TLP:WHITE

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

Esquema Nacional de Seguridad Industrial

ENSI_C4V_01- Modelo de Construcción de Capacidades de Ciberseguridad de la Cadena de Valor (C4V)

BORRADOR

certsi_

CERT DE SEGURIDAD E INDUSTRIA

ÍNDICE

INDICE DE FIGURAS

BORRADOR

*La información contenida en este documento, **podrá ser distribuido sin restricciones, sujeto a los controles de Copyright**. Para más información sobre el protocolo TLP de intercambio de información sensible puede consultar la página web: https://www.certsi.es/tlp*

ÍNDICE DE TABLAS

BORRADOR

NOVIEMBRE 2016

1. OBJETIVO Y ALCANCE DEL DOCUMENTO

1.1. Objetivo

El objetivo del presente modelo de construcción de capacidades de ciberseguridad para sistemas de control industrial es ayudar a todas las partes interesadas en su seguridad a disponer de un método que les permita conocer el grado de madurez y robustez de los controles y medidas de protección implementados en los mismos, prestando especial atención a la importancia que tienen las dependencias en los servicios esenciales y, en particular, a la gestión del riesgo en la cadena de suministrio TIC.

1.2. Alcance

El modelo de construcción de capacidades de ciberseguridad que se presenta en el documento está especialmente diseñado 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.

Aunque existen modelos equivalentes para las tecnologías de información de propósito general, las particularidades de estos sistemas justifican la necesidad de un modelo específico, en concreto:

- Foco en la seguridad y la disponibilidad
- Tecnologías específicas y propietarias
- Ciclo de vida del equipamiento

En el caso de que el nivel de capacidad esté afectado por proveedores de servicios terceros, el responsable del servicio deberá establecer mecanismos para asegurar que dichos terceros cumplen con los requisitos necesarios para el nivel de capacidad correspondiente definidos en el presente documento y disponer de procedimientos de supervisión para asegurar que dicho nivel se mantiene durante todo el ciclo de vida del servicio.

El presente modelo no está destinado a los terceros que formen parte de la cadena de valor, a menos, que en sí mismos sean responsables de la prestación de un servicio esencial.

BORRADOR

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 capacidad para proteger los SCI	Mejora continua capacidades ciberseguridad de SCIs
Área de Operaciones	Mejorar el nivel de capacidad en los SCI	Mejora continua capacidades ciberseguridad de SCIs
Responsables de riesgos / Seguridad	Disponer de un modelo para definir capacidades de ciberseguridad en SCI	Mejora continua capacidades ciberseguridad de SCIs
	Externas	
Accionistas	Conocer el nivel de capacidad para proteger los SCI	Información sobre capacidades ciberseguridad de SCI
Socios / partners	Asegurar niveles equiparables de capacidades en ciberseguridad	Información sobre capacidades ciberseguridad de SCI
Proveedores	Disponer de un marco homogéneo para la definición de requisitos	Evaluación del nivel de capacidad en ciberseguridad de los servicios prestados
Reguladores/gobierno	Conocer el nivel de ciberseguridad de los SCIs	Información sobre capacidades ciberseguridad de SCI
Usuarios externos	Conocer el nivel de ciberseguridad de los SCIs	Información sobre capacidades ciberseguridad de SCI
Consultores/auditores	Disponer de un modelo para definir / evaluar capacidades de ciberseguridad en SCI	Método para evaluación / mejora continua capacidades ciberseguridad de SCIs

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

BORRADOR

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.

BORRADOR

3. INTRODUCCIÓN Y ANTECEDENTES

3.1. ¿Qué son los modelos de construcción de capacidades?

3.1.1. Definición

Los modelos de construcción de capacidades (también conocidos como de *desarrollo de capacidades*) son una aproximación conceptual que se enfoca en comprender los obstáculos que impiden a las personas, gobiernos u organizaciones realizar sus objetivos de desarrollo a la vez que mejoran las habilidades que les permitirán alcanzar resultados medibles y sostenibles.

