CIATEQ, A. C. Centro de Tecnología Avanzada
Gerencia de Posgrado

Marco mínimo de ciberseguridad para PYMEs en el contexto de la Industria 4.0

TESIS QUE PRESENTA

Ing. Ricardo Díaz Sánchez
Asesor: Dr. Gerardo Rodriguez Barba

Para obtener el grado de

Maestro en
Sistemas Inteligentes Multimedia

Querétaro, Qro.
mayo, 2023

CARTA DE LIBERACIÓN DEL ASESOR

Guadalajara, Jalisco 20 de abril del 2023.

Mtro. Geovany González Carlos
Gerencia de Posgrado
CIATEQ, A.C.

Los abajo firmantes, miembros del Comité Tutorial del Ing. Ricardo Díaz Sánchez, una vez revisado su Proyecto Terminal de tesis/tesina, titulado "MARCO MÍNIMO DE CIBERSEGURIDAD PARA PYMES EN EL CONTEXTO DE LA INDUSTRIA 4.0" **autorizo** que el citado trabajo sea presentado por el alumno para su revisión, con el fin de alcanzar el grado de Maestro en Sistemas Inteligentes Multimedia.

Sin otro particular por el momento, agradezco la atención prestada.

Dr. Gerardo Rodríguez Barba
Asesor Académico

CARTA DE LIBERACIÓN DEL REVISOR

Santiago de Querétaro, Querétaro, 04 de mayo del 2023

MTRO. GEOVANY GONZÁLEZ CARLOS
GERENTE DE POSGRADO
CIATEQ, A.C.

Por medio de la presente me dirijo a usted en calidad de Revisor del proyecto terminal del (la) alumno (a) **RICARDO DÍAZ SÁNCHEZ**, cuyo título es:

"MARCO MÍNIMO DE CIBERSEGURIDAD PARA PYMES EN EL CONTEXTO DE LA INDUSTRIA 4.0"

Después de haberlo leído, corregido e intercambiado información con el (la) alumno(a), y realizado los cambios que le fueron sugeridos, puede ser autorizada su impresión, a fin de que se inicien los trámites correspondientes para su defensa.

Sin otro particular por el momento, y en espera de que mis sugerencias sean tomadas en cuenta en beneficio del estudiante y la Institución, agradezco la atención prestada.

Atentamente,

Mtro. Fernando González Díaz

F31b Revisión: 01-Mar-2021

DEDICATORIA

A Dios por permitirme avanzar en esta área de conocimiento.

A las PYMEs, esperando llegue el conocimiento a alguna de ellas y sea útil para que alguna inicie sus primeros pasos en el fortalecimiento de su ciberseguridad.

Este trabajo no termina, apenas inicia.

AGRADECIMIENTOS

A CONACYT por la beca otorgada, y al personal académico y administrativo de CIATEQ por las facilidades otorgadas y por la oportunidad de haber participado en este posgrado. A la empresa que me permitió acceder a sus instalaciones para el desarrollo de este proyecto. A mi asesor Dr. Gerardo Rodríguez Barba, por las observaciones realizadas a este trabajo, y al ing. Fernando González Díaz, por haber revisado este trabajo. A mi amiga Magda por su motivación, y apoyo a lo largo de este proceso de aprendizaje. A mis compañeros de estudio por el apoyo y el tiempo compartido durante el proceso.

* * *

RESUMEN

La ciberseguridad en una organización debe ser parte integral de su planeación estratégica. En el contexto de la 4ª Revolución Industrial, y la necesidad de las empresas en la transformación digital de sus procesos la ciberseguridad se ha vuelto parte esencial de su estrategia de transformación digital.

Con el objetivo de ayudar a las PYMEs que tienen recursos humanos limitados en el área de seguridad, en particular se desarrolla un caso de estudio para una PYME en el contexto de la Industria 4.0, basado en el marco NIST CSF v1.1, para ayudar a crear una cultura de valoración del riesgo, para minimizar ataques cibernéticos.

Para que este marco mínimo sea efectivo considera actividades de ciberseguridad, antes durante y después de que ocurre un incidente de ciberseguridad.

En el desarrollo del caso de estudio con una PYME de la Industria 4.0, la utilización de una hoja de cálculo le ayuda a la empresa a tener visibilidad, de áreas críticas, que requieren atención.

Del resultado de la autovaloración, se puede podrá establecer su línea base de ciberseguridad lo que le permitirá crear o mejorar su programa de ciberseguridad, la cual le permite iniciar o mejorar las actividades de ciberseguridad en relación a su postura frente al riesgo de incidentes.

Palabras clave: Industria 4.0, Seguridad, Ciberseguridad, Programa de ciberseguridad.

ABSTRACT

Cybersecurity in an organization must be an integral part of its strategic planning. In the context of the 4th Industrial Revolution, and the need for companies to digitally transform their processes, cybersecurity has become an essential part of their digital transformation strategy.

In order to help SMEs that have limited human resources in the area of security, in particular an Industry 4.0/SMEs case study is developed, based on the NIST CSF v1.1 framework, to help create a culture risk assessment, to minimize cyber-attacks.

For this minimum framework to be effective, consider cybersecurity activities, before, during, and after a cybersecurity incident occurs.

In the development of the case study with an industry 4.0/SME, the use of a spreadsheet helps the company to have visibility of critical areas that require attention.

From the result of the self-assessment, your cybersecurity baseline can be established, which will allow you to create or improve your cybersecurity program, which allows you to initiate or improve cybersecurity activities in relation to your posture against the risk of incidents.

Keywords: Industry 4.0, Security, Cybersecurity, Cybersecurity program.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO

Ciberseguridad: La ciberseguridad abarca una amplia gama de prácticas, herramientas y conceptos relacionados estrechamente con los de la seguridad de la tecnología operativa (TO) y de la información, la seguridad cibernética es un superconjunto de las prácticas incorporadas en la seguridad de TI, la seguridad de la información, seguridad de la tecnología operativa (OT) y seguridad ofensiva.

CIS (Center for Internet Security): El Centro para la seguridad de Internet desarrolló los Controles de seguridad Criticos (Critical Security Controls) el cual es un Marco de referencia reconocido por la industria. Se desarrollo como una guía para que las organizaciones se protejan de ataques conocidos.

ENCS Estrategia Nacional de Ciberseguridad: Se definen objetivos y ejes transversales, los principios rectores, identifica a los diferentes actores involucrados proporciona claridad sobre los esfuerzos entre individuos, sociedad civil, organizaciones privadas y públicas en materia de ciberseguridad en México; propuesta en 2017 por el gobierno de la República Mexicana.

IACS (Industrial Automation and Control Systems): Sistemas de Control y Automatización Industrial. Conjunto de personal, hardware, software y políticas involucradas en la operación de los procesos industriales que pueden afectar o influir en su seguridad, y en su seguridad y operación confiable.

ISA (International Society of Automation): Sociedad Internacional de Automatización. Asociación profesional sin fines de lucro que establece estándares para ingeniería y tecnología para mejorar la administración, seguridad y ciberseguridad de los sistemas de control y la automatización industrial. Desarrolló el standard ISA/62443 desarrollado para tratar las necesidades de seguridad de la automatización industrial y los sistemas de Control que utilizan las tecnologías operacionales (OT).

ISACA (Information Systems Audit and Control Association) Asociación de Auditoría y Control de Sistemas de Información: Es una comunidad de profesionales que ayuda a los negocios y profesionales a mejorar en diferentes áreas tales como la auditoria, la administración del riesgo, seguridad.

ITU (International Telecommunications Union): Unión Internacional de Telecomunicaciones. La ITU es un organismo intergubernamental con sede en Suiza con tres sectores que se ocupan del desarrollo y la publicación de recomendaciones para sistemas de radio (UIT-R), telecomunicaciones (UIT-T) y asistencia para el desarrollo (UIT-D).

NERC CIP North American Electric Reliability Corporation's Critical Infrastructure Protection standard. Estándar de Protección de Infraestructura Crítica de la Corporación de Confiabilidad Eléctrica de América del Norte, es un estándar específico para ayudar a mejorar la confiabilidad de la industria eléctrica.

NIST CSF El CSF (Cybersecurity Framework): Marco de Ciberseguridad es un marco de referencia de ciberseguridad desarrollado por NIST (National Institute for Standard and Technology) Instituto Nacional de Estándares y Tecnología de los Estados Unidos, para que las empresas lo utilicen de manera voluntaria para reducir los riesgos de ciberseguridad.

PERA (Purdue Enterprise Reference Architecture): Arquitectura de referencia empresarial de Purdue. El modelo de Purdue es una práctica recomendada de la industria y un modelo conceptual ampliamente adoptado para la segmentación de la red ICS y se usa ampliamente para explicar las estrategias y la arquitectura de seguridad.

RIESGO: es una combinación de las consecuencias que se derivan de la ocurrencia de un evento no deseado y la probabilidad de la ocurrencia del evento.

TI (Tecnología de la Información): Se refiere al software, los servidores, las computadoras personales, los teléfonos móviles y demás que comprenden el lado comercial de una organización.

TO (Tecnologías Operativas): Se refiere a los sistemas tradicionales de hardware y software que se encuentran dentro de los entornos industriales. Ejemplos incluyen controladores lógicos programables (PLC), sistemas de control distribuido (DCS) e interfaces hombre-máquina (HMI). Estos sistemas también se conocen como Sistemas de Control Industrial (ICS) porque controlan diversos procesos que ocurren dentro de un entorno industrial.

1. INTRODUCCIÓN

1.1. ANTECEDENTES

La 4ª revolución Industrial ha traído muchos beneficios y retos que las industrias tienen que afrontar en relación con la ciberseguridad. Entre los dominios aceptados actualmente en la 4ª Revolución Industrial se encuentran la automatización, digitalización, e información (Kumar, Vikas. Rezaei, Jafar. Akberdina, Victoria. Kuzmin 2021). En cuanto a la digitalización podemos encontrar las áreas de economía, sociedad, industria, servicios, educación. A la respuesta a la digitalización en el dominio industrial se le conoce como Industria 4.0, considerada como un caso especial de la digitalización. Por lo que la Industria 4.0 enfrenta grandes retos de ciberseguridad desde las perspectivas técnica, gobernanza, social, jurídica, normativa.

El trabajo a desarrollar se centra en los retos, en particular cómo enfrentarlos desde la perspectiva técnica de México. Esto puede ser el punto de partida para desarrollar proyectos que satisfagan los requerimientos en las áreas mencionadas.

De acuerdo con CANIETI (CANIETI 2017) "se ha demostrado que las organizaciones que implementan programas de ciberseguridad gestionados por riesgo tienen menores costos asociados con incidentes cibernéticos".

1.2. DEFINICIÓN DEL PROBLEMA

La mayoría de las empresas en México no cuenta con un programa de ciberseguridad, teniendo grandes costos asociados a los incidentes de ciberseguridad.

1.3. JUSTIFICACIÓN

En México en particular desde el año 2017 a través de la Estrategia Nacional de Ciberseguridad (ENCS)(Gobierno de la República Mexicana 2017), propuesta por

el gobierno de la República Mexicana, se dio inicio a la integración de un frente para combatir problemas de ciberseguridad, y estableció este documento como estratégico en materia de ciberseguridad. Esta propuesta no maduró. La Norma Mexicana NMX-I-27032-NYCE-218 (Secretaría de Gobernación. 2021) se publicó en 2018, "Tecnología de la información Técnicas de seguridad Lineamientos para la ciberseguridad", algo a destacar es que propone protección de la infraestructura de información crítica, y además tiene una visión más integral de la ciberseguridad está basada en ISO/IEC 27032:2012. Sin embargo, fue hasta octubre del año 2021, cuando a través de la Guardia Nacional dependiente de la Secretaría de Seguridad y Protección Ciudadana se publica el documento "Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos" (Gobierno de la República Mexicana. 2021). La Guardia Nacional es el organismo coordinador en materia de ciberseguridad, en la actualidad en México. Aún no hay colaboración entre los diferentes sectores en los ámbitos social, económico y políticos, y no se tienen dimensionados los riegos, amenazas, ataques, vulnerabilidades a la cuales se enfrenta la industria 4.0, no existe suficiente personal capacitado para los requerimientos de ciberseguridad, y falta cultura de ciberseguridad.

Entre los problemas que enfrentan aquellos que trabajan en la ciberseguridad en la Industria 4.0 se encuentran: la falta de integración y cooperación entre las partes interesadas (Thames, Lane. Schaefer 2017) de las organizaciones, por no tener un lenguaje en común, al existir muchas disciplinas con diferentes tipos de expertos, multiplicidad de tecnologías. Además de ataques, riesgos de seguridad y vulnerabilidades. La convergencia de las Tecnologías de la Información (TI) y las Tecnologías Operativas (TO), han venido a incrementar la problemática de integración en el desarrollo de proyectos en la Industria 4.0.

Se ha observado la falta de un marco normativo en el área de ciberseguridad en las organizaciones PYMEs, Industria 4.0. Para que la Industria 4.0 pueda alcanzar su máximo potencial se tienen que superar los problemas tradicionales de ciberseguridad juntos con los problemas propios de la Industria 4.0 (Thames, Lane. Schaefer 2017).

Se necesita tener un marco normativo integrado mínimo que ayude a delimitar alcances, funciones en las empresas, para que estas funciones y responsabilidad no queden sin poder ser rastreados en caso de un incidente relacionado con el acceso a los datos de manera no autorizada, y su trazabilidad no pueda ser reconocida al interior de las organizaciones.

1.4. OBJETIVOS

1.4.1. Objetivo general

Desarrollar una propuesta de un marco mínimo de ciberseguridad para la Industria 4.0/PYMEs, basado en el marco NIST CSF v1.1.(National Institute of Standards and Technology (NIST) 2018b), para ayudar a crear una cultura de valoración del riesgo.

1.4.2. Objetivos específicos

- Clasificar a la empresa de acuerdo con su tamaño para determinar el nivel de cumplimiento actual del modelo NIST CSF versión 1.1.
- Explorar formas para minimizar el riesgo de ataques de ciberseguridad por la implementación del modelo NIST CSF versión 1.1.
- Generar un modelo mínimo en base al NIST CSF v1.1.

1.5. HIPÓTESIS

La propuesta de un marco de ciberseguridad mínimo para las empresas PYMEs en el contexto de la Industria 4.0, basado en el marco NIST CSF v1.1 (National Institute of Standards and Technology (NIST) 2018b) ayudará a mejorar la postura de ciberseguridad para la reducción de ataques.

2. MARCO TEÓRICO

Para la elaboración del marco se realizó un análisis de la bibliografía para identificar el estado de la ciberseguridad en la Industria 4.0, y su entorno dentro del surgimiento de la 4ª revolución industrial, y la necesidad de las empresas para llevar a cabo su transformación digital para ubicar el desarrollo de este trabajo. De igual manera se identifica los estándares, y marcos de referencia que están usando las empresas para enfrentar los problemas de ciberseguridad. En relación con el contexto de México, se resumen algunos esfuerzos realizados al respecto.

La ciberseguridad en la Industria 4.0 ha llegado a ser esencial para el desarrollo de la industria en todos los sectores. El surgimiento de la Industria 4.0, de igual manera ha favorecido la convergencia de las tecnologías de información (TI) con las tecnologías operativas (TO), lo cual ha ayudado a hacer más grande los vectores de ataques dentro de la misma industria, razón por la cual es necesario que las empresas del sector refuercen su postura de ciberseguridad, para disminuir los ataques a sus activos más importantes.

2.1. LA 4ª REVOLUCIÓN INDUSTRIAL

Las revoluciones industriales que han sido consideradas hasta ahora son cuatro, Takakuwa (Takakuwa, Soemon. Veza, Ivica. Celar 2018), Kagermann et al (Kagermann, Henning. Wahlster, Wolfgang. Helbig 2013) resumen las cuatro etapas de revolución industrial de manera breve, como se muestra en la figura 1.

Algunos autores definen la 4ª Revolución Industrial como: "La Revolución Industrial se puede caracterizar por la integración entre Internet y los procesos productivos, con la ayuda de sensores más pequeños e inteligencia artificial aplicada a las máquinas" (Hamilton Ortiz 2020).

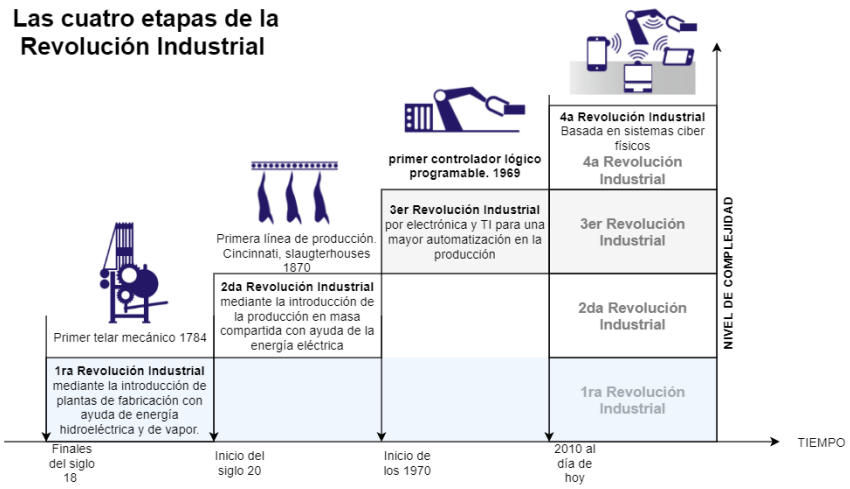


Figura 1. Cuatro etapas de la Revolución industrial
Traducida de (Takakuwa, Soemon. Veza, Ivica. Celar 2018), (Kagermann, Henning. Wahlster, Wolfgang. Helbig 2013)
Elaboración propia

2.2. INDUSTRIA 4.0

La Industria 4.0 puede considerarse como un caso especial de la tendencia de digitalización: esta es la implementación orientada a la práctica de tecnologías de la información avanzadas basadas en sistemas ciberfísicos y de análisis de datos, que están diseñadas para respaldar la individualización de la producción, aumentar la autonomía y la toma de decisiones.

