distintos sectores estratégicos nacionales, así como velar por su aplicación, sirviendo como puntos de contacto especializados en la materia, así como la elaboración y el mantenimiento de un Catálogo de infraestructuras, donde se determina la criticidad de cada Infraestructura Crítica.

Así pues, la citada normativa establece entre los distintos instrumentos de planificación, la necesidad de elaboración de los siguientes documentos por parte de los operadores críticos:

- **PSO, Plan de Seguridad del Operador.** Documento estratégico donde se recogen las políticas generales de los operadores críticos. Detalla las políticas de seguridad, la relación de servicios esenciales prestados, la metodología seguida para el análisis de riesgos (amenazas físicas y lógicas), su modelo de gestión y el criterio que se va a seguir para la aplicación de medidas de seguridad adecuadas.
- **PPE, Plan de Protección Especifico**, engloba los documentos operativos. En él se definen las medidas concretas tanto existentes, como las que se vayan a adoptar por los operadores críticos en cada una de las infraestructuras críticas sobre las que tiene responsabilidad.

Para la realización de ambos documentos CNPIC tiene a disposición de los operadores sendas guías de buenas prácticas [1] y [2].

Mientras, CNPIC se encarga de desarrollar los llamados **Planes Estratégicos Sectoriales (PES),** cada uno compuesto por cuatro documentos o entregables, cuya estructura es:

- Normativa de aplicación.
- Estructura del sector/subsector.
- Análisis general de riesgos.
- Propuesta de medidas estratégicas.

Por su parte, la Estrategia de Seguridad Nacional [3] de 2013 reconoce, por primera vez, las ciberamenazas como uno de los riesgos y amenazas a la seguridad nacional. Adicionalmente, la Estrategia de Ciberseguridad Nacional [4] 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 para la Protección de las 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 Seguridad (SES) promueven actuaciones para la mejora de la ciberseguridad de las infraestructuras críticas.

Posteriormente, la Resolución de 8 de septiembre de 2015 [5] de la Secretaría de Estado de Seguridad por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específico refrenda la responsabilidad del CERT de Seguridad e Industria (CERTSI) en la resolución de incidencias cibernéticas que puedan afectar a la prestación de los servicios esenciales gestionados por los operadores.

El CERTSI, operado técnicamente por INCIBE, y bajo la coordinación del CNPIC e INCIBE, a través del mencionado acuerdo entre la SESIAD y el SES da apoyo directo al CNPIC en todo lo relativo a la prevención y reacción ante incidentes que puedan afectar a las redes y sistemas de los operadores de infraestructuras críticas.

Para abordar la mejora de la seguridad del sector industrial se propone la creación del Esquema Nacional de Seguridad Industrial.

En este contexto, el Esquema Nacional de Seguridad Industrial (ENSI) surge como elemento sobre el que facilitar el desarrollo de las actuaciones en materia de seguridad industrial en un marco común a través del que homogeneizar el tratamiento de problemáticas comunes desde perspectivas particulares y cumpliendo la normativa establecida.

3. PRINCIPIOS Y OBJETIVOS DEL ENSI

La creación del ENSI parte de la declaración de sus principios, concretados a través de su misión, visión y valores y que se detallan como sigue:

- **Visión del ENSI:** Mejorar la seguridad de la industria, garantizando la continuidad del servicio en un marco común y homogéneo del tratamiento de problemáticas comunes desde perspectivas particulares y cumpliendo la normativa establecida.
- **Misión del ENSI:** Mejorar las capacidades actuales de la industria y sus proveedores favoreciendo una adaptación ágil ante nuevas amenazas desde una perspectiva integral de la seguridad.
- **Valores del ENSI:**
  - Colaborar con la Industria para asegurar el éxito del ENSI.
  - Búsqueda del entendimiento con las empresas del sector de la seguridad desde una perspectiva integral de la misma.
  - Agilidad para adaptarse a nuevos casos y sectores.

La mejora integral de la seguridad en el sector industrial es el principal objetivo del ENSI propuesto a través de esta Política.