Los pasos que construyen esta capacidad organizativa incluyen: Desarrollar un marco conceptual, establecer una actitud organizativa, desarrollar una visión y una misión, desarrollar una estructura organizativa y adquirir habilidades y recursos.

3.1.2. Orígenes

El término fue acuñado en 1991 por el Programa de Desarrollo de las Naciones Unidas (UNDP – United Nations Development Programme) y, desde entonces, este tipo de modelos ha venido siendo aplicado por organismos internacionales (como el Banco Mundial o las propias Naciones Unidas) para referirse a programas de desarrollo de ciertas regiones o comunidades. Originalmente, hace referencia al desarrollo de habilidades, competencias y habilidades de las personas de esas sociedades en desarrollo para que puedan superar las causas de su exclusión y falta de crecimiento.

3.1.3. Aproximaciones desde el mundo de las Tecnologías de la Información

En el mundo de las Tecnologías de la Información (TI) son particularmente conocidos dos aproximaciones a este concepto:

- Los Modelos de Madurez de las Capacidades (más conocidos por sus siglas en inglés, CMM - *Capability Maturity Model*) elaborados a comienzo de los 90, inicialmente para evaluar los procesos de desarrollo de software, aunque luego se ha generalizado a otros procesos. Su precursor es el modelo de etapas de crecimiento de TI de Richard L. Nolan (1973) y el desarrollo posterior ha sido obra del *Software Engineering Institute* de la Universidad Carnegie Mellon.
- Los Modelos de Capacidades, *liderados* por la familia de normas ISO/IEC 15504 (que lleva por título *Software Process Improvement and Capability dEtermination* lo que hace que se la conozca por SPICE). Al igual que en el caso anterior, se desarrolló inicialmente para el desarrollo software y posteriormente se ha extendido a otro tipo de procesos. El grupo de trabajo que la originó se formó en 1993 y ha sufrido una importante revisión en 2004, por la que el modelo de referencia de procesos se ha escindido de la norma, dejándola específicamente como el marco de medida que puede ser utilizado con cualquier modelo de referencia de procesos. Es decir, SPICE define dos dimensiones:
    - Dimensión de capacidad (niveles 2 a 5) que se centra en el proceso y que trata únicamente con atributos genéricos (es decir, aplicables a cualquier

BORRADOR

proceso: métricas, mecanismos de control, gestión de la innovación, optimización…)

- Dimensión de proceso que contiene indicadores específicos del proceso que se está evaluando (solo aplica al nivel 1).