Entre las tecnologías que han sido reconocidas como impulsoras de la Industria 4.0 se pueden mencionar: IoT, realidad aumentada, Analíticos de Big Data, computo en la nube, ciberseguridad, simulación, integración de sistemas, manufactura aditiva, robótica (Kumar, Vikas. Rezaei, Jafar. Akberdina, Victoria. Kuzmin 2021), sistemas ciber físicos (Kumar, S. V. Anil Bawge 2021) entre otras.

Según Jesús Hamilton Ortiz (Hamilton Ortiz 2020), el término Industria 4.0 apareció en 2011, establecido oficialmente por el gobierno alemán para referirse a un nuevo modelo de organización y control de la cadena de valor a través del ciclo de vida de un producto y a lo largo de los sistemas de fabricación, apoyado y posibilitado por las tecnologías de la información. Según Kumar (Kumar, S. V. Anil Bawge 2021),

La Industria 4.0 se presenta como un cambio global por la digitalización y automatización de cada parte de la empresa, así como del proceso de fabricación.

2.3. TRANSFORMACIÓN DIGITAL

De acuerdo con Vikas et al (Kumar, Vikas. Rezaei, Jafar. Akberdina, Victoria. Kuzmin 2021), la transformación digital ha permeado todas las áreas del desarrollo humano sociedad, industria, servicios, educación, y se encuentra en una etapa de desarrollo y transformación. Esto ha traído también nuevos retos que tienen que enfrentar la Industria 4.0/PYMEs, entre los que se encuentran el uso de nuevas herramientas del negocio, estandarización, inversiones, finanzas, ciberseguridad, y entender como la seguridad de la infraestructura, los procesos, personas, y sus comportamientos, interactúan.

2.4. CIBERSEGURIDAD

En la actualidad existen muchas definiciones sobre ciberseguridad, en la tabla 1, se pueden apreciar varias definiciones de organismos reconocidos mundialmente en el área de ciberseguridad, como: NIST, ITU, ISACA, Centro Nacional de Ciberseguridad del Reino Unido (Rashid, A., Chivers, H., Danezis, G., Lupu, E., & Martin 2019).

Para este trabajo vamos a considerar ciberseguridad de acuerdo con Gartner publicado en ISACA Journal (Rout 2015), y se define como: "La ciberseguridad abarca una amplia gama de prácticas, herramientas y conceptos relacionados estrechamente con seguridad de la tecnología operativa (TO) y de la información, la seguridad cibernética es un superconjunto de las prácticas incorporadas en la seguridad de TI, la seguridad de la información, seguridad de la tecnología operativa (TO) y seguridad ofensiva". En la figura 2 se pueden ver los conceptos descritos en la definición.

Tabla 1. Definiciones de ciberseguridad

CyBOK	Se refiere a la protección de los sistemas de información (hardware, software e infraestructura asociada), los datos en ellos y los servicios que brindan, del acceso no autorizado, daño o uso indebido. Esto incluye daños causados intencionalmente por el operador del sistema, o accidentalmente, como resultado de no seguir los procedimientos de seguridad (Rashid, A., Chivers, H., Danezis, G., Lupu, E., & Martin 2019).
ISACA	La ciberseguridad abarca una amplia gama de prácticas, herramientas y conceptos relacionados estrechamente con los de la seguridad de la tecnología operativa (TO) y de la información, la seguridad cibernética es un superconjunto de las prácticas incorporadas en la seguridad de TI, la seguridad de la información, seguridad de la tecnología operativa (OT) y seguridad ofensiva.(Rout 2015).
ITU	Definición de ciberseguridad, en referencia a ITU-T X.1205, resumen de ciberseguridad. (International Telecommunication Union (ITU) 2022). La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, garantías de seguridad, directrices, enfoques de gestión de riesgos, acciones, capacitación, mejores prácticas, garantías y tecnologías que se pueden utilizar para proteger el entorno cibernético y los activos de la organización y del usuario. Los activos de la organización y del usuario incluyen dispositivos informáticos conectados, personal, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y la totalidad de la información transmitida y/o almacenada en el entorno cibernético. La ciberseguridad se esfuerza por garantizar el logro y el mantenimiento de las propiedades de seguridad de la organización y los activos del usuario frente a los riesgos de seguridad relevantes en el entorno cibernético. Los objetivos generales de seguridad comprenden lo siguiente: • Disponibilidad. • Integridad, que puede incluir autenticidad y no repudio. • Confidencialidad.
NIST	Prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio (National Institute of Standards and Technology (NIST) n.d.).

Recopilación, traducción de (Rout 2015), (National Institute of Standards and Technology (NIST) n.d.), (International Telecommunication Union (ITU) 2022), (Rashid, A., Chivers, H., Danezis, G., Lupu, E., & Martin 2019)

Figura 2. Componentes de Ciberseguridad
(Traducido de Rout (Rout 2015))

La definición de ISACA junto con la definición de ITU se considera que incluyen de manera integral todos los conceptos necesarios para poder entender la definición de ciberseguridad de manera integral.

2.5. CIBERSEGURIDAD TERMINOLOGÍA

El estándar ISO/IEC 27000 define el vocabulario básico (International Organization for Standardization (ISO)/International Electrotechnical and (IEC) 2009). A continuación, se mencionan algunos de los términos más frecuentes dentro de la ciberseguridad, necesarios para comprender el contexto.

La ciberseguridad se encarga de proteger los activos de una organización de los ataques de los cibercriminales, estos activos dada su naturaleza pueden tener vulnerabilidades, las cuales puede ser explotadas por medio de un ataque, los profesionales de ciberseguridad tienen que poner controles (mecanismos de mitigación, salvaguardas, contramedidas), estos controles a su vez pueden contener otras vulnerabilidades que deben ser mitigadas. Una amenaza es una causa potencial de un incidente no deseado, el cual puede resultar en daños a un sistema u organización (activo). Por otro lado, el ataque, es un intento de destruir, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo. Un evento es la ocurrencia de un conjunto particular de circunstancias. Este evento en ocasiones se le conoce como incidente, o anomalía, es una forma que algunos profesionales de ciberseguridad utilizan para referirse a un ataque como una forma menos drástica del término ataque. Finalmente, riesgo es la combinación de la probabilidad de un evento, y sus consecuencias. En la figura 3, se muestra una relación de los términos de manera gráfica.

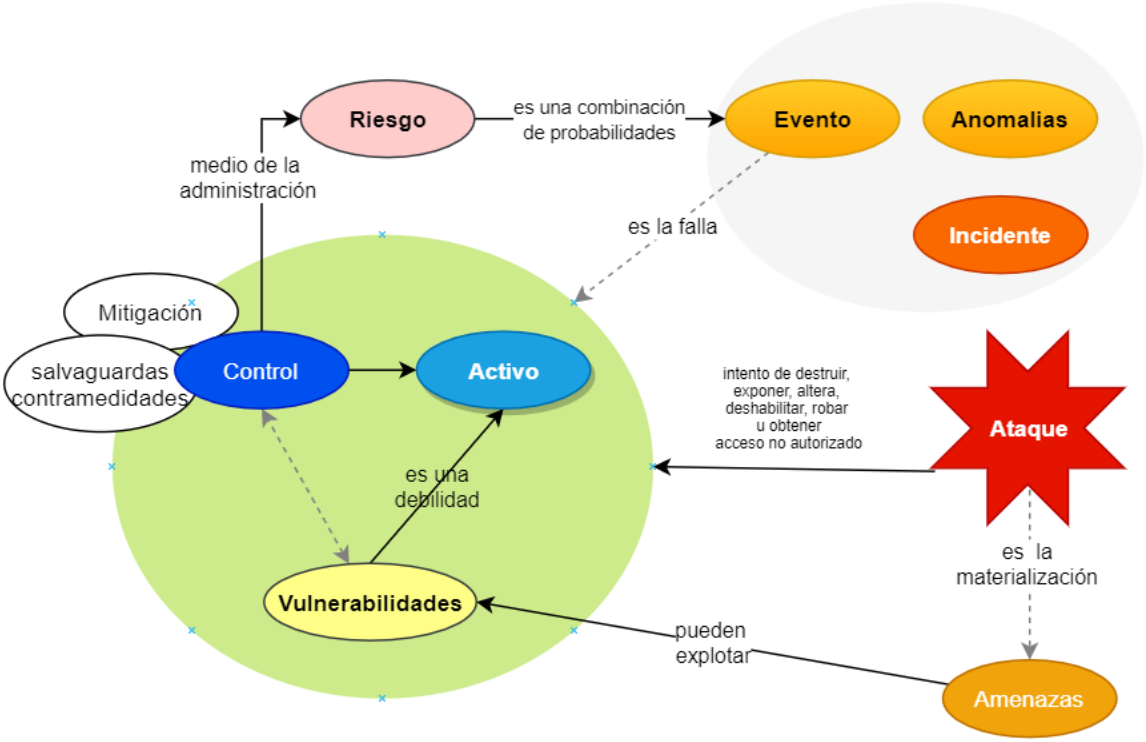


Figura 3. Terminología de ciberseguridad
Desarrollo propio basado en ISO27000 (International Organization for Standardization (ISO)/International Electrotechnical and (IEC) 2009)

2.6. ASPECTOS DE CIBERSEGURIDAD DE TI/TO PARA LA INDUSTRIA 4.0

Ampliando los términos de tecnología operativa (TO) y tecnologías de la información (TI) según Thames (Thames, Lane. Schaefer 2017) tenemos que:

La tecnología de operación (TO), se refiere a los sistemas tradicionales de hardware y software que se encuentran dentro de los entornos industriales. Algunos ejemplos incluyen controladores lógicos programables (PLC), sistemas de control distribuido (DCS) e interfaces hombre-máquina (HMI). Estos sistemas también se conocen como Sistemas de Control Industrial (ICS) porque controlan diversos procesos que ocurren dentro de un entorno industrial.

La tecnología de la información (TI) generalmente se refiere al software, los servidores, las computadoras personales, los teléfonos móviles y demás que comprenden el lado comercial de una organización.

La convergencia de TI y TO se relaciona con la interconexión de estos sistemas utilizando tecnologías de redes modernas como el protocolo de comunicaciones TCP/IP.

2.7. ESTÁNDARES DE SEGURIDAD

En las áreas de TI/TO existen una gran variedad de estándares enfocados en diferentes partes de los procesos, y componentes de la Industria 4.0. Unos se enfocan en TI, y otros en la parte de las TOs.

A continuación, se mencionan algunos de ellos.

Tecnologías de información. En el área de seguridad de la información se pueden encontrar los estándares de la familia ISO 27000, 27001, 27002.

ISACA promueve COBIT 2019, el Centro para la seguridad de Internet promueve los controles CIS v8 (Control Internet Security) (Center for Internet Security (CIS) 2021), para mejorar los programas de ciberseguridad de las empresas.

El NIST pública el documento SP 800-53 Rev. 5 (National Institute of Standards and Technology (NIST) 2020), "Para controlar los sistemas de información y las organizaciones para proteger las operaciones y los activos de la organización, las personas, otras organizaciones y la Nación de un conjunto diverso de amenazas y riesgos, incluidos ataques hostiles, errores humanos, desastres naturales, fallas estructurales, entidades de inteligencia extranjeras y riesgos de privacidad".

Tecnologías Operativas. La sociedad Internacional de Automatización (International Society of Automation) desarrolló una serie de estándares por el comité ISA99, (International Society of Automation (ISA). 2018) para mitigar las vulnerabilidades actuales y futuras en la automatización industrial, y los sistemas de control (IACS), ver tabla 2.

Existen otros estándares o regulaciones más específicos como el de la Corporación de confiabilidad eléctrica de América del Norte (NERC, North America Electric Reliability corporation) (North American Electric Reliability Corporation (NERC). 2022), publica los estándares de protección de infraestructura critica (CIP (Critical Infrastructure Protection)). Es una autoridad reguladora internacional sin fines de lucro cuya misión es asegurar la reducción efectiva y eficiente de los riesgos para la confiabilidad y seguridad de la red eléctrica.

Tabla 2. Serie de estándares IEC 62443

ISA-62443-4-2	Seguridad para sistemas de control y automatización industrial: requisitos técnicos de seguridad para componentes IACS	Proporciona los requerimientos técnicos de ciberseguridad para los componentes que conforman un IACS, específicamente los dispositivos integrados, los componentes de red, los componentes de host y las aplicaciones de software.
ISA/IEC 62443-3-3	Requisitos de seguridad del sistema y niveles de seguridad	Especifica las capacidades de seguridad que permiten que un componente mitigue las amenazas para un nivel de seguridad determinado sin la ayuda de contramedidas compensatorias.
ISA/IEC 62443-4-1	Requisitos del ciclo de vida del desarrollo de la seguridad del producto	Especifica los requisitos del proceso para el desarrollo seguro de productos utilizados en un IACS y define un ciclo de vida de desarrollo seguro para desarrollar y mantener productos seguros.
ISA/IEC 62443-3-2, (a)	Evaluación de riesgos de seguridad, partición del sistema y niveles de seguridad	Cada IACS presenta un riesgo diferente para una organización según las amenazas a las que está expuesta, la probabilidad de que surjan esas amenazas, las vulnerabilidades inherentes al sistema y las consecuencias si el sistema se viera comprometido. Además, cada organización que posee y opera un IACS tiene su propia tolerancia al riesgo.

(Traducida de (International Society of Automation (ISA). 2018))

ISA-95/PERA (Purdue Enterprise Reference Architecture (PERA)) (Rathwell 2004), proporciona una forma de dividir los componentes de la infraestructura de una empresa en componentes comprensibles. La empresa Cisco, junto con Rockwell Automation, y Panduit (Cisco. Rockwell. Panduit. 2022), desarrollaron una arquitectura de red enforcada a la infraestructura, llamada IDMZ Cisco, diseñada tomando en cuenta los principios de ciberseguridad.

2.8. NIST CYBERSECURITY FRAMEWORK

De acuerdo con NIST (National Institute of Standards and Technology (NIST) 2018a), "El Marco es una guía voluntaria, basada en estándares, pautas y prácticas existentes para que las organizaciones administren y reduzcan mejor el riesgo de seguridad cibernética. Además de ayudar a las organizaciones a gestionar y reducir los riesgos, se diseñó para fomentar las comunicaciones de gestión de riesgos y ciberseguridad entre las partes interesadas internas y externas de la organización." En el anexo A, se puede encontrar un resumen de los componentes del marco NIST CSF v1.1(National Institute of Standards and Technology (NIST) 2018b).

El marco se puede utilizar para:

- Revisión básica de prácticas de seguridad cibernética.
- Puede servir como base para un nuevo programa de seguridad cibernética o un mecanismo para mejorar un programa existente.
- Comunicación de requisitos de seguridad cibernética a las partes interesadas.
- Decisiones de compra.
- Identificación de oportunidades para referencias informativas nuevas o revisadas.

En lo relacionado a la creación y la mejora de un programa de ciberseguridad, el marco NIST CSF, establece siete pasos a considerar:

Paso 1: Priorización y alcance.

Paso 2: Orientación.

Paso 3: Crear un perfil actual.

Paso 4: Realizar una evaluación de riesgos.

Paso 5: Crear un perfil objetivo.

Paso 6: Determinar, analizar y priorizar brechas.

Paso 7: Implementar plan de acción

Para el desarrollo de este trabajo se va a considerar solo la parte de "Revisión básica de prácticas de seguridad cibernética". En lo referente al desarrollo de un programa de ciberseguridad, consideramos que estos siete pasos que tiene que seguir una empresa PYME que no cuenta con un programa de ciberseguridad es muy largo, y muy complicado. En la parte del desarrollo se va a continuar con este punto.

Como se puede apreciar existen muchos estándares enfocados en diferentes tecnologías tanto en TI, como en OT, lo cual hace complicado la convergencia, y el entendimiento de las partes involucradas para el desarrollo de proyectos, para las empresas PYMEs de la Industria 4.0.

El panorama en México en materia de ciberseguridad ha sido analizado por gobierno (ENCS), organismos nacionales (IFT, CANIETI [1]), internacionales (OEA, BID), y han coincidido que el desarrollo de una estrategia nacional de ciberseguridad basada en análisis de riesgos es lo más recomendable elaborar.

México al igual que otros países ha desarrollado una Estrategia Nacional de Ciberseguridad (ENCS) (Gobierno de la República Mexicana 2017), ayudado por la OEA a finales del año 2017. El Instituto Federal de Telecomunicaciones (IFT), se suma en 2018 a la ENCS para lograr los objetivos de la estrategia. Sin embargo, dice Patricio Garza (Garza 2021), "dicha estrategia no logró convertirse en un documento vinculante y menos en una verdadera política de Estado". Aunque esta estrategia no prospero continúa Garza, "fue el primer paso para posicionar el tema en la agenda del gobierno".

Fue hasta octubre del año 2021, cuando la Presidencia de la República, pública el documento, Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos. Después de analizar varios marcos (Gobierno de la República Mexicana. 2021), decide tomar como base para su desarrollo el NIST CSF v1.1, NIST 800-61, la Guía de Mejores Prácticas para la Gestión de Incidentes de ENISA (European Network and Information Security Agency).

Un estudio del Banco Interamericano de Desarrollo (BID) (Banco Interamericano de Desarrollo. Organización de Estados Americanos. 2020), y de la Organización de Estados Americanos (OEA) en el año 2020, cita "el presente estudio pone en evidencia que la región de América Latina y el Caribe aún no está suficientemente preparada para enfrentar los ataques que se producen en el ciberespacio", y recomienda que México debe enfocarse en mejorar el despliegue de estándares de ciberseguridad y controles técnicos.

Otro dato de interés es publicado por de igual manera el Índice Global de Ciberseguridad (International Telecommunication Union (ITU) 2020) publicado por la Unión Internacional de Comunicaciones (ITU), este tiene como objetivo ayudar a los países a identificar áreas de mejora en el campo de la seguridad cibernética y alentarlos a tomar medidas en esas áreas, en su reporte del año 2020 pone a México en el lugar número 56 de 182 países. Resultando áreas de oportunidad de mejora en el área de ciberseguridad para México.