Además, el ENSI tiene una vocación global y pretende acercar el conocimiento de un sector maduro, como es el de la seguridad de la información, a un sector en desarrollo, como es la seguridad de la información aplicada a las operaciones industriales.

Así pues, los **objetivos** que se persiguen con el ENSI se podrían concretar en los siguientes:

- Mejorar la seguridad de los Sistemas de Control Industrial (SCI), especialmente de aquellos implicados en la prestación de los servicios esenciales. (O1)
- Mejorar la capacidad de resiliencia de Operadores Críticos para mejorar la continuidad de la prestación de los Servicios Esenciales. (O2)
- Facilitar la aplicación de la regulación y normativa existente. (O3)
- Homogeneizar el tratamiento de la seguridad, facilitando la labor del regulador y aportando metodologías e instrumentos de aplicación común. (O4)
- Extender la mejora de la seguridad de los Operadores Críticos al resto de su cadena de valor. (O5)

A través de estos objetivos, los **beneficios** que persigue el ENSI son:

- Mejorar la internacionalización y competitividad de las empresas del sector industrial a través de la mejora de sus capacidades de seguridad. (B1)
- Dinamizar el sector de la seguridad industrial para promover la incorporación de medidas de seguridad de la información. (B2)
- Extender la cultura de la seguridad a un sector para acelerar la incorporación de medidas de ciberseguridad en los entornos de operación. (B3)
- Catalizar nuevas acciones regulativas, normativas y buenas prácticas. (B4)

- Aportar un punto de encuentro o contacto entre la industria de la seguridad de la información y el sector industrial, de forma que la madurez de la seguridad de la información se pueda aprovechar por parte de la industria. (B5)

El cumplimiento de estos objetivos debe hacerse acorde a una serie de **principios**, inherentes a la filosofía con la que se ha creado el ENSI. Estos principios regentes son los siguientes:

- Carácter eminentemente práctico: aportando herramientas o instrumentos de aplicación directa.
- Específico del sector industrial: contemplando las particularidades y necesidades comunes del sector.
- Ligero: minimizando posibles cargas adicionales a los gestores de la seguridad de los Operadores Críticos.
- Vocación global: en tanto que es específico para Operadores Críticos pero aplicable en Sistemas de Control Industrial de cualquier organización.

En definitiva, el ENSI propone instrumentos para la mejora integral de la seguridad especialmente diseñados para facilitar a los Operadores Críticos el cumplimiento de la legislación vigente en esa materia y facilitando la tarea del CNPIC de velar por dicha operación segura de servicios aportando con una aproximación sencilla para su aplicación en cualquier entorno industrial.

4. ACTORES Y PARTES INTERESADAS

La mejora integral de la seguridad en el sector industrial requiere de la colaboración de múltiples partes y la adecuada coordinación de los diferentes intereses y objetivos de aquéllas.

La seguridad industrial protege las operaciones del negocio teniendo en cuenta sus objetivos y sus problemáticas, que van desde la escasa capacidad de algunos de los equipos utilizados para controlar los procesos a la necesidad de mantener un flujo continuo de datos que asegure la no interrupción de los procesos productivos.

Adicionalmente, algunos de estos procesos industriales son de especial importancia para la población civil, por lo que es necesario ser sensibles a la necesidad del regulador de disponer de información acerca de las operaciones de los Servicios Esenciales.

El ENSI se constituye de esta forma en un punto de encuentro entre los Operadores Críticos y de Sistemas de Control Industrial y los organismos reguladores con un carácter global de forma que el resto de industria pueda acercarse a las herramientas y metodologías propuestas para mejorar la seguridad dentro de sus organizaciones, mejorando así de forma global su capacidad operativa.

Con esta visión de punto de encuentro se identifican a continuación aquellos agentes llamados a colaborar y beneficiarse del ENSI cuya misión general o función y papel en el mismo se resumen en la tabla siguiente.