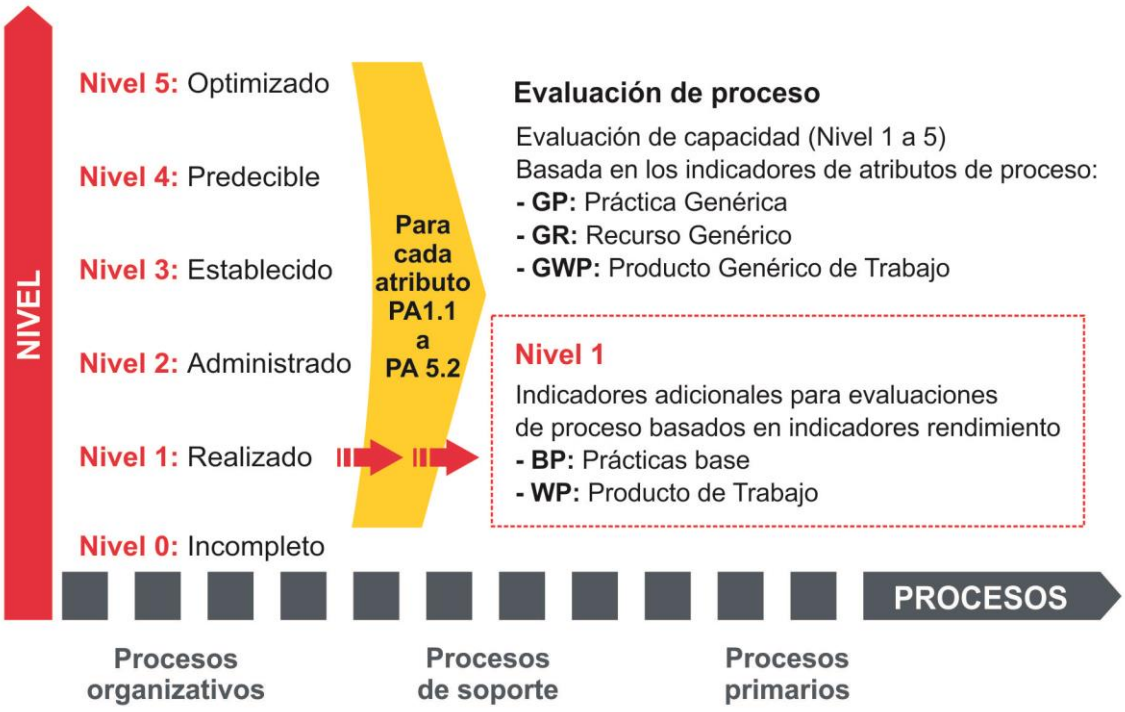

Ilustración 1: Indicadores de Evaluación

La diferencia fundamental entre ambos modelos es el concepto de **madurez**, ya que ésta aplica al nivel organizativo de la empresa u organización en su conjunto, mientras que la **capacidad** se evalúa al nivel del proceso y se realiza con fines de mejora del mismo.

Un modelo de madurez puede entenderse como un conjunto de niveles estructurados que describen hasta qué nivel de fiabilidad y sostenibilidad los comportamientos, prácticas y procesos de una organización conducen a los resultados esperados.

De hecho, la ISO/IEC 15504 entiende que estos modelos de madurez consisten en niveles de capacidad que se caracterizan por unos atributos de procesos que engloban prácticas genéricas y que es de lo que los evaluadores deben encontrar evidencias y poder así, determinar las capacidades de una organización para producir los productos esperados (software, sistemas o servicios TI).

Aunque en ambos casos, existen cinco niveles, como era de esperar no existe una equivalencia general y, de hecho, las evaluaciones realizadas respecto a SPICE suelen producir niveles inferiores a las realizadas con CMM (fundamentalmente porque para alcanzar el nivel 1 de SPICE es necesario que el proceso produzca ya el resultado esperado).

BORR

Nivel de Madurez	Nivel de Capacidad	Atributo
5 Optimizado	5 Optimizado	PA 5.1 Innovación de Proceso PA 5.2 Optimización de Proceso
4 Administrado y Medible	4 Predecible	PA 4.1 Medición de Proceso PA 4.2 Control de Proceso
3 Definido	3 Establecido	PA 3.1 Definición de Proceso PA 3.2 Despliegue de Proceso
2 Repetible pero intuitivo	2 Administrado	PA 2.1 Gestión de Rendimiento PA 2.2 Gestión del Producto de Trabajo
1 Inicial / ad hoc	1 Realizado	PA 1.1 Desempeño del Proceso
0 Inexistente	0 Incompleto	

Tabla 2. Comparación niveles CMM - SPICE.

3.1.4. Diferencias con otro tipo de documentos

Los modelos de construcción de capacidades no pretenden definir unos requisitos mínimos indispensables para los colectivos a los que se aplica, sino que su aproximación es más constructiva, persiguiendo una mejora de la preparación de las organizaciones para responder al reto que les impide alcanzar sus objetivos de desarrollo.

3.2. Colaboración público-privada

Con el objetivo de dotarse de un modelo de estas características en el menor tiempo posible, el Instituto Nacional de Ciberseguridad y LEET Security han firmado un Convenio de Colaboración para el desarrollo del modelo sobre la base de la metodología de calificación de seguridad desarrollada por esta última.