Finalmente, en México con la entrada en vigor del Tratado de Libre Comercio entre México, Estados Unidos y Canadá (T-MEC) desde el 01 de julio del año 2020 (Secretaría de relaciones exteriores. 2020), incluye disposiciones en materia de ciberseguridad, En su Artículo 19.15: Ciberseguridad, que tiene que cumplir y es necesario consolidar para poder cumplir con este requerimiento.

3. PROCEDIMIENTO

Esta sección explica cómo se hace uso del marco NIST CSF v1.1 y los pasos utilizados para generar un Marco mínimo de ciberseguridad para PYMEs en el contexto de la Industria 4.0/PYME. Primero, se llevó a cabo una revisión bibliográfica de los temas relacionados con el trabajo a desarrollar. Los resultados de la búsqueda se utilizaron para el desarrollo de este trabajo, de igual forma se utilizaron las referencias y se incluyen las citas, donde es adecuado, y agregándose a la bibliografía.

Para llevar a cabo la propuesta, se seleccionó una empresa de la Industria 4.0 del ramo autopartes, ubicada en el parque industrial Apaseo el Grande en el Estado de Guanajuato. En particular se aplica la autoevaluación a la red empresarial. No se proporcionan datos específicos de la empresa por cuestiones de confidencialidad.

El marco NIST CSF v1.1, en su componente núcleo está formado de funciones, categorías y subcategorías y cada subcategoría tiene referencias informativas. Estas referencias corresponden a estándares reconocidos y aceptados en la industria de la seguridad. Entre los estándares propuestos se encuentran los siguientes: CIS CSC, COBIT5, ISA 62443, ISO/IEC 27000, NIST SP. De cada estándar y de acuerdo con cada categoría el marco propone el estándar y algunas de las cláusulas que aplican a cada subcategoría. Cada empresa tiene que seleccionar los estándares que aplican al sector y las cláusulas correspondientes. En la figura 4, se puede ver la subcategoría ID.AM-1, y la izquierda las referencias informativas.

Función	Categoría	Subcategoría	Referencias Informativas
IDENTIFICAR (ID)	Adminsitración de Activos (ID.AM)	ID.AM-1: Los dispositivos y sistemas físicos dentro de la organización están inventariados.	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5

Figura 4. Referencias informativas
Elaboración propia

Los criterios utilizados para la selección de las cláusulas en cada subcategoría se utilizaron como criterio de selección, el estándar que pertenece a la red

empresarial, la existencia del documento del estándar en la empresa, fuentes bibliográficas (Brumfield, Cynthia. Haugli 2022) entre otras; la experiencia del personal de la empresa (una persona) y la experiencia personal. Se estuvo revisando cada función, categoría y subcategoría para seleccionar los estándares y las cláusulas que aplican a cada subcategoría.

En la figura 5, se muestra de manera general el proceso:

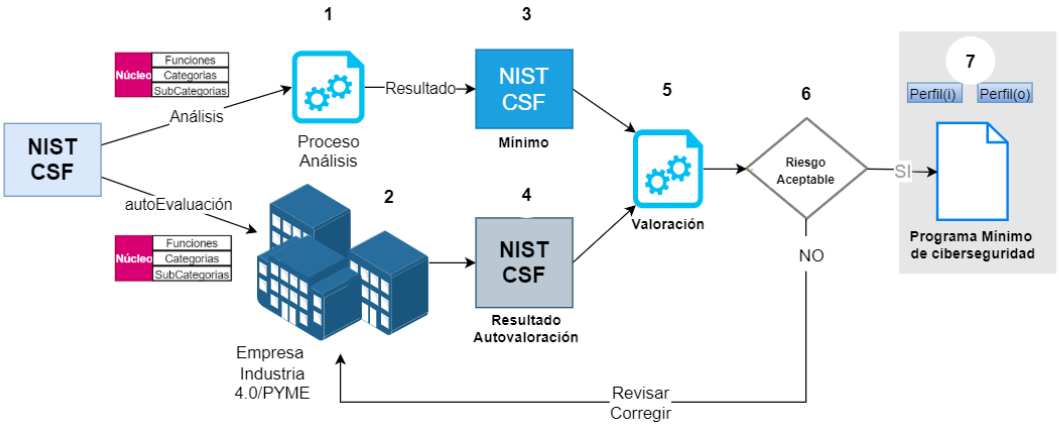


Figura 5. Procedimiento utilizado
Elaboración propia

A continuación, se muestran los pasos llevados a cabo para la elaboración de la propuesta del marco mínimo de ciberseguridad:

1. Se usa el componente núcleo del NIST CSF v1.1 como punto de entrada al proceso de análisis, en este proceso de análisis se van a utilizar como criterios de selección de las subcategorías la normatividad vigente a la industria en estudio, la bibliografía analizada y la experiencia propia.
2. En la parte de la empresa que se está analizando se le va a asignar el componente núcleo para que se realice una auto evaluación de las subcategorías correspondientes de acuerdo con el personal encargado del área de ciberseguridad.
3. Este proceso de análisis va a generar como resultado un marco mínimo. En la figura 5 se puede apreciar el proceso completo.
4. El resultado de esta autoevaluación se contrastó con el marco mínimo del punto 3.

5. Se realizó la valoración para el análisis de los resultados obtenidos.
6. En conjunto con la empresa del caso de estudio, se analizaron si estos resultados eran aceptables para la organización. En caso de no ser aceptables se iteró para revisar y volviendo a valorar, regresando al paso 2.
7. Al final de las iteraciones se generó el marco mínimo de ciberseguridad para la empresa del caso de estudio. Se obtuvo un perfil inicial (i) y un perfil objetivo (o/Propuesta), la diferencia entre Perfil (o) menos el Perfil (i) dio como resultado las subcategorías que se deben incluir en el programa de ciberseguridad de la empresa de caso de estudio.

4. RESULTADOS

Si no se tiene el conocimiento básico el marco NIST CSF v1.1, se recomienda leer el anexo A, para tener un conocimiento sobre el marco y para poder apreciar de manera clara los resultados obtenidos en este trabajo.

Para iniciar el proceso se utiliza una hoja de cálculo proporcionada por el marco NIST CSF v1.1 como referencia inicial, donde se incluyen todos los componentes de la parte del núcleo del marco figura 6: funciones (5), categorías (23), y subcategorías (108).

	Funtiones	Categorias	Subcategorias
1 Identificar-ID	1	6	29
2 Proteger-PR	1	6	39
3 Detectar-DE	1	3	18
4 Responder-RS	1	5	16
5 Recuperar-RC	1	3	6
	5	**23**	**108**

Figura 6. Resumen del componente núcleo del NIST SCF v1.1
Elaboración propia

Como parte del desarrollo se divide esta hoja en diferentes pestañas para que se pueda manejar de manera adecuada la información generada. En la figura 7, se muestran las pestañas que corresponden a cada función junto con sus categorías y subcategorías.

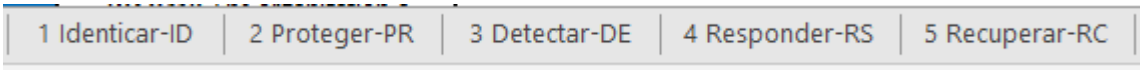


Figura 7. Pestañas correspondientes a las funciones del Marco NIST CSF v1.1
Elaboración propia

Por ejemplo: en la figura 8, se muestra el contenido de la función Identificar (ID), tiene como categoría Gestión de Activos (ID.AM), y sus correspondientes subcategorías cada subcategoría corresponde a una actividad de ciberseguridad que se tiene que evaluar.

				Nivel de Implementación (0,1,2,3,4)		1er Iteración
Función	Categoría	Subcategoría	Perfil Objetivo Propuesta	Perfil Inicial Perfil Actual	GAP	Empresa Target
IDENTIFICAR (ID)	Gestión de activos (ID.AM)	ID.AM-1	4	3	1	4
		ID.AM-2	4	0	4	2
		ID.AM-3	4	0	4	2
		ID.AM-4	4	4	0	4
		ID.AM-5	4	3	1	4
		ID.AM-6	3	3	0	4

Figura 8. Descripción función Identificar-categoría Gestión Activos-Subcategorías Marco NIST CSF v1.1.
Elaboración propia

A continuación, se define el contenido de cada una de las columnas que contiene cada una de las funciones.

Propuesta (Perfil objetivo).

Este valor indica el nivel que se propone para la implementación de cada una de las subcategorías. El valor se propone de acuerdo con las referencias informativas propuestas por el marco de referencias NIST CSF v1.1. Este valor se obtiene revisando los estándares propuestos para cada subcategoría, y solo se selecciona los que aplican para este caso de estudio.

Perfil actual (Perfil inicial).

Este valor se obtuvo de la autoevaluación realizada por el personal de la empresa del caso de estudio. El personal a cargo selecciona el valor para cada subcategoría. Se apoyó en la determinación sobre conceptos mencionados en cada categoría, el nivel de implementación lo determinó el encargado del área.

GAP

Para la determinación del GAP se utiliza la siguiente formula:

Propuesta – Perfil actual …… (1)

Para los resultados del GAP, se propone lo siguiente en la tabla 3:

Tabla 3. GAP, resultados

Resultado	Descripción	Observaciones
Cero (0)	El valor de propuesta y el valor del perfil actual resultaron iguales.	No se requiere implementar controles de seguridad.
Número positivo (1~4)	El valor de propuesta es mayor que el valor de la autoevaluación.	Se tiene que valorar si desea quedarse en ese nivel de implementación, o se desea implementar un control de seguridad para mitigar el riesgo. Si no desea llevarlo al nivel sugerido se debe documentar su justificación y ponerlo como un riesgo aceptado, por así convenir a la empresa.
Número negativo (-1) ~ (-4)	El valor de la propuesta fue menor que el valor de la autoevaluación.	Indica que el nivel de implementación de la subcategoría está arriba de la propuesta. No es necesario modificar ningún control.

Elaboración propia

Target

Este valor es el resultado de la primera iteración. Este valor lo determinó la empresa como un valor que desea alcanzar para la mejora de su postura de ciberseguridad. Este valor se puede mejorar en relación con el GAP encontrado. Si la empresa no desea mejorar el GAP se debe quedar establecido por escrito que la mejora no es conveniente para la empresa por el costo beneficio de la inversión en la implementación y se acepta ese nivel de riesgo encontrado. Ver tabla 4.

Tabla 4. Target, resultados

Target	Descripción
Número positivo (0~4)	El perfil actual se debe incrementar. La empresa debe valorar hasta que nivel desea incrementarlo de acuerdo a las recomendaciones de cada subcategoría. Si no desea llevarlo al nivel sugerido se debe documentar su justificación y ponerlo como un riesgo aceptado, por así convenir a la empresa.

Elaboración propia

Gráficas

Se puede apreciar de manera visual cada una de las categorías y subcategorías, y cuál de ellas está más alejada del valor objetivo (target). Esta diferencia le sirve a la empresa para determinar si desea invertir en la implementación de los controles de ciberseguridad, o aceptar el riesgo de no implementar nada porque

la inversión resultante es más cara que lo que el valor de la perdida en caso de un incidente de ciberseguridad.

Barras

Muestra los valores de la Propuesta, El perfil Actual, el GAP, y el Target. De manera gráfica se puede ver cuando el valor de la Propuesta es superior al valor del Perfil actual para cada una de las funciones, y sus categorías junto con sus subcategorías. De igual forma se puede ver el valor del Target y la diferencia actual con el perfil actual.

Radar

Grafica el valor de la Propuesta, el Perfil Actual. Esta gráfica apoya para percibir de manera clara cuando el valor de la Propuesta es superior al valor del Perfil actual.

Perfil actual y Perfil objetivo

A continuación, se muestran los resultados de las gráficas de cada función junto son sus categorías y sus correspondientes subcategorías. Se hacen las explicaciones correspondientes donde se tiene que valorar si la empresa tiene que verificar si se acepta el nivel de riesgo. Si el nivel de riesgo se acepta se tiene que dejar por escrito la justificación al respecto. Los valores resultantes en cada función formarán el perfil actual y el perfil objetivo.

Función Identificar

La figura 9 muestra el concentrado de las subcategorías que conforman la función Identificar. Aquí se puede ver la diferencia entre el perfil objetivo (propuesta) y el valor del Inicial.

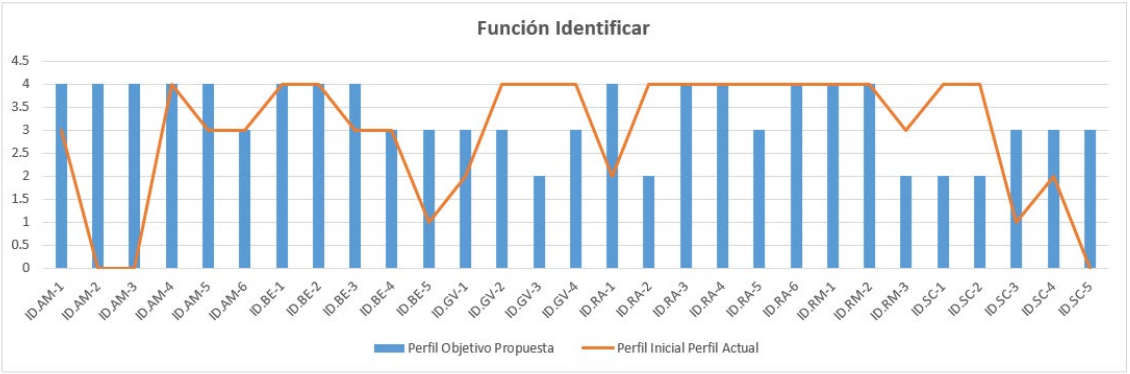


Figura 9. Descripción función: Identificar. Categorías-subcategorías
Elaboración propia

La figura 10 muestra el detalle de cada la categoría Gestión de Activos. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de radar, puede ver de ovalo de color donde ver el valor de cero del perfil actual, contra el valor de 4 de la propuesta.

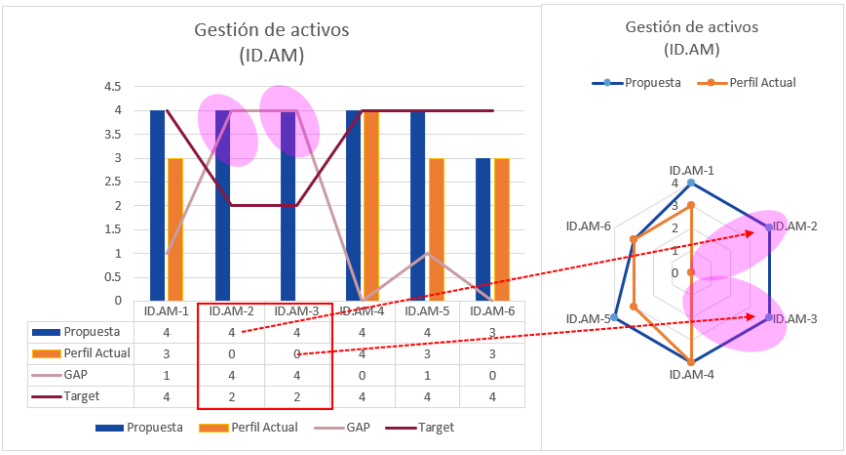


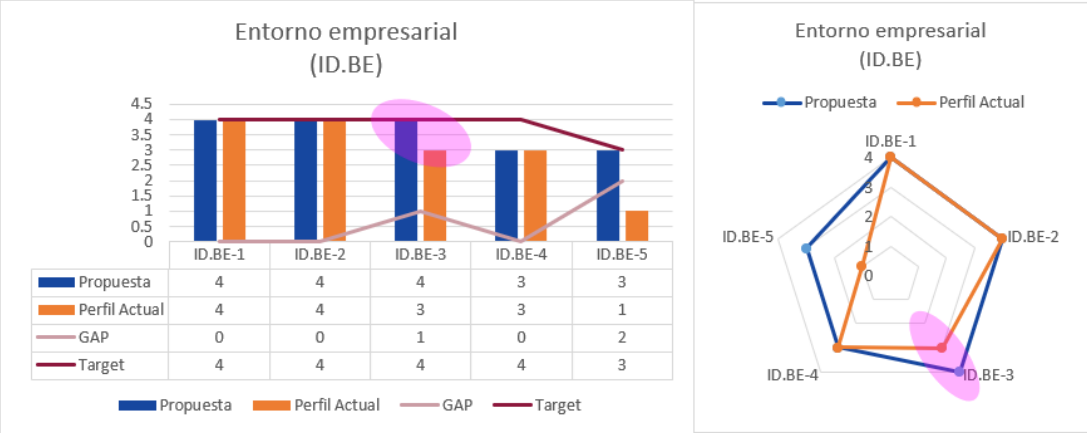
Figura 10. Descripción función: Identificar. Categoría: Gestión activos-subcategorías
Elaboración propia

Las subcategorías ID.AM-2, ID.AM-3 tienen un perfil actual menor a la propuesta. La empresa tiene que valorar si acepta ese nivel de riesgo.

Recomendación: "Para determinar si la empresa acepta este nivel de riesgo o no, se deben consultar las referencias de los estándares que aplican a esta subcategoría. Si no desea llevarlas al nivel sugerido se debe documentar su justificación y ponerlo como un riesgo aceptado, por así convenir a la empresa".

Para las gráficas restantes se hace la misma recomendación para todas las subcategorías donde el perfil actual es menor a la propuesta.

La figura 11 muestra el detalle de cada la categoría Entorno Empresarial. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de radar, puede ver de ovalo de color donde ver el valor de tres del perfil actual, contra el valor de 4 de la propuesta.