Actor	Misión general	Papel en el ENSI
Operador Crítico	Prestar los Servicios Esenciales en condiciones de seguridad y cumpliendo la normativa vigente.	Aplicar las herramientas propuestas por el ENSI para mejorar su nivel de seguridad y el tratamiento homogéneo de la información.
Proveedores Operadores Críticos	Proporcionar sus servicios dentro de su ámbito de actividad a los Operadores Críticos en condiciones de seguridad.	Aplicar las herramientas propuestas por el ENSI para mejorar sus capacidades y nivel de seguridad como parte de la cadena de valor de los Operadores Críticos.
Sector industrial en general	Proporcionar servicios dentro de su ámbito de actividad y siguiendo las necesidades del negocio.	Aplicar las herramientas propuestas por el ENSI para mejorar sus capacidades y nivel de seguridad.
CNPIC	Impulsar las políticas de seguridad dentro de los operadores críticos.	Validar la utilidad del ENSI con objeto de facilitar el cumplimiento normativo y la actuación del regulador.

INCIBE	Mejorar el nivel y la cultura de ciberseguridad del sector industrial.	Promover la utilización y aplicación del ENSI dentro de su colaboración con el CNPIC en la gestión de incidentes de ciberseguridad de las infraestructuras críticas así como en el sector industrial en general.

Tabla 1: Destinatarios del ENSI

Los diferentes objetivos del ENSI mencionados en el apartado anterior tienen diferente impacto en la labor de los diferentes actores y partes interesadas, tal y como se puede ver en la siguiente tabla.

Objetivos y beneficios	OC	Proveedores	Industria	CNPIC	INCIBE
(O1) Mejora de la seguridad de los SCI	✓	✓	✓	✓	✓
(O2) Mejorar la resiliencia	✓	✓	✓	✓	✓
(O3) Facilitar la aplicación de la regulación	✓			✓	✓
(O4) Homogeneizar el tratamiento de la seguridad				✓	✓
(O5) Extender la seguridad a la cadena de valor	✓	✓	✓		✓
(B1) Mejorar la internacionalización y competitividad		✓	✓		
(B2) Dinamizar el sector		✓	✓		
(B3) Extender la cultura de seguridad			✓		✓
(B4) Catalizar nuevas normativas				✓	
(B5) Contacto entre seguridad de Tecnologías de la Información y de Operación					✓

Tabla 2: Relación entre objetivos y beneficios y actores.

5. DEFINICIÓN

El Esquema Nacional de Seguridad Industrial (ENSI) es un instrumento para la mejora de la seguridad de las empresas del sector industrial, especialmente particularizado a Operadores Críticos, para minimizar los riesgos relacionados los que se ven sometidos los servicios y establecer estrategias y medidas para la mitigación de aquellos.

El ENSI se fundamenta en áreas de acción:

- Instrumentos y guías de aplicación relativos a cuestiones o problemáticas específicas.
- Apoyo al esquema regulatorio actualmente existente en España.

Ilustración 1: Esquema resumen del ENSI

Así, 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.

Estos elementos están diseñados para 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, claves para dibujar el panorama completo al que responde el ENSI. La aproximación práctica y ligera predomina en todos los elementos del ENSI y dibuja un marco completo para la mejora de la seguridad 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.

6. ELEMENTOS BÁSICOS DEL ENSI

6.1. ARLI-SI: Metodología de Análisis de Riesgos Ligero de Seguridad Integral

El ENSI propone una metodología de Análisis de Riesgos Ligero de Seguridad Integral (ARLI-SI) elaborada al objeto de proporcionar un modelo sencillo y práctico de análisis de riesgos de seguridad en sistemas de control industrial desde una perspectiva integral de la seguridad lógica y física.

Así, ARLI-SI está basado en una metodología con valores y estimaciones de los diferentes parámetros y criterios (vulnerabilidad, impacto...) homogéneos, facilitando que los mismos sean repetibles y comparables a lo largo del tiempo, entre el propio operador y el resto de operadores.