BORRADOR

4. MODELO

4.1. Descripción general

Un programa de ciberseguridad representa una suma de procesos, tecnología, políticas, gobierno, alineamiento con el negocio, actividades de concienciación y otros elementos necesarios para gestionar, de manera efectiva, la postura de ciberseguridad de la organización. Como se ha mencionado anteriormente, los modelos de capacidad tienen su origen en el Modelo de Estados de Richard L. Nolan y su utilización ofrece las siguientes ventajas:

- Es fácil de entender y explicar a no expertos.
- Un profesional con experiencia puede usar el modelo para evaluar la capacidad sobre la base de entrevistas, observaciones y otras evidencias.
- Proporcionan una medida cualitativa de la capacidad.
- Permite elaboración de *benchmarkings* con un criterio común.
- Han sido diseñados originalmente para evaluar las tecnologías de la información, siendo fácilmente adaptables al entorno de la ciberseguridad.

El modelo descrito en este documento no persigue evaluar la madurez de la organización en su conjunto, sino proporcionar un mecanismo lo más objetivo posible para evaluar el nivel de capacidades en materia de ciberseguridad que presenta un sistema de control industrial.

En este sentido, el modelo expuesto se diferencia de los modelos de madurez existentes en que, no solo evalúa los procesos establecidos en la organización, sino también la robustez de las medidas de seguridad técnicas que se aplican, de manera efectiva, sobre los sistemas de control industrial incluidos en el alcance.

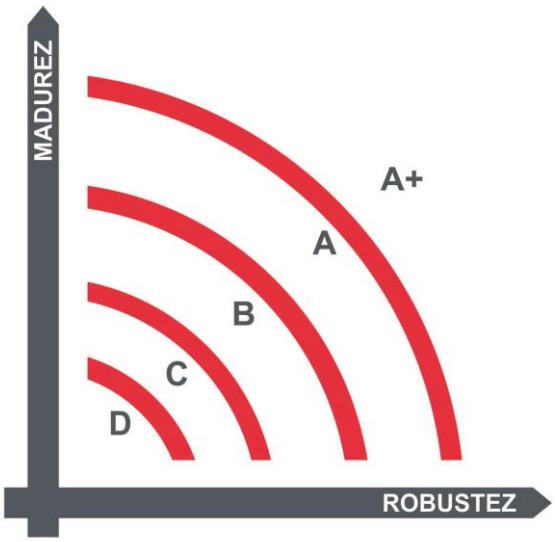

Ilustración 2: Niveles de capacidades del modelo

Este doble enfoque, que aúna madurez de procesos y robustez de medidas técnicas, permite a las organizaciones obtener una visión completa y fácilmente comprensible sobre

su nivel de capacidad en ciberseguridad en relación a la protección de los sistemas de control industrial que opera. Es decir, permite conocer el nivel de capacidades actual, y lo que es más importante, permite establecer un nivel objetivo y conocer los pasos que se deben dar para alcanzar ese nivel superior de capacidades de ciberseguridad.

4.2. Niveles

El modelo de construcción de capacidades cuenta con cinco niveles de la 'A+' a la 'D' (siendo la 'A+' la mejor valoración). El sistema evalúa las medidas de seguridad y resiliencia en la gestión del SCI, es decir que diferentes SCIs operados por una misma organización podrían obtener diferentes evaluaciones de capacidades.

A diferencia de los modelos que evalúan procesos, los niveles utilizados en el presente documento no pueden tener una denominación para caracterizar a procesos, por lo que se ha optado por una denominación genérica sin asociar a ningún tipo de adjetivo. No obstante, los elementos que influyen en obtener unos mayores niveles serían los siguientes:

- Políticas y procedimientos
- Involucración de la dirección
- Mecanismos de supervisión
- Concienciación
- Presupuesto
- Profesionalización de la función
- Robustez de medidas técnicas
- Relaciones con terceros (incluyendo proveedores de servicios)
- Resiliencia

4.3. Dimensiones

Dado que se pueden establecer diferentes medidas de seguridad para cada SCI, el modelo asigna un nivel en tres dimensiones de la seguridad: confidencialidad, integridad y disponibilidad. De esta forma la evaluación de la capacidad toma la forma de una triada de letras:

- La primera letra corresponde al nivel de **confidencialidad**.
- La segunda letra es el nivel para la **integridad**.
- Y la tercera letra es el nivel asignado para la dimensión de **disponibilidad**.