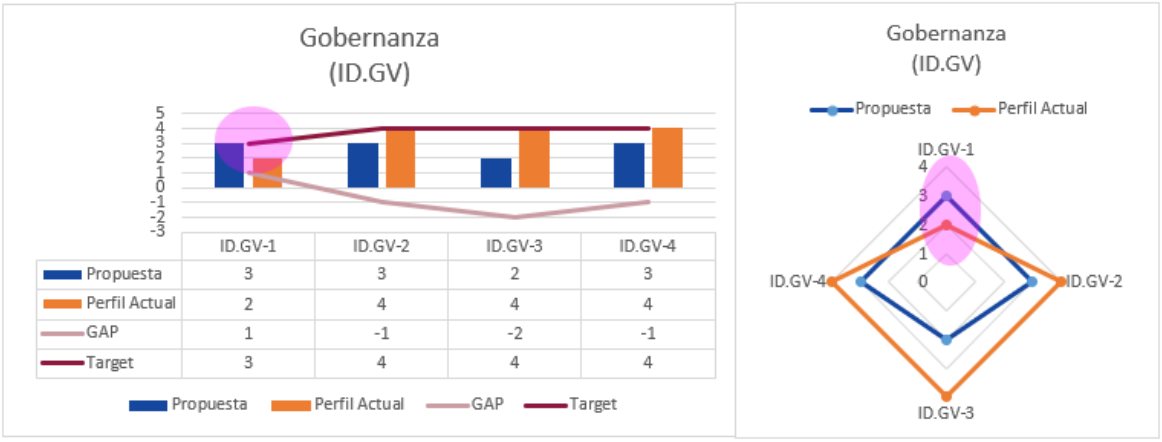


	ID.BE-1	ID.BE-2	ID.BE-3	ID.BE-4	ID.BE-5
Propuesta	4	4	4	3	3
Perfil Actual	4	4	3	3	1
GAP	0	0	1	0	2
Target	4	4	4	4	3

Figura 11. Descripción función: Identificar. Categoría: Entorno empresarial-subcategorías
Elaboración propia

La subcategoría ID.BE-3, tiene un perfil actual 3 menor a la propuesta. La empresa tiene que valorar si acepta ese nivel de riesgo.

La figura 12 muestra el detalle de cada la categoría Entorno Empresarial. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de radar, puede ver de ovalo de color donde ver el valor de tres del perfil actual, contra el valor de 3 de la propuesta.

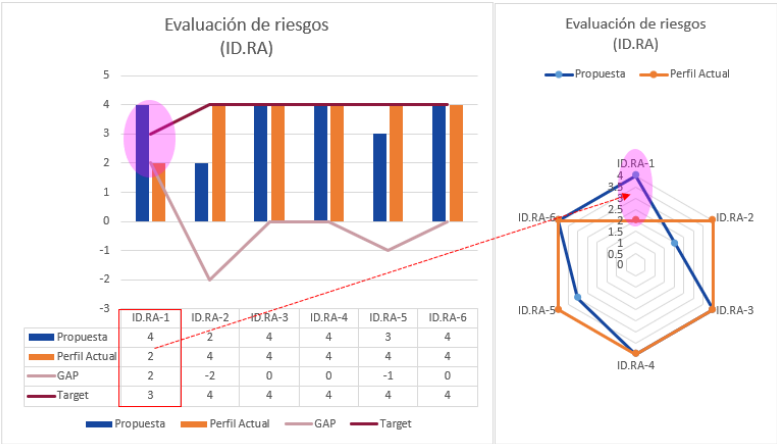


	ID.GV-1	ID.GV-2	ID.GV-3	ID.GV-4
Propuesta	3	3	2	3
Perfil Actual	2	4	4	4
GAP	1	-1	-2	-1
Target	3	4	4	4

Figura 12. Descripción función: Identificar. Categoría: Gobernanza-subcategorías
Elaboración propia

La subcategoría ID.GV-1, tiene un perfil actual 2 menor a la propuesta de 3. La empresa tiene que valorar si acepta ese nivel de riesgo.

La figura 13 muestra el detalle de cada la categoría Evaluación de Riesgo. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de radar, puede ver de ovalo de color donde ver el valor de dos del perfil actual, contra el valor de 4 de la propuesta.



	ID.RA-1	ID.RA-2	ID.RA-3	ID.RA-4	ID.RA-5	ID.RA-6
Propuesta	4	2	4	4	3	4
Perfil Actual	2	4	4	4	4	4
GAP	2	-2	0	0	-1	0
Target	3	4	4	4	4	4

Figura 13. Descripción función: Identificar. Categoría: Evaluación de riesgos-subcategorías
Elaboración propia

La subcategoría ID.RA-1, tiene un perfil actual 2 menor a la propuesta de 4. La empresa tiene que valorar si acepta ese nivel de riesgo.

La figura 14 muestra el detalle de cada la categoría Estrategia de Gestión de Riesgos. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En esta gráfica la propuesta y el perfil actual son igual, o el perfil actual es superior y no se requiere ninguna modificación.

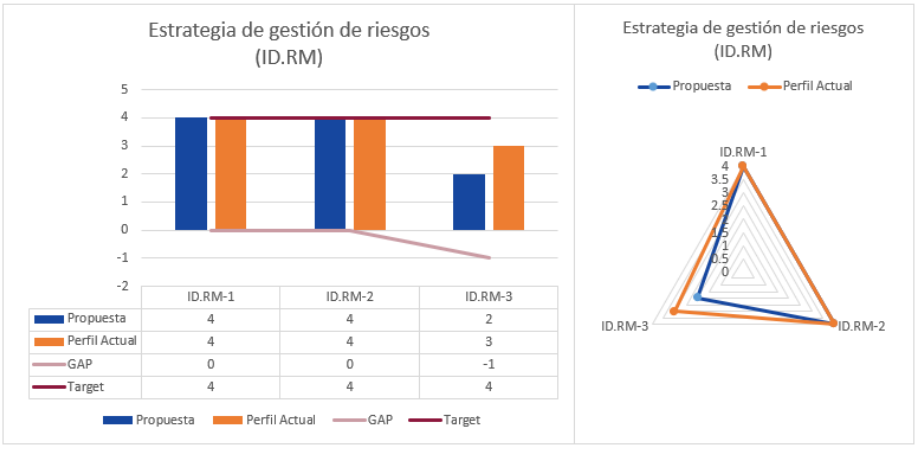


Figura 14. Descripción función: Identificar. Categoría: estrategia de gestión de riesgos-subcategorías
Elaboración propia

La figura 15 muestra el detalle de cada la categoría Gestión de Riesgo de la Cadena de Suministros. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de radar, puede ver de ovalo de color donde ver el valor de 1 del perfil actual, contra el valor de 3 de la propuesta para la subcategoría ID.SC-3, y la diferencia en la subcategoría ID.SC-4. La empresa tiene que valorar si acepta ese nivel de riesgo.

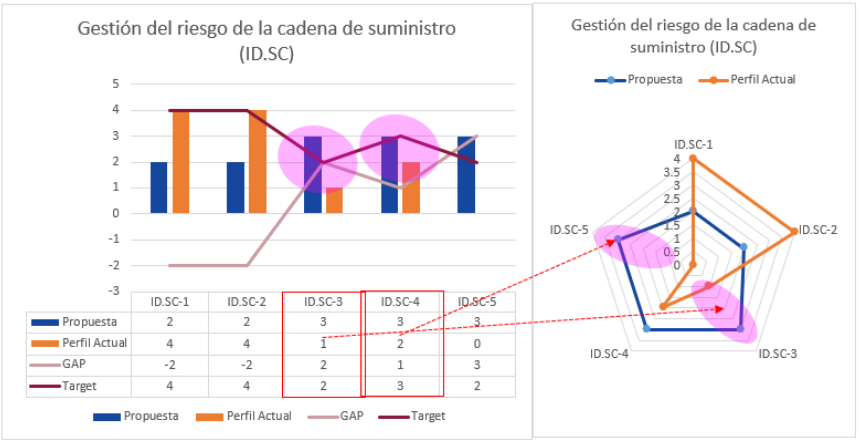


Figura 15. Descripción función Identificar-categoría Gestión Activos-subcategorías marco NIST CSF v1.1
Elaboración propia

Función Proteger

La figura 16 muestra el concentrado de las subcategorías que conforman la función Proteger. Aquí se puede ver la diferencia entre el perfil objetivo (propuesta) y el valor del Inicial. Los puntos donde el perfil actual es menor al perfil objetivo son las subcategorías a revisar. Las subcategorías donde el perfil objetivo es menor al perfil actual también se pueden analizar para determinar las diferencias.

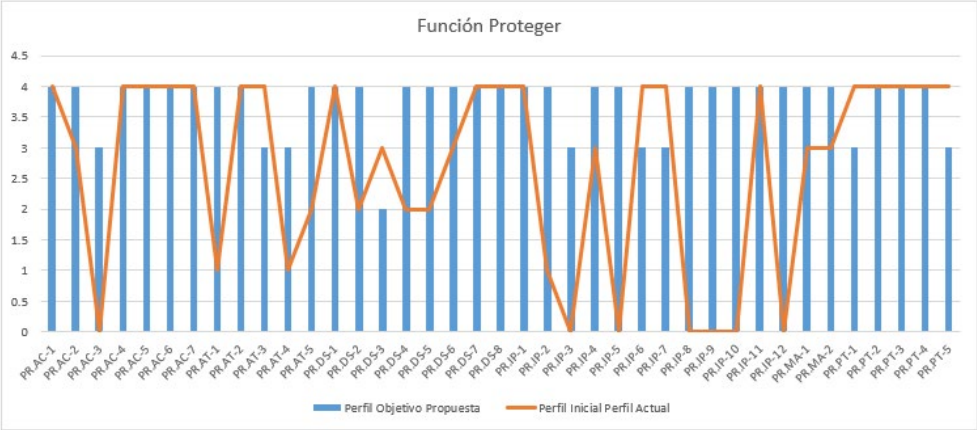


Figura 16. Descripción función: Proteger. Categorías-subcategorías
Elaboración propia

La figura 17 muestra el detalle de cada la categoría Gestión de Identidad. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de radar, puede ver de ovalo de color donde ver el valor del perfil actual PR.SC-3, es menor al valor de la propuesta.

La empresa tiene que valorar si acepta ese nivel de riegos. Para determinar si la empresa acepta este nivel de riesgo o no, debe consultar las referencias de los estándares que aplican a esta categoría. Si no desea llevarla al nivel sugerido se debe documentar su justificación y ponerlo como un riesgo aceptado, por así convenir a la empresa. Esta observación aplica para todas las demás categorías y subcategorías donde corresponda.

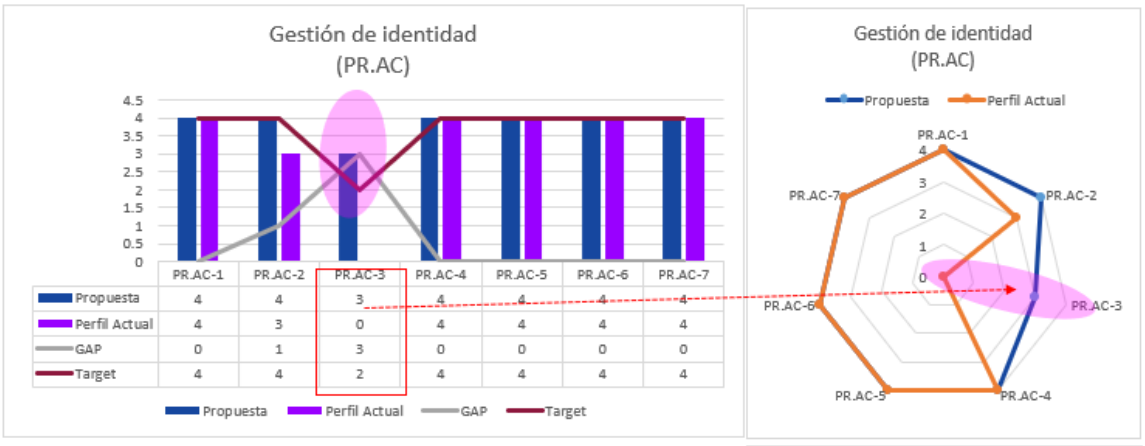


Figura 17. Descripción función: Proteger. Categoría: Gestión Identidad-subcategorías
Elaboración propia

La figura 18 muestra el detalle de cada la categoría Concientización y capacitación. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de radar, puede ver de ovalo de color donde ver el valor del perfil actual PR.AT-1, 4, y 5, es menor al valor de la propuesta.

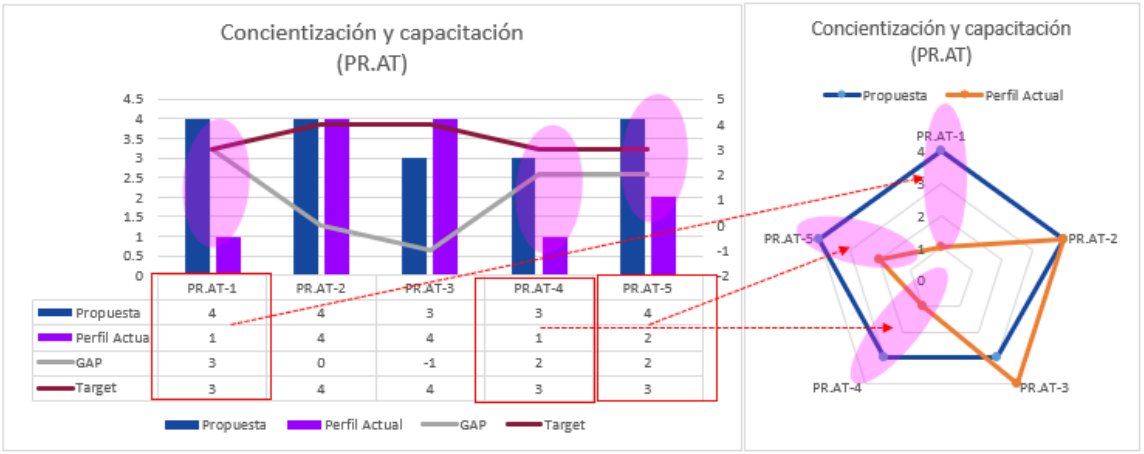


Figura 18. Descripción función: Proteger. Categoría: Concientización y capacitación-subcategorías
Elaboración propia

La figura 19 muestra el detalle de cada la categoría Seguridad de Datos. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de radar, puede ver de ovalo de color donde ver el valor del perfil actual para las subcategorías PR.DS-2, 4, 5, y 6 son menores al valor de la propuesta.

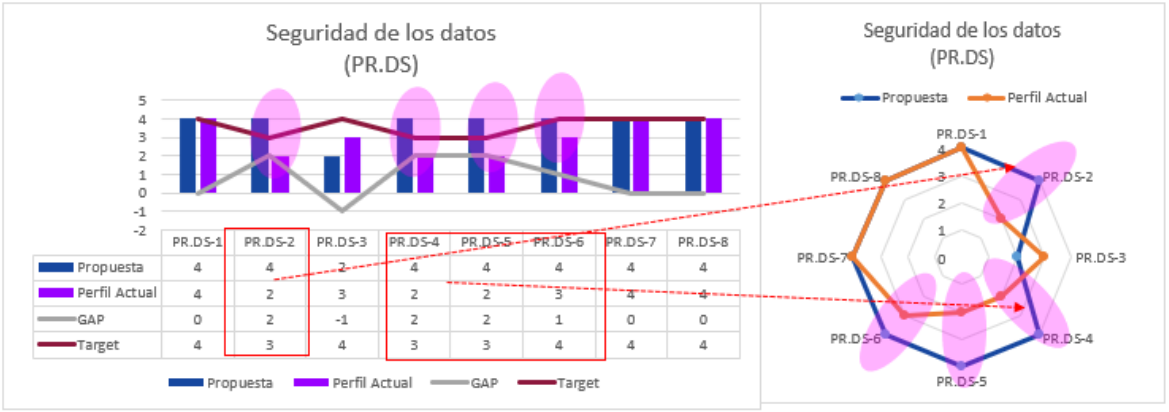


Figura 19. Descripción función: Proteger. Categoría: Seguridad de datos-subcategorías
Elaboración propia

La figura 20 muestra el detalle de cada la categoría Procesos y procedimientos de Protección de la Información. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de radar, puede ver de ovalo de color donde ver el valor del perfil actual para las subcategorías PR.IP-2, 4, 8, 9, 10 son menores al valor de la propuesta.

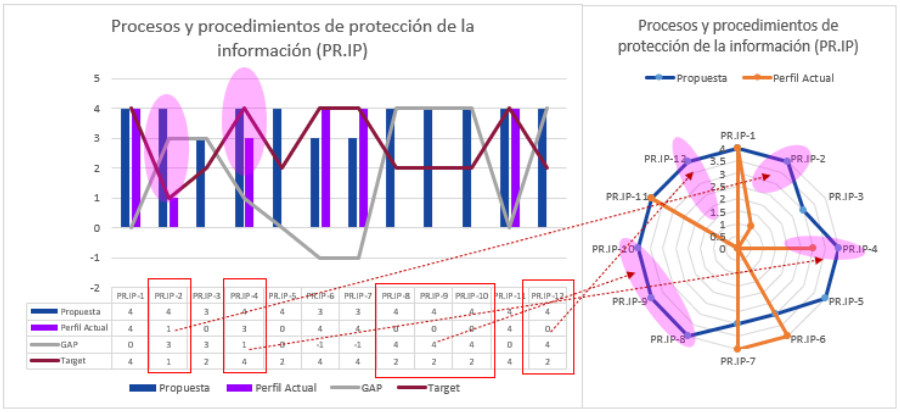


Figura 20. Descripción función: Proteger. Categoría: Procesos y procedimientos de protección de la Información-subcategorías
Elaboración propia

La figura 21 muestra el detalle de la categoría Mantenimiento. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de barras se puede ver que el valor del perfil objetivo es mayor que la propuesta. No es necesario realizar modificaciones a los controles de seguridad.