ARLI-SI persigue cuatro objetivos principales:

- Identificar los riesgos que pueden afectar a una instalación.
- Estimar la probabilidad de que dichos riesgos se materialicen
- Estimar su impacto potencial en caso de producirse.
- Tratar los riesgos hasta un punto en el que puedan ser asumibles.

El uso de esta metodología está orientada al cumplimiento de uno de los requisitos del Plan de Seguridad del Operador, la realización de un Análisis de Riesgos y reportar dicho análisis al organismo competente.

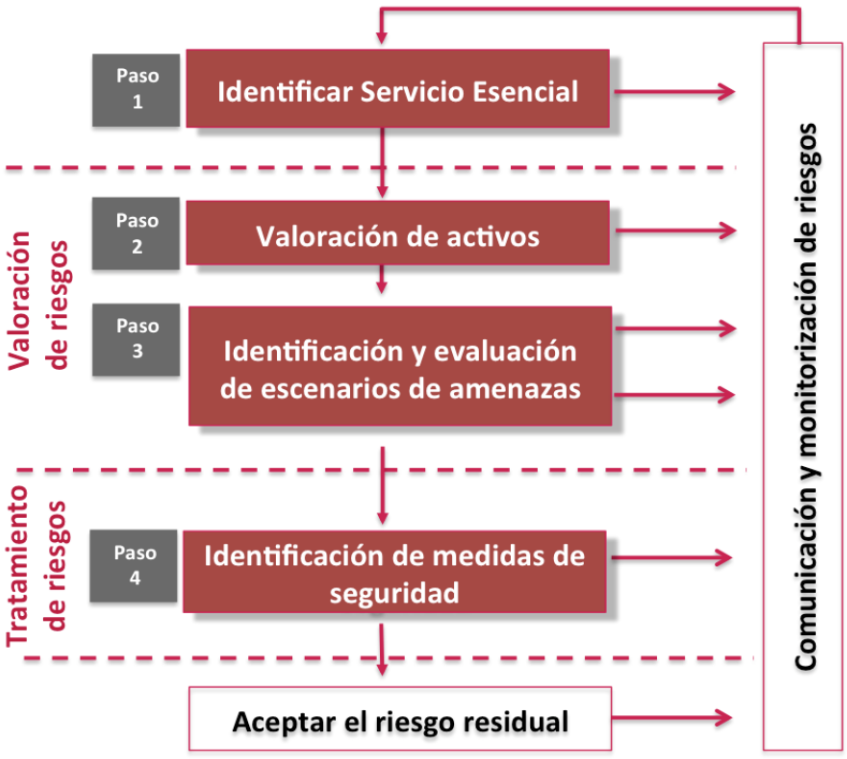

Ilustración 2: Metodología ARLI-SI

Una vez realizado este análisis es necesario valorar el riesgo aplicable sobre los activos de forma que se genere alguna actuación sobre dicho activo. Estas actuaciones pueden ser muy diversas siendo ejemplos de las mismas la transferencia del riesgo, la reducción del nivel de riesgo mediante la incorporación de salvaguardas o la asunción del riesgo. Estas actuaciones deben ejecutarse por la organización y, posteriormente, respetarse el proceso para volver a evaluar el nivel de riesgo residual sobre el que se pueden decidir nuevas actuaciones en un ciclo repetitivo.

Dentro de ARLI-SI, el ARLI-CIB permite un acercamiento específico, y también ligero, al análisis de riesgos de ciberseguridad en sistemas de control industrial. Este ARLI-CIB modelo está basado en guías y estándares reconocidos por la industria, como las familias de normas internacionales ISA/IEC 62443 e ISO/IEC 27000.

6.2. IMC: Indicadores para la Mejora de la Ciberresiliencia

La capacidad de resiliencia se define como capacidad de un sistema de soportar y recuperarse ante desastres y perturbaciones. La ciberresiliencia es, por tanto, la capacidad de soportar y sobreponerse a aquellos desastres y perturbaciones procedentes del ámbito digital.