Ilustración 3: Formato de la evaluación de la capacidad

BORRADOR

4.4. Funciones clave de la ciberseguridad y ciberresiliencia

Las funciones organizan las actividades básicas de ciberseguridad a alto nivel y también permiten alinearse con metodologías existentes para la gestión de incidentes, permitiendo mostrar el impacto de las inversiones en ciberseguridad. Las funciones clave que se identifican en relación a la ciberseguridad de forma general por varios marcos y documentos son las cinco siguientes:

- **Identificar**: Desarrollar la comprensión organizativa necesaria para gestionar los riesgos de ciberseguridad sobre los sistemas, activos, datos y capacidades.
- **Proteger**: Desarrollar e implantar las salvaguardas apropiadas para asegurar la entrega de los servicios críticos.
- **Detectar**: Desarrollar e implementar las actividades adecuadas para identificar la ocurrencia de eventos de ciberseguridad.
- **Responder**: Desarrollar e implantar las actividades apropiadas para adoptar acciones en relación a los eventos de ciberseguridad detectados.
- **Recuperar**: Desarrollar e implementar las actividades adecuadas para mantener planes orientados a la resiliencia y para recuperar las capacidades o servicios afectados por los eventos de ciberseguridad.

Ilustración 4: Funciones clave de ciberseguridad

Estas cinco funciones clave han sido desarrolladas en un marco de ciberseguridad por el NIST (*National Institute of Standards and Technology*) para incluir:

- **Categorías**: Grupos de resultados de ciberseguridad relacionados estrechamente con necesidades de un programa de ciberseguridad y con actividades particulares.
- **Subcategorías**: Divisiones más detalladas que representan resultados específicos de actividades de gestión y/o técnicas. Proporcionan un conjunto de resultados que, sin ser exhaustivas, ayudan a conseguir alcanzar los resultados de cada categoría.

Esta división permitirá trazar las medidas de ciberseguridad incluidas en este modelo de construcción de capacidades con las funciones claves mencionadas anteriormente.

BORRADOR

Por otro lado, dado que existen múltiples tipos de ciberataques que pueden sufrir las organizaciones, entre ellos, ataques que persiguen interrumpir los servicios que prestan, o ataques que explotan las vulnerabilidades de sus sistemas para acceder a información valiosa con fines delictivos o ciberespionaje, poniendo en riesgo los intereses nacionales, y la vulneración de la confianza de sus clientes, es necesario avanzar en dotarse de capacidades de ciberresiliencia. La ciberresiliencia se entiende como 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.

Para conseguir dicha ciberresiliencia, partiendo de unos objetivos, capacidades y técnicas, debemos ser capaces de medirla, de una manera eficiente, coordinada y metodológica, con el fin de garantizar que las organizaciones tienen adoptadas unas medidas razonables que garanticen la protección de sus datos, sistemas y equipos. Esta ha sido la razón que ha llevado a INCIBE (*Instituto Nacional de Ciberseguridad*) a desarrollar un conjunto de métricas e indicadores de ciberresliencia.

Las capacidades en dichas métricas e indicadores están organizadas en seis niveles de madurez:

- **Inexistente** (nivel 0)
- **Inicial / ad-hoc** (nivel 1)
- **Repetible pero intuitivo** (nivel 2)
- **Definido** (nivel 3)
- **Gestionado y medible** (nivel 4)
- **Optimizado** (nivel 5)

Estos niveles permitirán incluir las medidas orientadas a conseguir esta ciberresiliencia en el modelo de construcción de capacidades que se detalla en este documento.