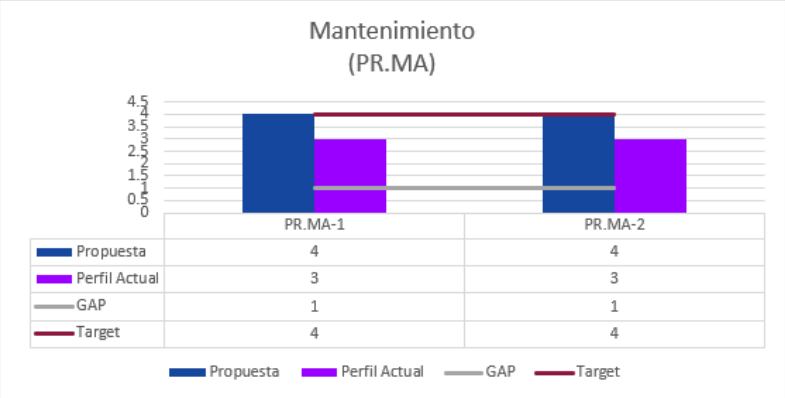


Figura 21. Descripción función: Proteger. Categoría: Mantenimiento-subcategorías
Elaboración propia

La figura 22 muestra el detalle de la categoría Tecnología de Protección. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de barras se puede ver que el valor del perfil objetivo es mayor o igual que la propuesta. No es necesario realizar modificaciones a los controles de seguridad.

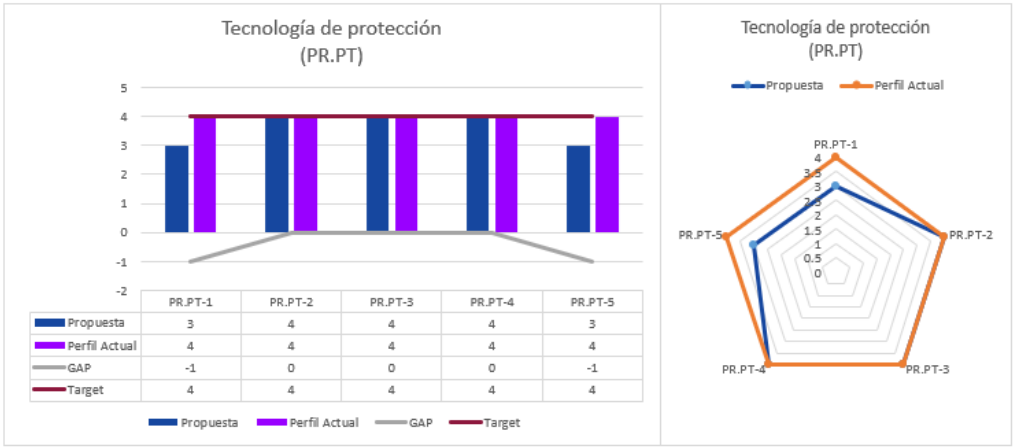


Figura 22. Descripción función: Proteger. Categoría: Tecnología de Protección-subcategorías
Elaboración propia

Función Detectar

La figura 23 muestra el concentrado de las subcategorías que conforman la función Detectar. Aquí se puede ver la diferencia entre el perfil objetivo (propuesta) y el valor del Inicial. Los puntos donde el perfil actual es menor al perfil objetivo son las

subcategorías a revisar. Las subcategorías donde el perfil objetivo es menor al perfil actual también se pueden analizar para determinar las diferencias.

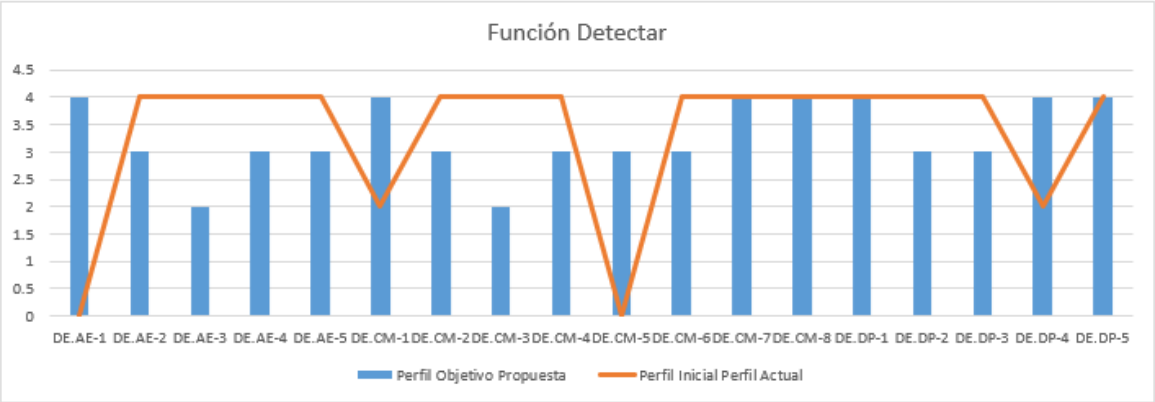


Figura 23. Descripción función: Detectar. Categorías-subcategorías
Elaboración propia

La figura 24 muestra el detalle de la categoría Anomalías y Eventos. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de barras se puede ver que el valor del perfil objetivo es mayor o igual que la propuesta en la subcategoría DE.AE-1. En las demás subcategorías el perfil actual es mayor que el perfil objetivo. No es necesario realizar modificaciones a los controles de seguridad.

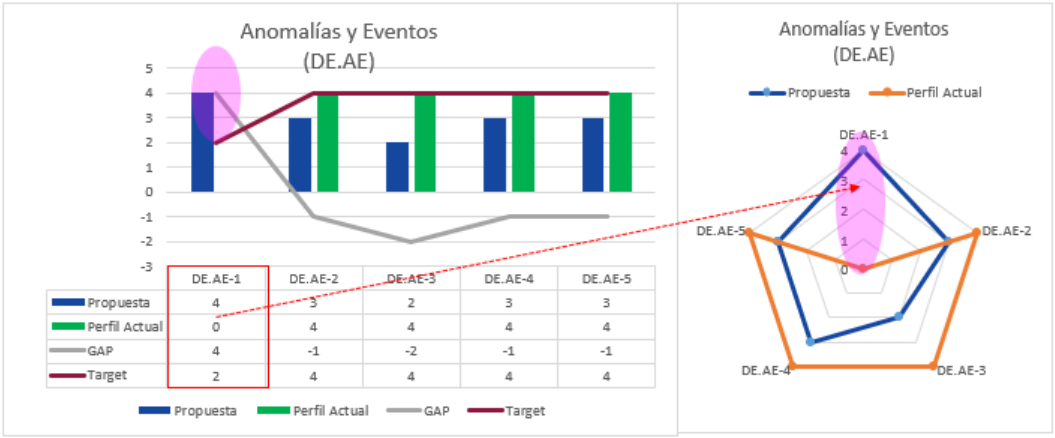


Figura 24. Descripción función: Detectar. Categoría: Anomalías y Eventos-subcategorías
Elaboración propia

La subcategoría DE.AE-1, tiene un target menor a la propuesta, la empresa tiene que valorar si acepta ese nivel de riegos. Para determinar si la empresa acepta este nivel de riesgo o no, debe consultar las referencias de los estándares que aplican

a esta categoría. Si no desea llevarla al nivel sugerido se debe documentar su justificación y ponerlo como un riesgo aceptado, por así convenir a la empresa.

La figura 25 muestra el detalle de la categoría Monitoreo continuo de la Seguridad. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de barras se puede ver que el valor del perfil objetivo es mayor o igual que la propuesta en la subcategoría DE.CM-1 y 5. En las demás subcategorías el perfil actual es mayor que el perfil objetivo. No es necesario realizar modificaciones a los controles de seguridad.

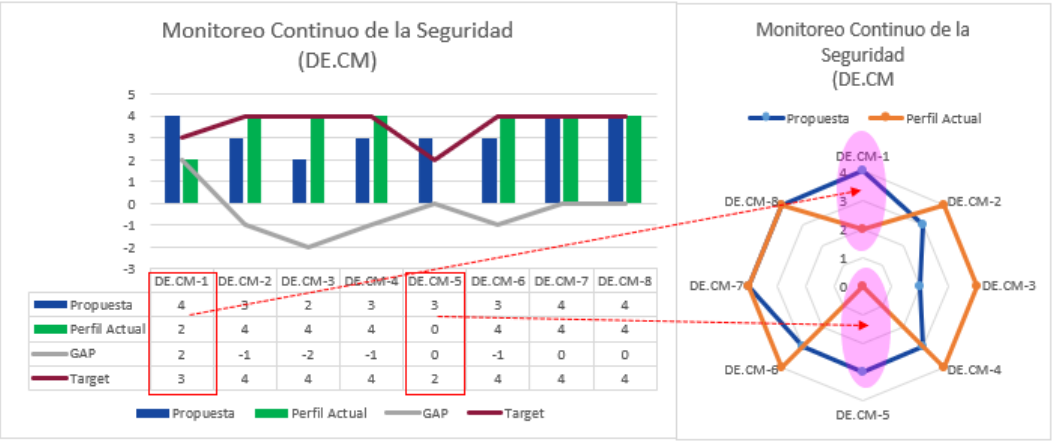


Figura 25. Descripción función: Detectar. Categoría: Monitoreo de la Seguridad-subcategorías
Elaboración propia

Las subcategorías DE.CM-1, DE.CM-5 tienen un target menor a la propuesta, la empresa tiene que valorar si acepta ese nivel de riegos. Para determinar si la empresa acepta este nivel de riesgo o no, debe consultar las referencias de los estándares que aplican a esta categoría. Si no desea llevarla al nivel sugerido se debe documentar su justificación y ponerlo como un riesgo aceptado, por así convenir a la empresa.

La figura 26 muestra el detalle de la categoría Procesos de Detección. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de barras se puede ver que el valor del perfil objetivo es mayor o igual que la propuesta en la subcategoría DE.DP-4. En las demás subcategorías el perfil

actual es mayor o igual que el perfil objetivo. No es necesario realizar modificaciones a los controles de seguridad.

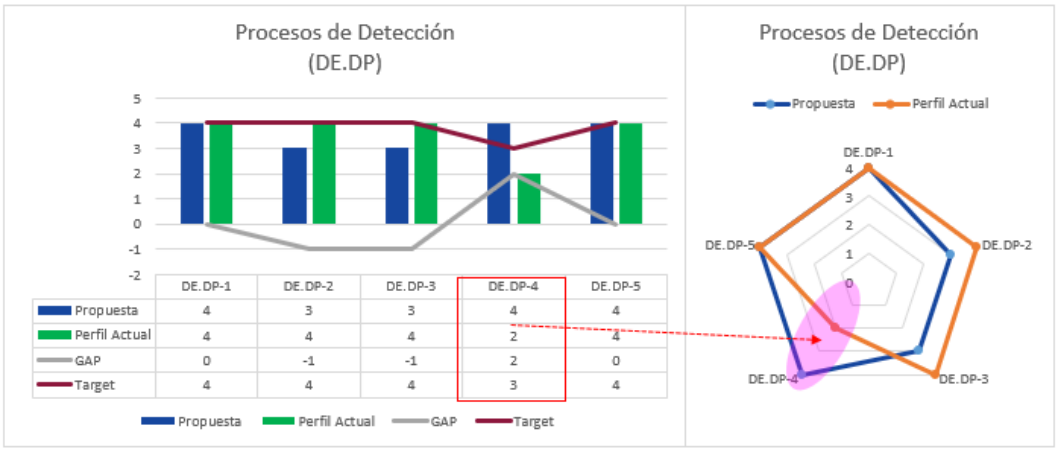


Figura 26. Descripción función: Detectar. Categoría: Procesos de Detección-subcategorías
Elaboración propia

La subcategoría DE.DP-4, tiene un target menor a la propuesta, la empresa tiene que valorar si acepta ese nivel de riegos. Para determinar si la empresa acepta este nivel de riesgo o no, debe consultar las referencias de los estándares que aplican a esta categoría. Si no desea llevarla al nivel sugerido se debe documentar su justificación y ponerlo como un riesgo aceptado, por así convenir a la empresa.

Función Responder

La figura 27 muestra el concentrado de las subcategorías que conforman la función Responder. Aquí se puede ver la diferencia entre el perfil objetivo (propuesta) y el valor del Inicial. Los puntos donde el perfil actual es menor al perfil objetivo son las subcategorías a revisar. Las subcategorías donde el perfil objetivo es menor al perfil actual también se pueden analizar para determinar las diferencias.

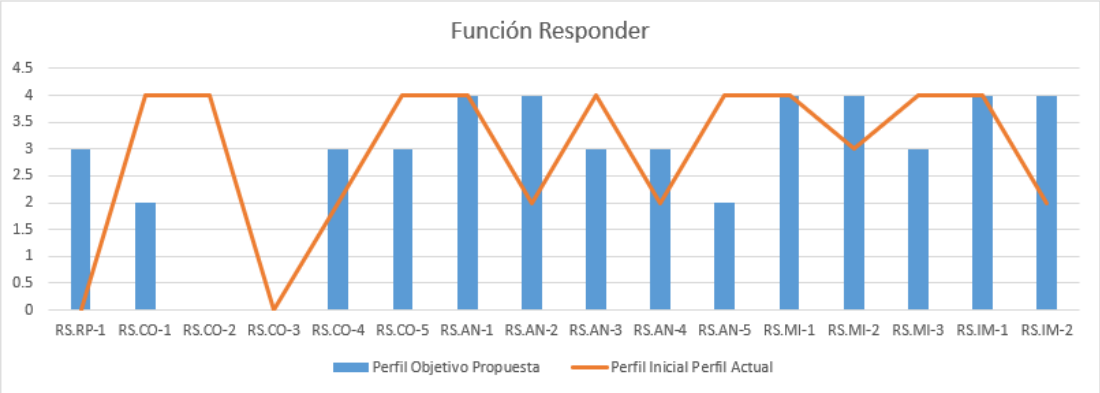


Figura 27. Descripción función: Responder. Categorías -subcategorías
Elaboración propia

Las siguientes gráficas tienen el mismo comportamiento que ya se ha mencionada anteriormente. Se recomienda revisar aquellas donde el perfil objetivo es mayor que el perfil actual y determinar si se va a implementar controles de seguridad o se va a dejar el mismo nivel y documentar como un riesgo aceptado, figura 28.

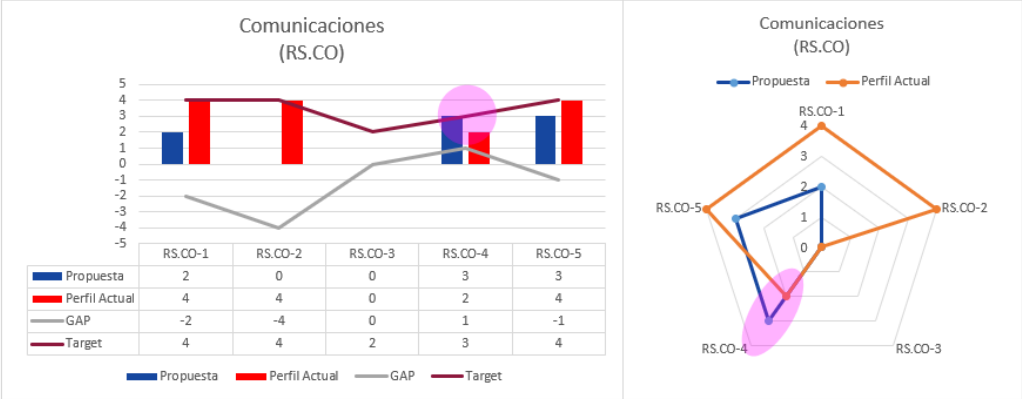


Figura 28. Descripción función: Responder. Categoría: Comunicaciones-subcategorías
Elaboración propia

La figura 29 muestra el detalle de la categoría Análisis. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de barras se puede ver que el valor del perfil objetivo es mayor o igual que la propuesta en la subcategoría RS.AN-2 y RS.AN-4. En las demás subcategorías el perfil actual es mayor o igual que el perfil objetivo. No es necesario realizar modificaciones a los controles de seguridad.

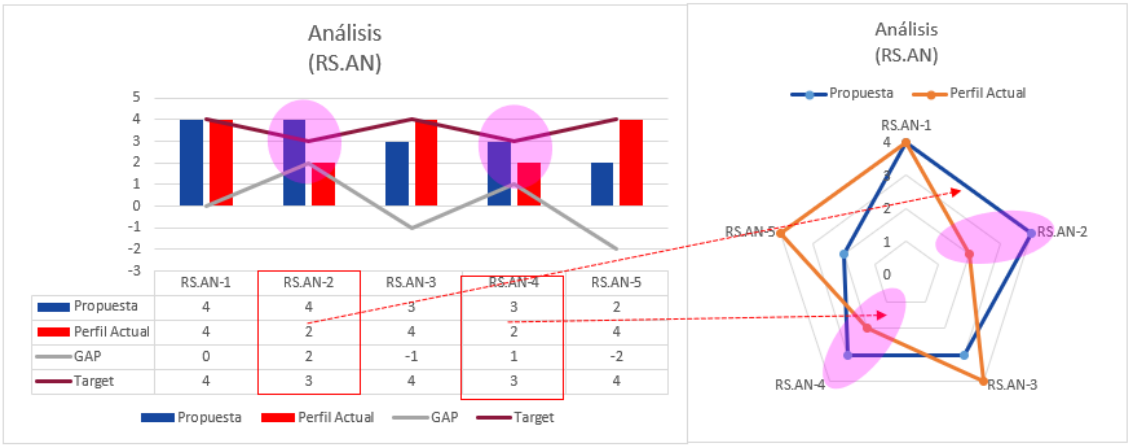


Figura 29. Descripción función: Responder. Categoría: Análisis-subcategorías
Elaboración propia

La subcategoría RS.AN-2, y RS.AN-4 tienen un perfil actual menor a la propuesta. La empresa tiene que valorar si acepta ese nivel de riegos. Para determinar si la empresa acepta este nivel de riesgo o no, debe consultar las referencias de los estándares que aplican a esta categoría. Si no desea llevarla al nivel sugerido se debe documentar su justificación y ponerlo como un riesgo aceptado, por así convenir a la empresa.

La figura 30 muestra el detalle de la categoría Mitigación. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de barras se puede ver que el valor del perfil objetivo es mayor o igual que la propuesta en la subcategoría RS.MI-1. En las demás subcategorías el perfil actual es mayor o igual que el perfil objetivo. No es necesario realizar modificaciones a los controles de seguridad.