La ciberresiliencia tiene como objetivo cuatro metas:

- Anticipar la posibilidad de un incidente.
- Resistir durante la duración de dicho incidente.
- Recuperar la actividad tras solucionar el incidente.
- Evolucionar la organización para evitar la repetición futura del incidente.

El modelo IMC de Indicadores para la Mejora de la Ciberresiliencia contempla aproximadamente 250 controles y está basado en estándares como: NIST SP 800-55 R1, ISO/IEC 27004, CIS Security Metrics v1.1.0 y ENISA Measurement Frameworks and Metrics for Resilient Networks and Services).

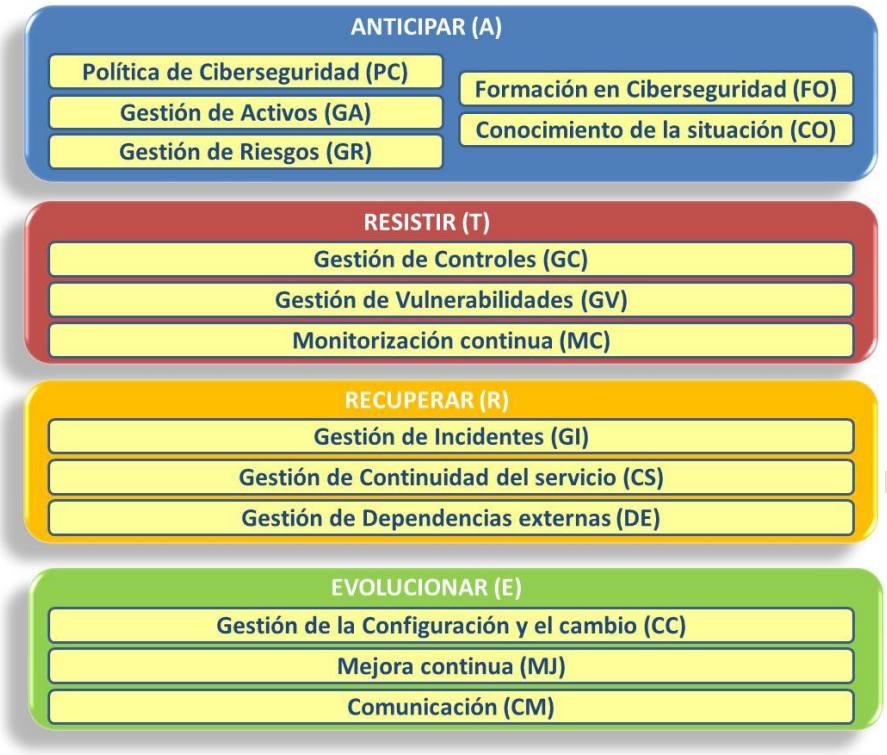

Ilustración 3: Marco de trabajo de IMC

La herramienta directora del IMC es la medición de la capacidad de ciberresiliencia a través de 46 puntos de control. Estos puntos de control han de ser evaluados por el responsable, o los responsables, de seguridad en la empresa u organización de forma que queden reflejados todos los aspectos que influyen en la capacidad de resiliencia, ya sea en el plano de la seguridad en las tecnologías de la información, el control industrial o el físico.

Una vez completada la medición, los indicadores de ciberresiliencia resultantes proporcionan un diagnóstico particular basado en un modelo de madurez de cinco niveles (L0 a L5). Además, su aplicación de forma generalizada en todos los operadores permite realizar otros análisis también a nivel sectorial o en el entorno específico que sea necesario en cada caso.

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

El modelo C4V consiste en la mejora de la ciberseguridad de la cadena de valor mediante el análisis de una serie de controles tanto a la organización promotora como a los proveedores de la misma. De esta forma, se favorece o asegura la extensión del esfuerzo por la mejora de la ciberseguridad a toda la operativa y actividad de prestación de servicio del operador implicando a proveedores y clientes.

C4V proporciona una serie de controles basándose en un modelo de madurez de diferentes niveles que permita tanto la evaluación interna o a la cadena de valor como establecer niveles mínimos aceptables en función de los resultados obtenidos durante la fase de análisis de riesgos.