BORRADOR

5. METODOLOGÍA DE EVALUACIÓN

5.1. Asignación de nivel de capacidad

5.1.1. Atributos del modelo

La determinación del nivel de capacidad se basa en la evaluación de atributos clasificados en 14 capítulos:

Atributos del modelo	
■ Programa de Gestión de Seguridad de la Información	■ Protección de código malicioso
■ Operación de Sistemas	■ Controles de red
■ Seguridad del Personal	■ Supervisión
■ Seguridad de las Instalaciones	■ Control de acceso
■ Procesamiento de terceros	■ Seguridad en el desarrollo
■ Resiliencia	■ Gestión de incidentes
■ Cumplimiento	■ Criptografía

Cada capítulo está dividido en diferentes controles que deben ser evaluados determinar el nivel de capacidad. La metodología de evaluación establece las condiciones que deben cumplirse para alcanzar cada uno de los niveles, considerando que las condiciones son acumulativas, es decir para alcanzar el nivel 'A', se deben cumplir también las condiciones para los niveles 'D', 'C' y 'B'.

Considerando que existen tres dimensiones de evaluación (confidencialidad – integridad – disponibilidad) el nivel de capacidad final estará compuesto de tres letras, una por cada dimensión de la seguridad. Para determinar cada dimensión, se deberá identificar el mínimo de los niveles correspondientes a las medidas de seguridad comunes y a aquellos medidas aplicables a cada dimensión. Por este motivo, los controles están divididos en cuatro tipos:

- Medidas de seguridad comunes.
- Medidas de seguridad relacionadas con la confidencialidad.
- Medidas de seguridad relativas a la integridad.
- Medidas de seguridad correspondientes a la disponibilidad.

5.1.2. Definición del alcance

Como se ha comentado previamente, las capacidades se evalúan en relación a la protección de un SCI, por tanto, el alcance depende la arquitectura concreta del sistema sobre el que se aplique el modelo.

BORRADOR

El alcance debería incluir todos los sistemas conectados y no segregados completamente de cualquiera de los componentes del SCI puesto que pueden afectar a la seguridad del mismo.

Los sistemas están compuesto de personas, procesos y tecnología, como servidores, aplicaciones, componentes de red, incluyendo componentes virtualizados, y lógicamente, componentes propios de un SCI. Algunos ejemplos de los elementos previamente mencionados son los siguientes:

- Servidores: web, aplicación, base de datos, autenticación, correo electrónico, proxy, protocolos de red, servidores de nombre de dominio…
- Aplicaciones: internas / externas, compradas / adaptadas…
- Componentes de red: cortafuegos, switches, enrutadores, puntos de acceso wireless, appliances de red, appliances de seguridad…
- Componentes SCI: PLC, SIS…

Si no existiera ningún tipo de segmentación en la red, la red completa debería ser incluida en el alcance de la evaluación. La segmentación de red puede ser implementada mediante diferentes métodos físicos o lógicos que restrinjan el acceso a un segmento de red concreto (como, por ejemplo, la red de dispositivos de campo o la red de puestos de control).

Si se utiliza la segmentación de la red para reducir el alcance de la evaluación, se deben documentar los mecanismos utilizados y cómo se garantiza que la configuración es adecuada (configuraciones de red, tecnologías desplegadas y cualquier otro control que se haya implementado) para facilitar su valoración y permitir su evaluación posterior.

5.1.3. Evaluación de la Cadena de Valor

La capacidad se evalúa sobre la base de todos los componentes del SCI. Por tanto, si existen proveedores de servicio implicados en cualquier parte de la provisión del servicio por parte de dichos SCI o para gestionar cualquier componente (enrutadores, cortafuegos, bases de datos, seguridad física, aplicaciones, seguridad, servidores, PLCs, etc.) pueden tener, obviamente, un impacto sobre la seguridad del sistema.