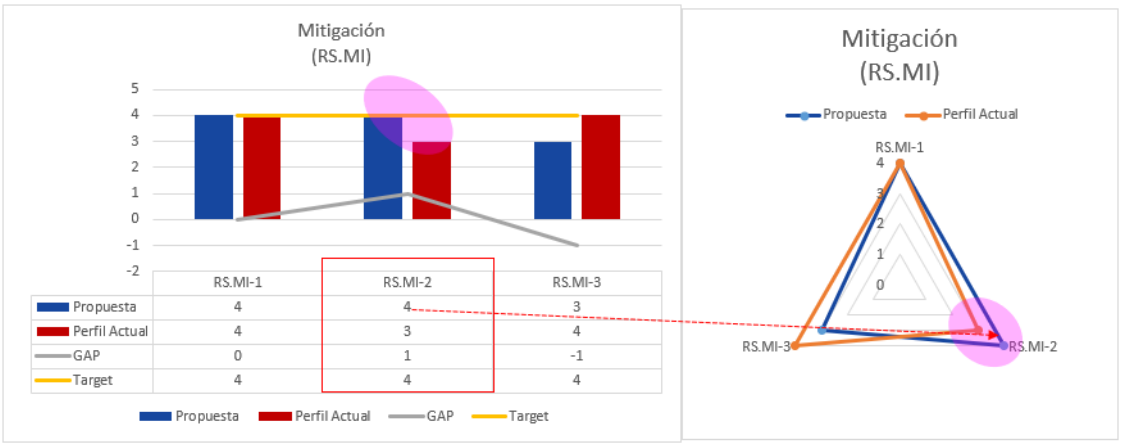


Figura 30. Descripción función: Responder. Categoría: Mitigación-subcategorías
Elaboración propia

La figura 31 muestra el detalle de la categoría Mejoras. Aquí se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de barras se puede ver que el valor del perfil objetivo es mayor que el perfil actual en la subcategoría RS.IM-2. En las demás subcategorías el perfil actual es mayor o igual que el perfil objetivo. No es necesario realizar modificaciones a los controles de seguridad.

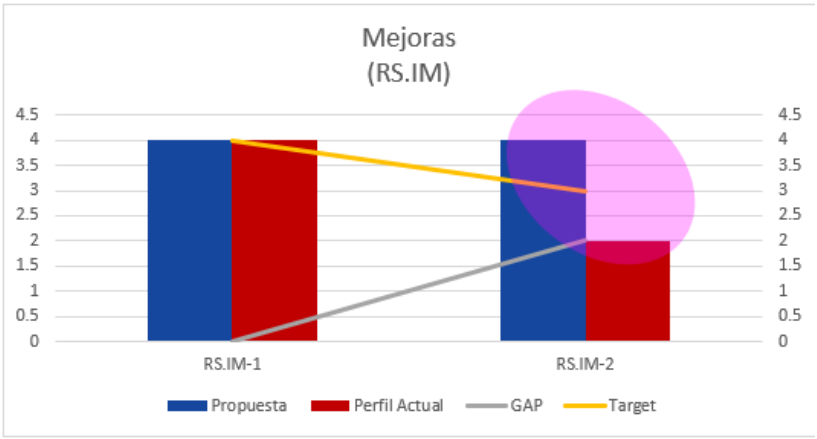


Figura 31. Descripción función: Responder. Categoría: Mitigación-subcategorías
Elaboración propia

Función Recuperar

La figura 32 muestra el concentrado de las subcategorías que conforman la función Recuperar. Aquí se puede ver la diferencia entre el perfil objetivo (propuesta) y el valor del Inicial. Los puntos donde el perfil actual es menor al perfil objetivo son las

subcategorías a revisar. Las subcategorías donde el perfil objetivo es menor al perfil actual también se pueden analizar para determinar las diferencias.

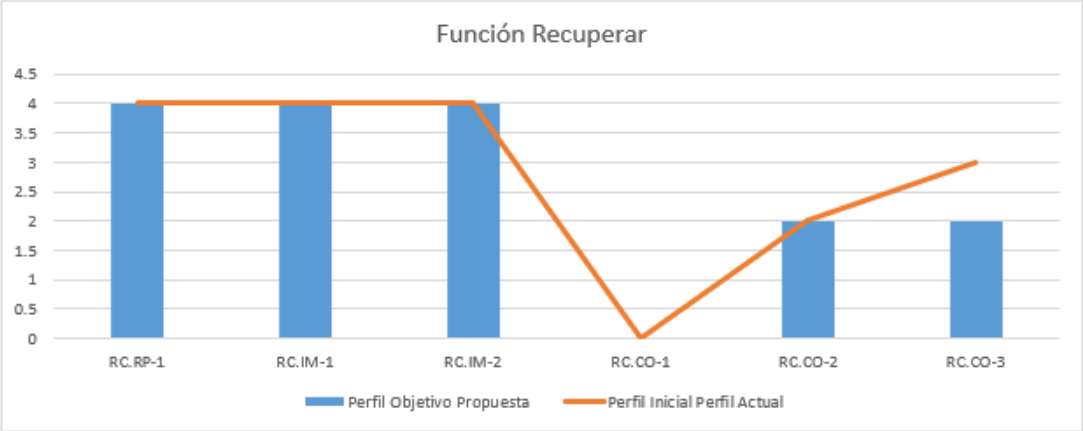


Figura 32. Descripción función: Recuperar. Categorías-subcategorías
Elaboración propia

La figura 33 muestra el detalle de la categoría Recuperar. En esta gráfica se puede ver las diferencias entre el perfil objetivo (propuesta) y el valor del Inicial. En la gráfica de barras se puede ver que el valor del perfil actual es mayor que el perfil objetivo en la subcategoría RC.CO-3. En las demás subcategorías el perfil actual es igual que el perfil objetivo. No es necesario realizar modificaciones a los controles de seguridad. En esta gráfica se incluyeron las subcategorías: RC.RP, RC.IM, RC.CO porque son pocas subcategorías.

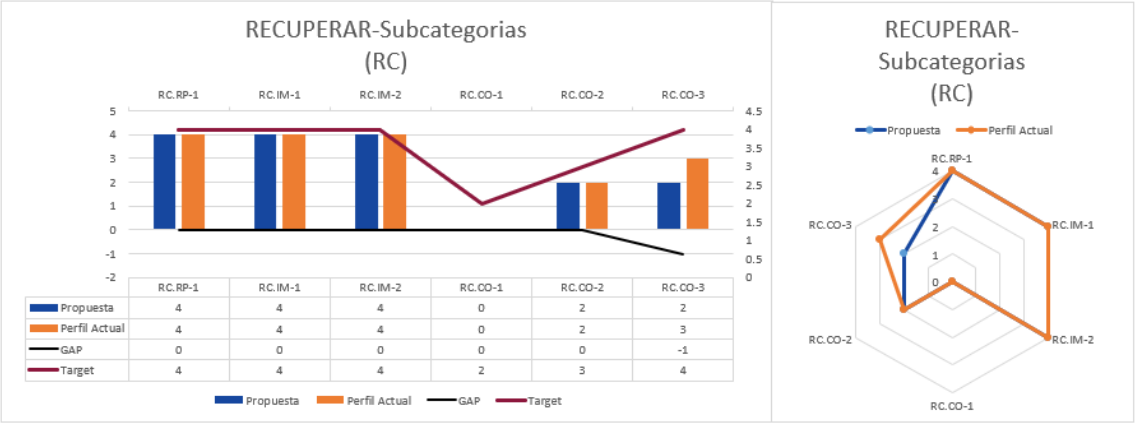


Figura 33. Descripción función: Recuperar. Categorías: Planificación de la Recuperación/Mejoras/Comunicaciones-subcategorías
Elaboración propia

Programa de Ciberseguridad

El programa de ciberseguridad estará formado por cada una de las funciones, junto con sus categorías y subcategorías. Este programa le permitirá a la empresa tener una línea base para mejor, y monitorear su postura de ciberseguridad. De acuerdo con estos resultados la empresa tiene que priorizar cada subcategoría dentro de cada función. De esta forma puede planear donde desea invertir para mejorar su postura de ciberseguridad. Cada subcategoría está clasificada en color verde obligatoria, color naranja opcional, y el color gris No obligatorio. Ver figura 34, 35, 36, 37 y 38.

				Nivel de Implementación (0,1,2,3,4)		1er Iteración
Función	Categoría	Subcategoría	Perfil Objetivo Propuesta	Perfil Inicial Perfil Actual	GAP	Empresa Target
IDENTIFICAR (ID)	Gestión de activos (ID.AM)	ID.AM-1	4	3	1	4
		ID.AM-2	4	0	4	2
		ID.AM-3	4	0	4	2
		ID.AM-4	4	4	0	4
		ID.AM-5	4	3	1	4
		ID.AM-6	3	3	0	4
			Propuesta	Perfil Actual	GAP	Target
	Entorno empresarial (ID.BE)	ID.BE-1	4	4	0	4
		ID.BE-2	4	4	0	4
		ID.BE-3	4	3	1	4
		ID.BE-4	3	3	0	4
		ID.BE-5	3	1	2	3
			Propuesta	Perfil Actual	GAP	Target
	Gobernanza (ID.GV)	ID.GV-1	3	2	1	3
		ID.GV-2	3	4	-1	4
		ID.GV-3	2	4	-2	4
		ID.GV-4	3	4	-1	4
			Propuesta	Perfil Actual	GAP	Target
	Evaluación de riesgos (ID.RA)	ID.RA-1	4	2	2	3
		ID.RA-2	2	4	-2	4
		ID.RA-3	4	4	0	4
		ID.RA-4	4	4	0	4
		ID.RA-5	3	4	-1	4
		ID.RA-6	4	4	0	4
			Propuesta	Perfil Actual	GAP	Target
	Estrategia de gestión de riesgos (ID.RM)	ID.RM-1	4	4	0	4
		ID.RM-2	4	4	0	4
		ID.RM-3	2	3	-1	4
			Propuesta	Perfil Actual	GAP	Target
	Gestión del riesgo de la cadena de suministro (ID.SC)	ID.SC-1	2	4	-2	4
		ID.SC-2	2	4	-2	4
		ID.SC-3	3	1	2	2
		ID.SC-4	3	2	1	3
		ID.SC-5	3	0	3	2

Obligatorio
Opcional
No Obligatorio

Figura 34. Función: Identificar–Categorías–subcategorías
Elaboración propia

				Nivel de Implementación (0,1,2,3,4)		1er Iteración
			Perfil Objetivo	Perfil Inicial		Empresa
Función	Categoría	Subcategoría	Propuesta	Perfil Actual	GAP	Target
PROTEGER (PR)	Gestión de identidad, autenticación y control de acceso (PR.AC)	PR.AC-1	4	4	0	4
		PR.AC-2	4	3	1	4
		PR.AC-3	3	0	3	2
		PR.AC-4	4	4	0	4
		PR.AC-5	4	4	0	4
		PR.AC-6	4	4	0	4
		PR.AC-7	4	4	0	4
			Propuesta	Perfil Actual	GAP	Target
	Concienciación y capacitación (PR.AT)	PR.AT-1	4	1	3	3
		PR.AT-2	4	4	0	4
		PR.AT-3	3	4	-1	4
		PR.AT-4	3	1	2	3
		PR.AT-5	4	2	2	3
			Propuesta	Perfil Actual	GAP	Target
	Seguridad de los datos (PR.DS)	PR.DS-1	4	4	0	4
		PR.DS-2	4	2	2	3
		PR.DS-3	2	3	-1	4
		PR.DS-4	4	2	2	3
		PR.DS-5	4	2	2	3
		PR.DS-6	4	3	1	4
		PR.DS-7	4	4	0	4
		PR.DS-8	4	4	0	4
			Propuesta	Perfil Actual	GAP	Target
	Procesos y procedimientos de protección de la información (PR.IP)	PR.IP-1	4	4	0	4
		PR.IP-2	4	1	3	1
		PR.IP-3	3	0	3	2
		PR.IP-4	4	3	1	4
		PR.IP-5	4	0	0	2
		PR.IP-6	3	4	-1	4
		PR.IP-7	3	4	-1	4
		PR.IP-8	4	0	4	2
		PR.IP-9	4	0	4	2
		PR.IP-10	4	0	4	2
		PR.IP-11	4	4	0	4
		PR.IP-12	4	0	4	2
			Propuesta	Perfil Actual	GAP	Target
	Mantenimiento (PR.MA)	PR.MA-1	4	3	1	4
		PR.MA-2	4	3	1	4
			Propuesta	Perfil Actual	GAP	Target
	Tecnología de protección (PR.PT)	PR.PT-1	3	4	-1	4
		PR.PT-2	4	4	0	4
		PR.PT-3	4	4	0	4
		PR.PT-4	4	4	0	4
		PR.PT-5	3	4	-1	4

Obligatorio
Opcional
No Obligatorio

Figura 35. Función: Proteger–Categorías–subcategorías
Elaboración propia

				Nivel de Implementación (0,1,2,3,4)		1er Iteración
Función	Categoría	Subcategoría	Perfil Objetivo Propuesta	Perfil Inicial Perfil Actual	GAP	Empresa Target
DETECTAR (DE)	Anomalías y Eventos (DE.AE)	DE.AE-1	4	0	4	2
		DE.AE-2	3	4	-1	4
		DE.AE-3	2	4	-2	4
		DE.AE-4	3	4	-1	4
		DE.AE-5	3	4	-1	4
			Propuesta	Perfil Actual	GAP	Target
	Monitoreo Continuo de la Seguridad (DE.CM)	DE.CM-1	4	2	2	3
		DE.CM-2	3	4	-1	4
		DE.CM-3	2	4	-2	4
		DE.CM-4	3	4	-1	4
		DE.CM-5	3	0	0	2
		DE.CM-6	3	4	-1	4
		DE.CM-7	4	4	0	4
		DE.CM-8	4	4	0	4
			Propuesta	Perfil Actual	GAP	Target
	Procesos de Detección (DE.DP)	DE.DP-1	4	4	0	4
		DE.DP-2	3	4	-1	4
		DE.DP-3	3	4	-1	4
		DE.DP-4	4	2	2	3
		DE.DP-5	4	4	0	4

Obligatorio
Opcional
No Obligatorio

Figura 36. Función: Detectar–Categorías–subcategorías
Elaboración propia

				Nivel de Implementación (0,1,2,3,4)		1er Iteración
			Perfil Objetivo	Perfil Inicial		Empresa
Función	Categoría	Subcategoría	Propuesta	Perfil Actual	GAP	Target
RESPONDER (RS)	Planificación de la Respuesta (RS.RP)	RS.RP-1	3	0	3	2
			Propuesta	Perfil Actual	GAP	Target
	Comunicaciones (RS.CO)	RS.CO-1	2	4	-2	4
		RS.CO-2	0	4	-4	4
		RS.CO-3	0	0	0	2
		RS.CO-4	3	2	1	3
		RS.CO-5	3	4	-1	4
			Propuesta	Perfil Actual	GAP	Target
	Análisis (RS.AN)	RS.AN-1	4	4	0	4
		RS.AN-2	4	2	2	3
		RS.AN-3	3	4	-1	4
		RS.AN-4	3	2	1	3
		RS.AN-5	2	4	-2	4
			Propuesta	Perfil Actual	GAP	Target
	Miligación (RS.MI)	RS.MI-1	4	4	0	4
		RS.MI-2	4	3	1	4
		RS.MI-3	3	4	-1	4
			Propuesta	Perfil Actual	GAP	Target
	Mejoras (RS.IM)	RS.IM-1	4	4	0	4
		RS.IM-2	4	2	2	3

Obligatorio
Opcional
No Obligatorio

Figura 37. Función: Responder–Categorías–subcategorías
Elaboración propia

			Nivel de Implementación (0,1,2,3,4)		1er Iteración
Función	Categoría	Subcategoría	Perfil Objetivo Propuesta	Perfil Inicial Perfil Actual	GAP	Empresa Target
RECUPERAR (RC)	Planificación de la recuperación (RC.RP)	RC.RP-1	4	4	0	4
			Propuesta	Perfil Actual	GAP	Target
	Mejoras (RC.IM)	RC.IM-1	4	4	0	4
		RC.IM-2	4	4	0	4
			Propuesta	Perfil Actual	GAP	Target
	Comunicaciones (RC.CO)	RC.CO-1	0	0	0	2
		RC.CO-2	2	2	0	3
		RC.CO-3	2	3	-1	4

Obligatorio
Opcional
No Obligatorio

Figura 38. Función: Recuperar–Categorías–subcategorías
Elaboración propia

ANÁLISIS DE RESULTADOS

A continuación, se realiza el análisis de los casos más sobresalientes. En la figura 39. se muestran los resultados obtenidos en una barra de acumulación de los resultados obtenidos en cada una de las funciones. Se puede ver por medio de porcentajes, donde la Perfil objetivo = Perfil Actual, Perfil objetivo > Perfil Actual, Perfil objetivo < Perfil Actual.

El valor más significativo se puede apreciar en la función Proteger donde los resultados de la función para el Perfil Objetivo > Perfil Actual, es 46% de todo el total y Perfil objetivo = Perfil Actual es igual al 18%. En otras palabras, en la función Proteger hubo más coincidencias, entre lo propuesto y el perfil actual.