Este modelo está pensado para poder evaluar de forma independiente la Disponibilidad, Confidencialidad e Integridad de la información, obteniéndose de esta forma una calificación para cada uno de los tres aspectos en función de la aplicación de la regla de mínimos a los diferentes controles aplicables.

C4V también permite orientar a todo aquel que se someta al modelo en el proceso de mejora necesario para elevar el nivel de seguridad.

6.4. SA: Sistema de Acreditación en Ciberseguridad

Mediante este sistema, y **para cada conjunto de servicios que puedan considerarse semejantes**, se busca:

1. Especificar un conjunto mínimo de controles de ciberseguridad que deben estar implantados en los operadores y arquitecturas que controlan la prestación de esos servicios, así como las prácticas mínimas requeridas de implantación de esos controles.
2. Definir los métodos que permitan evaluar la implantación de esos controles.
3. Desarrollar los procedimientos, medios y mecanismos que permitan acreditar la correcta implantación de los mínimos requeridos.

Es conveniente destacar que prestadores de servicios semejantes, deberán haber implantado un mínimo de seguridad equivalente para poder obtener la acreditación. Por encima de esta línea base, las empresas podrán aumentar sus niveles de seguridad, pero la acreditación busca garantizar unos niveles mínimos equiparables entre todos los operadores que prestan servicios análogos.