Para aquellos responsables de SCI que subcontraten parte de la gestión de su infraestructura en terceras partes proveedoras de servicio, la evaluación de la capacidad debe incluir el rol de cada proveedor de servicio, identificando claramente de qué requerimientos se encarga dicho proveedor. Existen dos opciones para evaluar la capacidad de terceras partes:

1. El proveedor puede someter a evaluación su propia capacidad y proporcionar el resultado de la evaluación al responsable del SCI; o
2. Si no realizan su propia evaluación; deberán incluir sus servicios en el alcance de la evaluación del responsable del SCI.

El objetivo es asegurar que todos los componentes de la cadena de valor tienen un nivel de capacidades en ciberseguridad, al menos, igual al nivel objetivo establecido para el responsable del servicio.

En general, los responsables de servicio deberán establecer un proceso de gestión de riesgo proveedor orientado a garantizar que, sus proveedores satisfacen los requisitos

BORRADOR

definidos en este documento para el nivel de capacidad alcanzado, tanto en el momento de la contratación como a lo largo de todo el ciclo de vida del servicio.

Dicho proceso se fundamentará en los siguientes elementos que el responsable del servicio deberá definir, establecer y asegurar que se ponen en funcionamiento (idealmente, en colaboración entre las áreas de seguridad y aprovisionamiento):

- Identificación de los servicios subcontratados en terceros con impacto potencial en el servicio prestado.
- Caracterización del nivel de impacto potencial de los servicios subcontratados.
- Definición de requisitos de ciberseguridad en función del nivel de criticidad.
- Definición de mecanismos de supervisión en función del nivel de criticidad.
- Gestión y mejora continua del proceso.

5.1.4. Criterio para la determinación del nivel capacidad

El criterio definido para determinar el nivel de capacidad de ciberseguridad está basado en el método establecido en el estándar ISO/IEC 15504 pero considerando que no sólo se está evaluando la madurez de un proceso sino que se busca también evaluar la robustez de las medidas de seguridad establecidas en la provisión de un servicio.

Por este motivo, se ha asignado a cada control un nivel de prioridad (de 1 a 3) en los niveles en los que es de aplicación. Estos niveles se utilizarán, como se indica a continuación, para evaluar el nivel de capacidad de un servicio atendiendo al siguiente criterio: Para alcanzar un determinado nivel, el servicio debe haber implementado,

- el 100% de los controles de prioridad 1 correspondientes a dicho nivel;
- al menos, el 85% de los controles de prioridad 2 correspondientes a dicho nivel; y
- al menos, el 50% de los controles de prioridad 3 correspondientes a dicho nivel

5.1.5. Utilización del modelo de capacidades

Este apartado incluye unas pautas básicas sobre cómo utilizar este modelo para abordar un proceso de identificación del nivel de capacidad actual y un plan de mejora del mismo (el motivo que conduce a la necesidad de mejora dependen de cada situación y cada organización).

Los pasos recomendados para abordar este proceso de mejora del nivel de capacidad son los siguientes:

1. Identificación de medidas aplicables.
2. Evaluación del nivel de capacidad actual.
3. Identificación del nivel de capacidad objetivo.
4. Definición de un plan de acción.

BORRADOR

Ilustración 5: Utilización del modelo de capacidades

5.1.5.1. Identificación de medidas aplicables.

En primer lugar, dado lo establecido en el apartado anterior sobre la definición del alcance (ver 4.1.2) y las dependencias de proveedores externos (ver 4.1.3), se deberán identificar qué medidas de seguridad, de las incluidas en el modelo son de aplicación al sistema concreto que se desea evaluar.

Este paso equivale al habitual en las metodologías de sistemas de gestión de seguridad de la información de elaborar la denominada "*Declaración de aplicabilidad*", es decir, qué medidas del total se van a considerar en una situación concreta.

5.1.5.2. Evaluación del nivel de capacidad actual

Para la determinación del nivel de capacidad actual se recomienda utilizar un evaluador independiente de los responsables de la operación del sistema, ya sea interno (seguridad o auditoría) o externo (empresa sin relación con la operación) y, en ambos casos, asegurando que los profesionales que realicen la evaluación cuenten con los conocimientos y experiencia suficiente para llevar a cabo dicha evaluación.