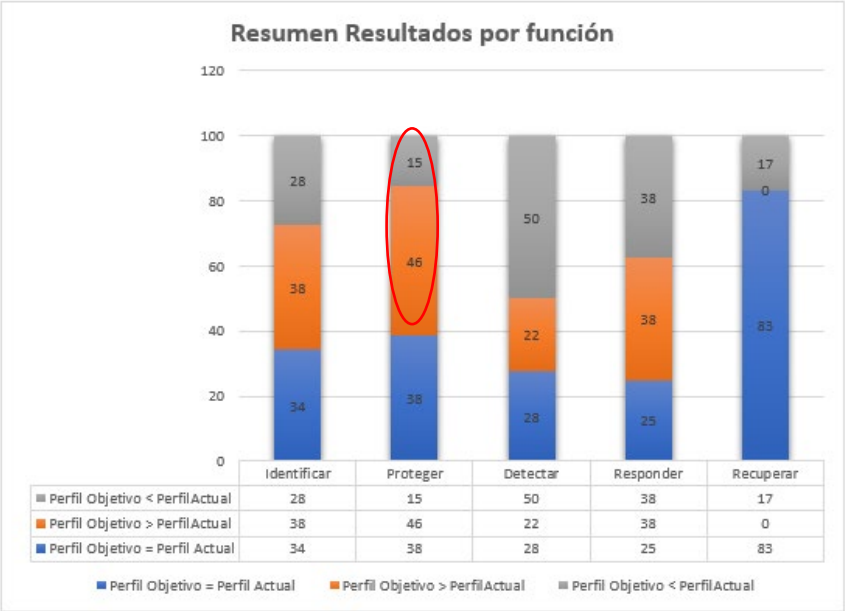


Figura 39. Resumen, resultados
Elaboración propia

En la figura 40, se puede ver en círculos las categorías PR.IP-2, PR.IP-4, PR.IP-,8,9,10, PR.IP-12, donde la Propuesta > Perfil Actual. Este caso significa que lo que se propone como parte del marco mínimo la empresa no lo cumple. Estas categorías fueron identificadas y la empresa no estaba consciente de estas vulnerabilidades. Las cuales se deben considerar para mejor su postura de ciberseguridad.

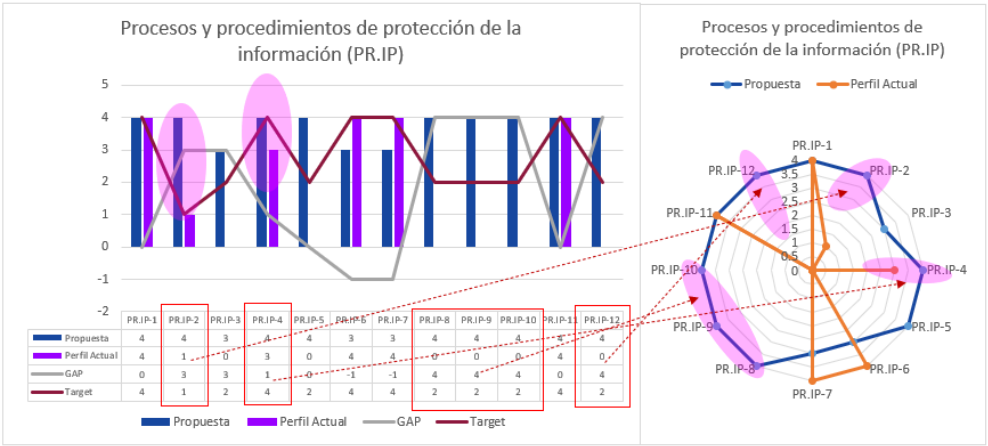


Figura 40. Descripción función Proteger-Categoría Proceso y procedimientos de protección de la información-subcategorías
Elaboración propia

Como resultado del análisis de las subcategorías se puede concluir lo siguiente en la tabla 5:

Tabla 5. Resultados, conclusiones

Subcategoría	Descripción	Observaciones
PR.IP-2	Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.	*La empresa no se dedica al desarrollo de aplicaciones de software razón por la cual hay diferencias.*
PR.IP-4	Se realizan, se mantienen y se prueban copias de seguridad de la información.	*Se comento que esta categoría no se tiene implementada al 100%, no se tenía conocimiento de esta vulnerabilidad.*
PR.IP-8	Se comparte la efectividad de las tecnologías de protección.	*La empresa actualmente no documento las lecciones aprendidas.*
PR.IP-9	Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).	*La empresa no cuenta con planes de respuesta a incidentes. Planea dar inicio a su creación. Y priorizarlos después de esta autoevaluación.*

Recopilación, traducción basada en NIST CSF v1.1 (National Institute of Standards and Technology (NIST) 2018b)

Otros resultados donde se aprecian diferencias significativas son: Responder comunicaciones (RS.CO-1,2), Recuperar-Comunicaciones (RC.CO-1): estas se refieren a subcategorías que no se consideraron necesarias para empresas PYMEs mexicanas porque no aplican al no existir obligaciones legales; sin embargo, al ser esta una empresa transnacional, ella cumple con normas requeridas en Estados Unidos de donde esta empresa tiene su matriz principal.

CONCLUSIONES

Después de que la empresa haya realizado la autovaloración, y se hayan analizado los resultados se recomienda lo siguiente para establecer su programa de ciberseguridad o línea base de ciberseguridad.

En base a las funciones del modelo NIST CSF v1.1, la empresa:

1. Debe realizar las actividades propuestas por la función identificar, estas actividades se deben realizar antes de que ocurra un incidente de ciberseguridad.
2. Deben realizar las actividades propuestas por la función proteger, estas actividades se deben realizar antes de que ocurra un incidente de ciberseguridad.
3. Las actividades de las funciones detectar, responder, se pueden realizar cuando está ocurriendo un incidente, o después de que ocurre el incidente.
4. Las actividades de la función recuperar se realizan después de que ocurre un incidente de ciberseguridad.

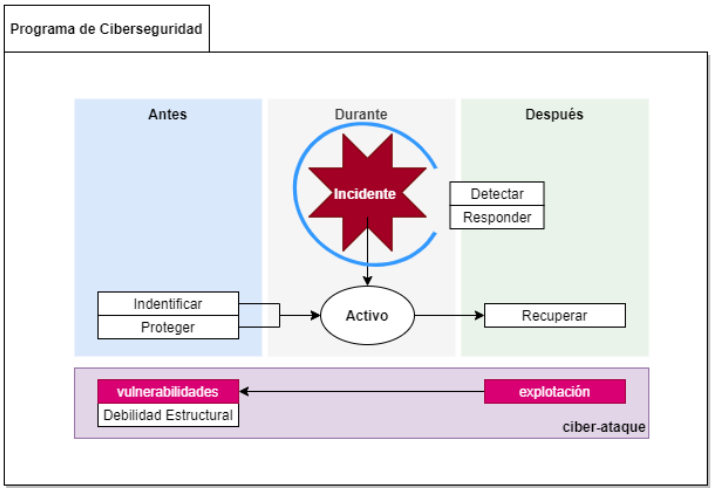


Figura 41. Programa de ciberseguridad
Elaboración propia

Se debe considerar las subcategorías de acuerdo con su clasificación (obligatoria, opcional, no obligatorio), para incluirlas, y priorizarlas. En la figura 41, se muestra la secuencia mencionada.

- Por medio de la herramienta de la hoja de cálculo se permite dar visibilidad de manera detallada a los componentes del programa de ciberseguridad.
- Se identificaron áreas críticas que necesitan atención.
- De las subcategorías identificadas se podrá priorizar en cuales áreas se necesita implementar controles de seguridad; para mejorar la postura de ciberseguridad de la organización.

Después de la implementación de las actividades propuestas en cada subcategoría la empresa podrá establecer su línea base de ciberseguridad, e iniciar su mejora continua del programa de ciberseguridad con cada nueva iteración realizada.

RECOMENDACIONES

A mediano plazo se tienen que definir indicadores de riesgo clave (Key Risk Indicators, KRIs), e Indicadores Clave de Eficiencia (Key Performance Indicators, KPIs). Por medio de la definición de KRIs, y KPIs se podrá determinar de manera objetiva si la implementación del programa de ciberseguridad está siendo efectiva.

En esta etapa se trata de simplificar el proceso para que la PYME pueda iniciar el proceso de ciberseguridad y en la medida de su compromiso con el desarrollo del programa pueda continuar con la evolución del proceso.

Dado que uno de los objetivos de este trabajo es la simplificación del proceso de valoración del riesgo por la falta de recursos (materiales, humanos) en las PYMEs, no se desarrollaron las métricas porque para su realización se requiere estar monitoreando los controles propuestos y se requiere inversión de recursos materiales y humanos para poder valorar su avance.

Se debe reconocer que los problemas de ciberseguridad son un problema de la organización no solo de IT o OT toda la organización se debe involucrar para que el programa de ciberseguridad tenga éxito. Lo que significa que antes de cualquier cosa se tiene que desarrollar una estrategia de administración de ciberseguridad.

APORTACIÓN DE LA TESIS

Este trabajo puede ser de utilidad si alguna pyme desea iniciar en la creación su programa de ciberseguridad, puede realizar los siguientes pasos:

En base a las funciones del modelo NIST CSF v1.1, y las categorías y subcategorías la empresa:

1. Puede utilizar la hoja de cálculo para realiza su autoevaluación.
2. Antes de que ocurra un incidente de ciberseguridad:
    a. Deben realizar las actividades propuestas por la función identificar.
    b. Deben realizar las actividades propuestas por la función proteger.
3. Si está ocurriendo un incidente:
    a. Se deben realizar las actividades de la función detectar, y las actividades de la función responder.
4. Después de que ya ocurrió un incidente:
    a. Se deben realizar las actividades de la función recuperar.

Al finalizar la autoevaluación de las categorías y subcategorías de cada función, la empresa ha obtenido su perfil inicial. Posteriormente debe realizar su perfil objetivo donde se establece hasta que nivel desea llegar. Y el resultado de cada subcategoría, y categoría de cada función se debe priorizar para que la empresa pueda identificar cuales subcategorías debe priorizar para dar inicio a la implementación de su programa de ciberseguridad.

APORTACIÓN SOCIAL DE LA TESIS

El trabajo desarrollado lo podrá utilizar la PYME que así lo decida y adaptarlo de acuerdo con sus necesidades como un punto de inicio para comenzar su línea base de ciberseguridad.

REFERENCIAS

Banco Interamericano de Desarrollo. Organización de Estados Americanos. 2020. *Ciberseguridad Riesgos, Avances y El Camino a Seguir En América Latina y El Caribe*.

Brumfield, Cynthia. Haugli, Brian. 2022. *Cybersecurity Risk Management. Mastering the Fundamentals Using the NIST Cybersecurity Framework*. Hoboken, NJ: John Wiley & Sons, Inc.

CANIETI. 2017. *Evaluación de La Ciberseguridad En México: Brechas y Recomendaciones En Un Mundo Híper-Conectado*. Ciudad de México.

Center for Internet Security (CIS). 2021. "CIS Critical Security Controls Version 8.0." Retrieved July 4, 2022 (https://www.cisecurity.org/controls).

Cisco. Rockwell. Panduit. 2022. "Securely Traversing IACS Data across the IDMZ Using Cisco Firepower Threat Defense. Design and Implementation Guide." 162. Retrieved May 5, 2022 (https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_2_CVD.pdf).

Garza, Patricio. 2021. "La Ciberseguridad En México: ¿una Necesidad?" *KAS Blog: México2021: Realidades y Desafíos*. Retrieved March 20, 2022 (https://www.kas.de/es/web/mexiko/einzeltitel/-/content/la-ciberseguridad-en-mexico-una-necesidad).

Gobierno de la República Mexicana. 2021. *Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.* México.

Gobierno de la República Mexicana. 2017. *Estrategia Nacional de Ciberseguridad*. México.

Hamilton Ortiz, Jesús. 2020. *Industry 4.0 - Current Status and Future Trends*.

International Organization for Standardization (ISO)/International Electrotechnical, and Commission (IEC). 2009. *ISO/IEC 27000. Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary*. First edit. edited by ISO/IEC. Switzerland: ISO/IEC.

International Society of Automation (ISA). 2018. "New ISA/IEC 62443 Standard Specifies Security Capabilities for Control System Components." Retrieved July 18, 2022 (https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c).

International Telecommunication Union (ITU). 2020. "Global Cybersecurity Index 2020." 172. Retrieved (https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf).

International Telecommunication Union (ITU). 2022. "Cybersecurity." 1. Retrieved July 14, 2022 (https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx).

Kagermann, Henning. Wahlster, Wolfgang. Helbig, Johannes. 2013. "Securing the Future of German Manufacturing Industry. Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0. Final Report of the Industrie 4.0 Working Group." 84. Retrieved February 22, 2022 (https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf).

Kumar, S. V. Anil Bawge, Ganapathy. Kumar. B. C. Vinay. 2021. "An Overview of Industrial Revolution and Technology of Industrial 4.0." *International Journal of Research in Engineering and Science (IJRES)* 9(1):8.

Kumar, Vikas. Rezaei, Jafar. Akberdina, Victoria. Kuzmin, Evgeny. 2021. *Digital Transformation in Industry. Trends, Management, Strategies*. Springer Nature Switzerland.

National Institute of Standards and Technology (NIST). 2018a. "Cybersecurity Framework. Getting Started." Retrieved July 15, 2022 (https://www.nist.gov/cyberframework/getting-started).

National Institute of Standards and Technology (NIST). 2018b. "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1." 55. Retrieved February 19, 2021 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf).

National Institute of Standards and Technology (NIST). 2020. "SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations." 492. Retrieved July 4, 2022 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final).

National Institute of Standards and Technology (NIST). n.d. "COMPUTER SECURITY RESOURCE CENTER." Retrieved July 14, 2022 (https://csrc.nist.gov/glossary/term/cybersecurity).

North American Electric Reliability Corporation (NERC). 2022. "About NERC." Retrieved July 14, 2022 (https://www.nerc.com/AboutNERC/Pages/default.aspx).

Rashid, A., Chivers, H., Danezis, G., Lupu, E., & Martin, A. 2019. "The Cyber Security Body of Knowledge (CYBOK) 1.0" edited by The National Cyber Security Centre. 854. Retrieved June 20, 2022 (https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf).

Rathwell, Gary. 2004. "PERA Enterprise Integration Web Site." Retrieved July 15, 2022 (http://www.pera.net).

Rout, Deepak. 2015. "Developing a Common Understanding of Cybersecurity." *ISACA JOURNAL*, 4.

Secretaría de Gobernación. 2021. "Diario Oficial de La Federación." 159. Retrieved April 28, 2023 (https://sidof.segob.gob.mx/welcome/26-06-2018).

Secretaría de relaciones exteriores. 2020. "T-MEC." 1101. Retrieved October 20, 2022 (https://dof.gob.mx/2020/SRE/T_MEC_290620.pdf).

Takakuwa, Soemon. Veza, Ivica. Celar, Stipe. 2018. "'Industry 4.0' in Europe and East Asia." P. 9 in. Vienna, Austria: DAAAM International.

Thames, Lane. Schaefer, Dirk. 2017. *Cybersecuriy for Industry 4.0. Analysis for Design and Manufacturing. Springer Series in Advanced Manufacturing*. edited by Springer.

ANEXO A

Instituto Nacional de Estándares y Tecnología (National Instituto Standard Technology, NIST) Marco de ciberseguridad versión 1.1 (Cybsercurity Framework, CSF) v1.1.

El marco es un enfoque basado en riego para administrar el riesgo de ciberseguridad, está compuesto de tres partes: el núcleo (1), niveles de implementación (2), y perfiles (3).

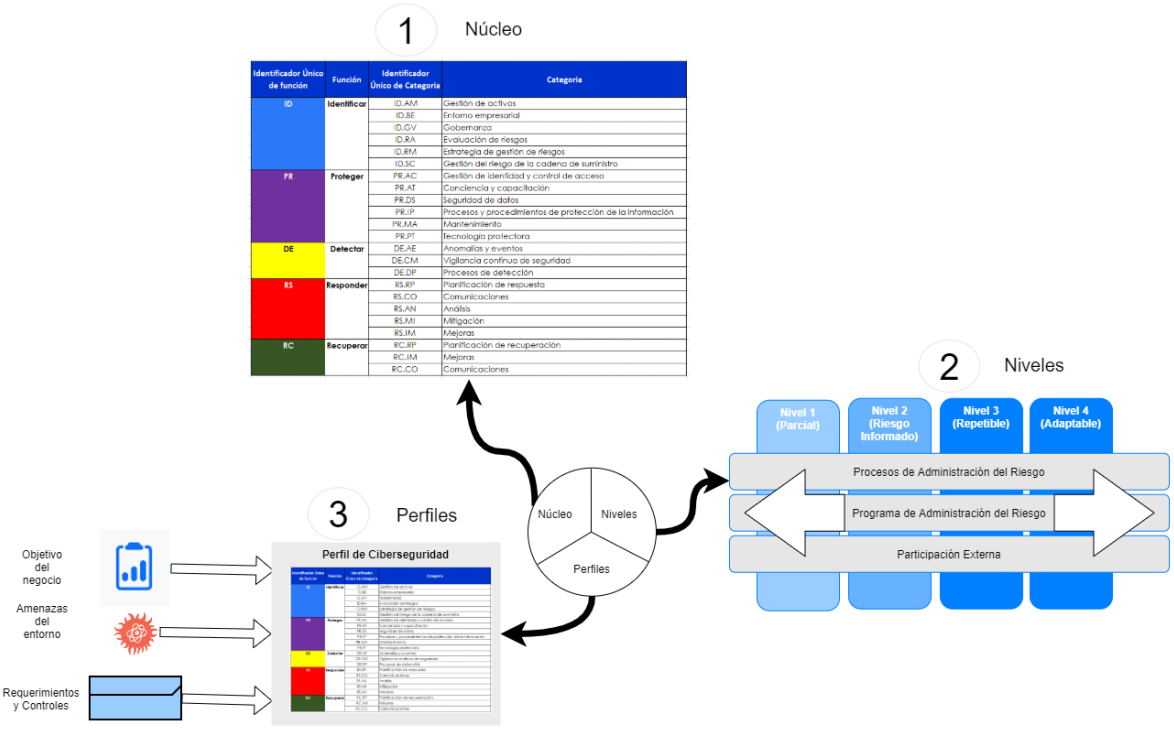


Figura A1: Componentes del NIST CSF v1.1
Elaboración propia

El núcleo, es un conjunto de actividades de ciberseguridad. Está formado de cinco funciones, veintitrés categorías, y 108 subcategorías. En la figura A2, se puede apreciar el núcleo, y en la figura A3, se muestra el resumen de sus componentes.