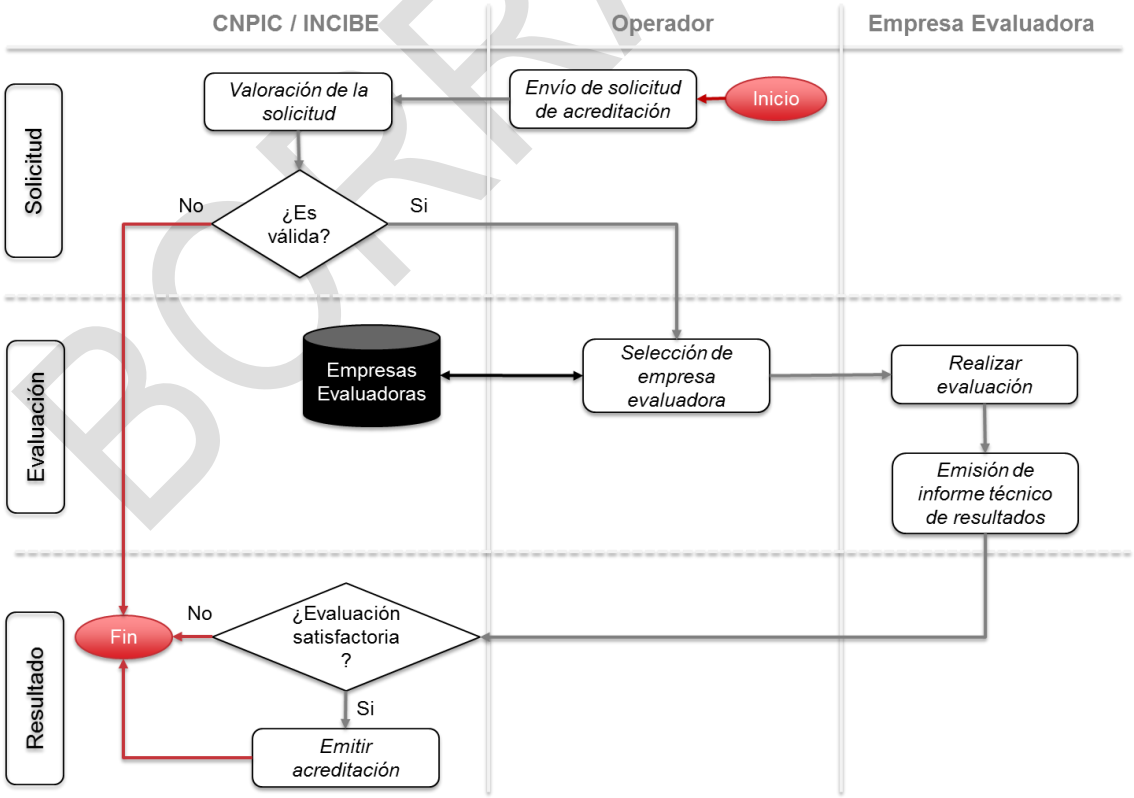

Ilustración 4: Resumen procedimiento de acreditación

7. EL ENSI Y LA GESTIÓN DE LA CIBERSEGURIDAD

Para facilitar la acometida de la mejora de la ciberseguridad, el ENSI permite una aplicación centrada en la gestión de la ciberseguridad desde una perspectiva integral.

Así, aunque los elementos del ENSI pueden ser aplicados de manera independiente, asegurando los resultados de cada uno de ellos, una aplicación integral en materia de ciberseguridad permite generar y gestionar una secuencia o cadena de actuación que permite la mejora continua y maximiza los beneficios.

Según esta aproximación, el primer paso a realizar es un análisis de riesgos de ciberseguridad. Este análisis persigue que la organización mejore el conocimiento que tiene de sus operaciones, de cómo se realizan las operaciones y de aquellos activos vitales para la prestación de los servicios y su protección en el ámbito ciber. Para acometer dicho análisis de una forma homogénea y sencilla, el ENSI propone ARLI-CIB como punto de partida para el resto de elementos de aplicación.

Tras este análisis de riesgos, las otras utilidades proporcionadas por el ENSI pueden ser aplicadas de forma simultánea o secuencial, mejorando la capacidad de ciberresiliencia de la organización o ayudando a proveedores y clientes a mejorar sus capacidades. La aplicación del ENSI se plantea por tanto de dentro hacia afuera, partiendo del operador interesado y llegando a los constituyentes de su cadena de valor.

Ilustración 5: Aproximación metodológica de la gestión de la ciberseguridad a través del ENSI

Ilustración 6: Etapas de aplicación del ENSI

La realización de un análisis de riesgos proporcionará información valiosa y permite cuantificar los riesgos y su probabilidad de suceso. Con esta información es posible tomar decisiones acerca de las salvaguardas a aplicar a fin de reducir tanto la probabilidad de ocurrencia como el impacto en la organización.

Una vez implantados los cuatro elementos o acciones, las posteriores iteraciones de cada uno de ellos contribuyen a un ecosistema de mejora continua de la ciberseguridad en las organizaciones.

8. ACRÓNIMOS

ARLI-CIB: Análisis de Riesgos Ligero de Ciberseguridad.

ARLI-SI: Análisis de Riesgos Ligero de Seguridad Integral.

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.

ENSI: Esquema Nacional de Seguridad Industrial.

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.

9. REFERENCIAS

[1] CNPIC, «GUÍA DE BUENAS PRÁCTICAS Plan de Protección Específico (PPE),» [En línea]. Available: http://cnpic.es/Biblioteca/Noticias/GUIA_BUENAS_PRACTICAS_PPE.pdf.

[2] CNPIC, «GUÍA DE BUENAS PRÁCTICAS Plan de Seguridad del Operador (PSO),» [En línea]. Available: http://cnpic.es/Biblioteca/Noticias/GUIA_DE_BUENAS_PRACTICAS_PSO.pdf.

[3] Gobierno de España, «ESTRATEGIA DE SEGURIDAD NACIONAL,» 2013. [En línea]. Available: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf.

[4] Gobierno de España, «ESTRATEGIA NACIONAL DE CIBERSEGURIDAD,» 2013. [En línea]. Available: http://www.dsn.gob.es/es/file/146/download?token=Kl839vHG.

[5] Boletín Oficial del Estado, «Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.,» 18 Septiembre 2015. [En línea]. Available: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10060.

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR | GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

certsi_
CERT DE SEGURIDAD E INDUSTRIA

certsi_
CERT DE SEGURIDAD E INDUSTRIA