5.1.5.3. Identificación del nivel de capacidad objetivo

Por definición, los modelos de construcción de capacidades no tienen un nivel de capacidad "adecuado" o "mejor", sino que, cada organización, en función del sistema, del nivel de riesgo existente y los criterios de aceptación de riesgo que se definan, debe establecer cual es el nivel de capacidad más adecuado.

Normalmente, el nivel de capacidad objetivo será más elevado cuanto más crítico sea el sistema sobre el que se aplica o el escenario de amenazas empeore.

Dada la estructura del modelo, los niveles de capacidad se definen en las tres dimensiones mencionadas (confidencialidad – integridad – disponibilidad) por lo que la organización debe identificar un nivel de capacidad objetivo por cada una de estas dimensiones.

BORRADOR

5.1.5.4. Definición de un plan de acción

En caso de que se desee optar a un nivel de capacidad más elevado que el actual, se deberá trazar un plan de acción para la implementación de las medidas que sean necesarias para alcanzar dicho nivel. Para facilitar la implantación de medidas, las prioridades recogidas en cada medida de seguridad y nivel, ayudan a identificar las medidas que son básicas (prioridad 1) y se han de implantar primero, puesto que son el fundamento de las siguientes (prioridades 2 y 3).

Para abordar la implantación de medidas, las organizaciones se pueden apoyar en metodologías de gestión de proyectos o incluso de cambio organizacional, como la propuesta en COBIT 5 Implementación.

BORRADOR

6. ACRÓNIMOS

CMM: Capability Maturity Model

IEC: *International Elecrotechnical Commission*

ISO: International Organization for Standardization

SPICE: *Software Process Improvement and Capability Determination*

PIC: Protección de Infraestructuras Críticas

UNDP: United Nations Development Programme

BORRADOR

7. 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

BORRADOR

8. BIBLIOGRAFIA

United Nations Committee of Experts on Public Administration (2006). "Definition of basic concepts and terminologies in governance and public administration" (PDF). United Nations Economic and Social Council.

Kaplan, Allan (Aug 2000). "Capacity Building: Shifting the Paradigms of Practice". Development in Practice. 3/4 10 (10th Anniversary Issue): 517–526.

Paulk, Mark C.; Weber, Charles V; Curtis, Bill; Chrissis, Mary Beth (February 1993). "Capability Maturity Model for Software (Version 1.1)" (PDF). Technical Report (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University). CMU/SEI-93-TR-024 ESC-TR-93-177.

Nolan, R. L. (July 1973). "Managing the computer resource: A stage hypothesis". Comm. ACM 16 (7): 399–405

Anderson, Kerry A. (December, 2014). “From Here to Maturity-Managing the Information Security Life Cycle. ISACA Journal, Volume 6, 2014.

ISO/IEC 15504-4:2004 Information technology — Process assessment — Part 4: Guidance on use for process improvement and process capability determination

“Process Assessment Model (PAM): Using COBIT® 5” , ISACA, 2013

“Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans”, National Institute of Standards and Technology Special Publication 800-53, 2008

“Guide to Industrial Control Systems (ICS) Security”, National Institute of Standards and Technology Special Publication 800-82 Revision 2, mayo 2015

“Framework for Improving Critical Infrastructure Cybersecurity” Versión 1.0, National Institute of Standards and Technology, febrero 2014

Cyber Security Capability Maturity Model (CMM) – Pilot, Global Cyber Security Capacity Centre University of Oxford (15/12/2014)

BORRADOR

“Rating guide” Versión 2, LEET Security, 2016, www.leetsecurity.com/descargar-guia/

“COBIT® 5 Implementación” , ISACA, 2012

BORRADOR

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR GOBIERNO DE ESPAÑA MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

certsi_

CERT DE SEGURIDAD E INDUSTRIA

BORRADOR