1 Núcleo

Identificador Único de función	Función	Categoria	Identificador Único de Categoria
ID	Identificar	Gestión de activos	ID.AM
		Entorno empresarial	ID.BE
		Gobernanza	ID.GV
		Evaluación de riesgos	ID.RA
		Estrategia de gestión de riesgos	ID.RM
		Gestión del riesgo de la cadena de suministro	ID.SC
PR	Proteger	Gestión de identidad y control de acceso	PR.AC
		Conciencia y capacitación	PR.AT
		Seguridad de datos	PR.DS
		Procesos y procedimientos de protección de la información	PR.IP
		Mantenimiento	PR.MA
		Tecnología protectora	PR.PT
DE	Detectar	Anomalías y eventos	DE.AE
		Vigilancia continua de seguridad	DE.CM
		Procesos de detección	DE.DP
RS	Responder	Planificación de respuesta	RS.RP
		Comunicaciones	RS.CO
		Análisis	RS.AN
		Mitigación	RS.MI
		Mejoras	RS.IM
RC	Recuperar	Planificación de recuperación	RC.RP
		Mejoras	RC.IM
		Comunicaciones	RC.CO

Figura A2: Resumen de los componentes del núcleo. Basado en NIST CSF v1.1
Elaboración propia

	Funtiones	Categorias	Subcategorias
1 Identificar-ID	1	6	29
2 Proteger-PR	1	6	39
3 Detectar-DE	1	3	18
4 Responder-RS	1	5	16
5 Recuperar-RC	1	3	6
	5	**23**	**108**

Figura A3: Resumen de los componentes del núcleo
Elaboración propia

Las cinco funciones son: identificar, proteger, detectar, responder, recuperar.

Cada función tiene categorías como se muestra en la figura A4.

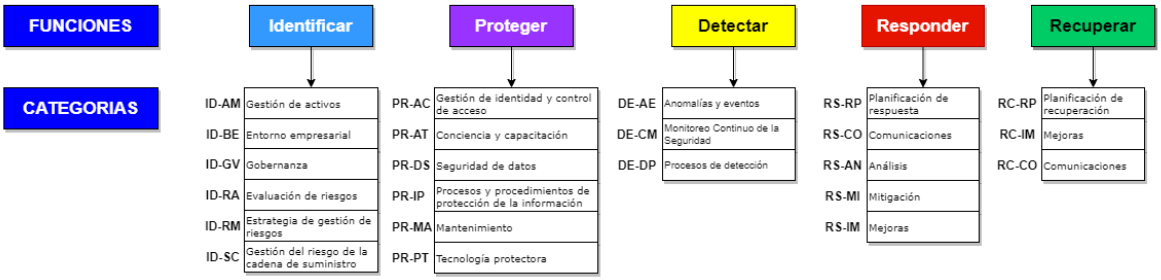


Figura A4: Funciones y sus categorías
Elaboración propia

Las categorías tienen subcategorías que han sido mapeadas a los controles de los principales estándares de la industria, estos controles son las recomendaciones para implementar en cada subcategoría. Las subcategorías de cada función se muestran en las figuras A5, A6, A7, A8, A9, A10.

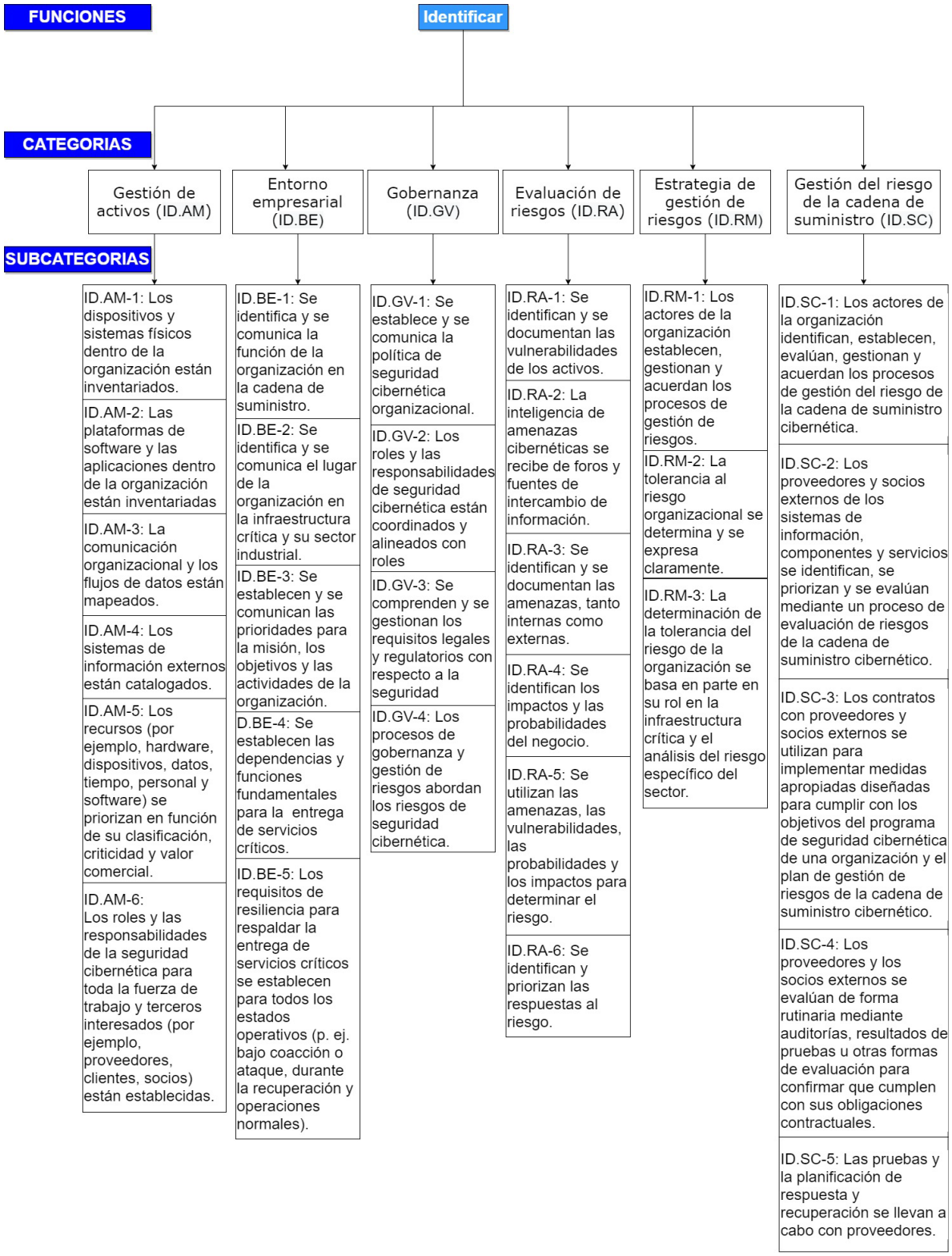


Figura A5: Función Identificar-subcategorías
Elaboración propia

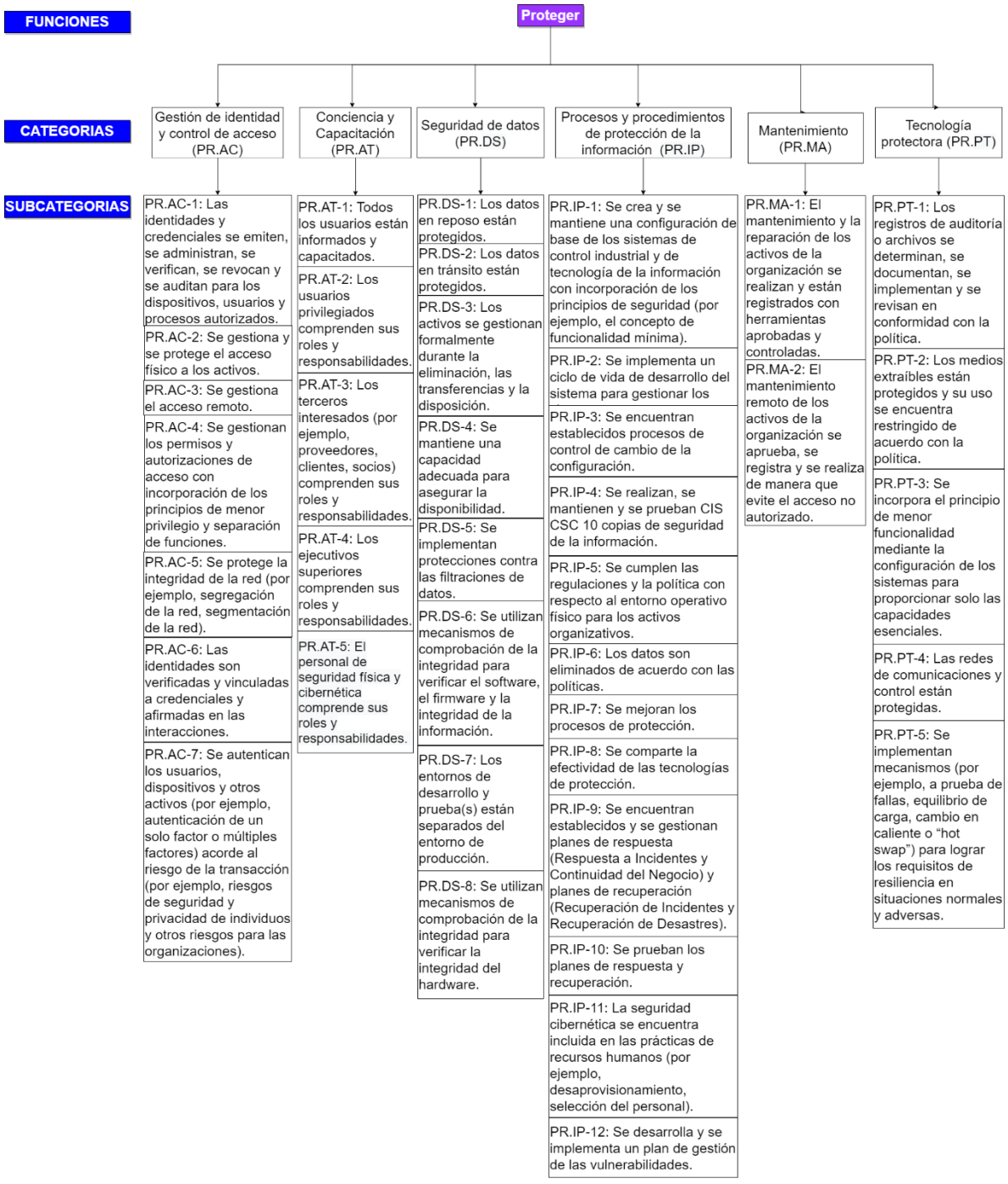


Figura A6: Función Proteger-subcategorías
Elaboración propia

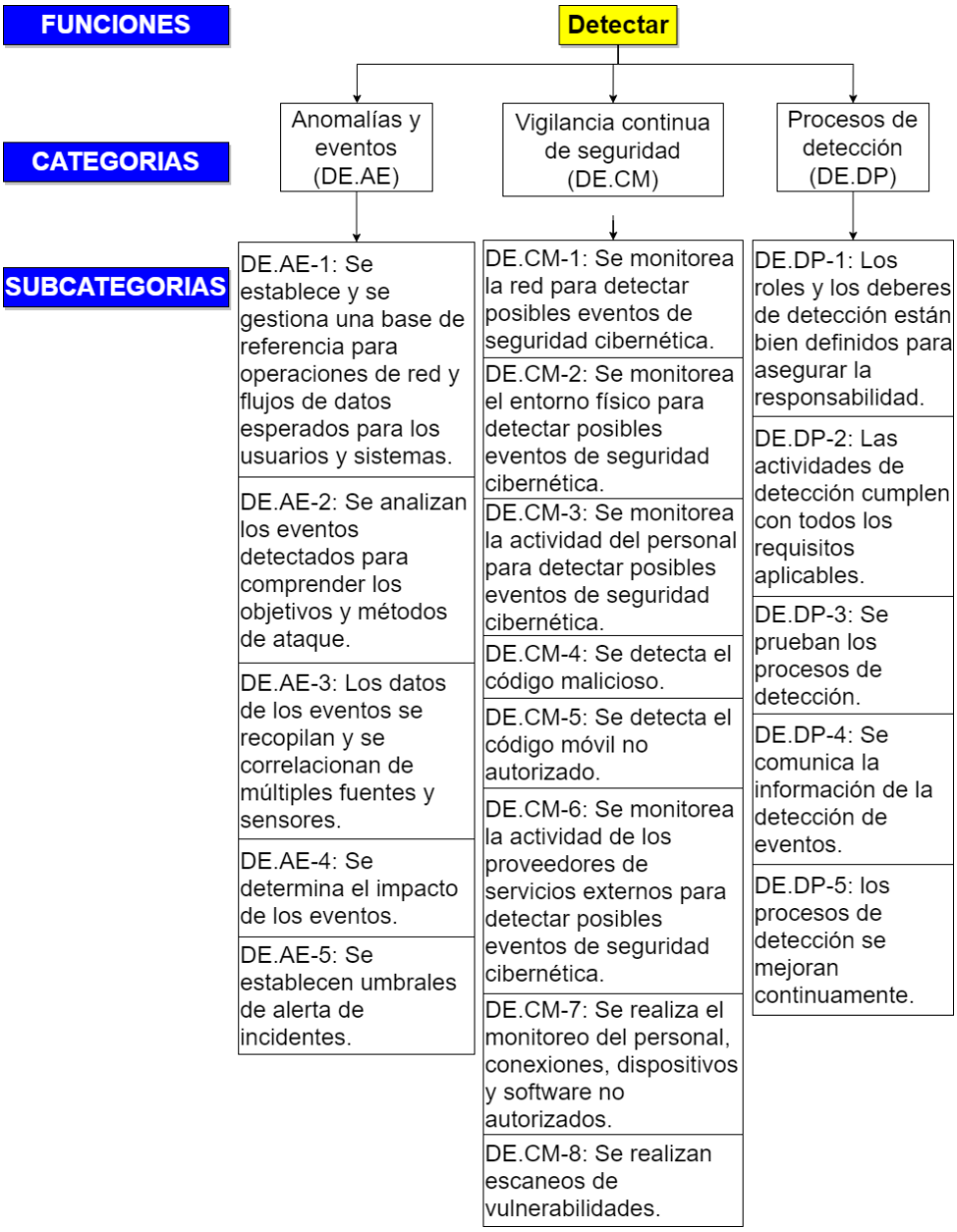


Figura A7: Función Detectar-Subcategorías
Elaboración propia

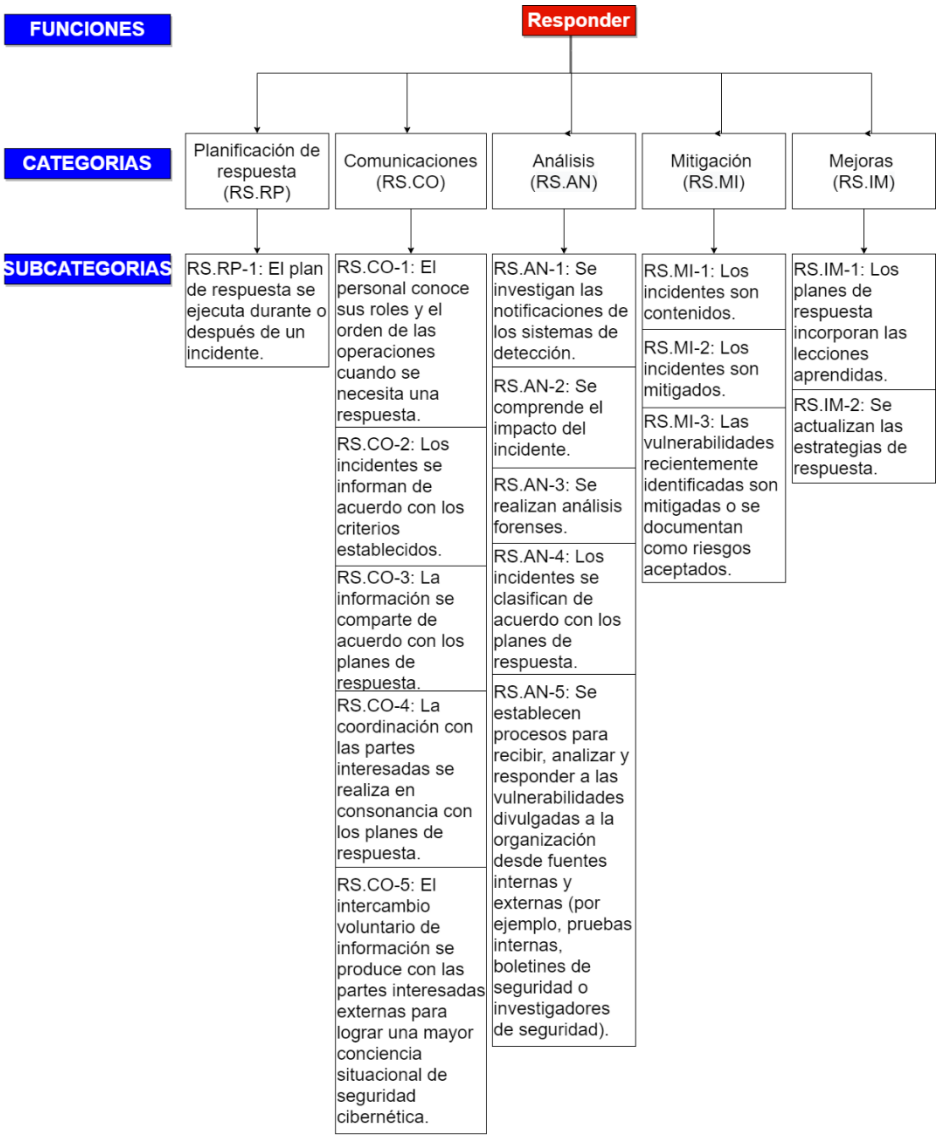


Figura A8: Función Responder-Subcategorías
Elaboración propia

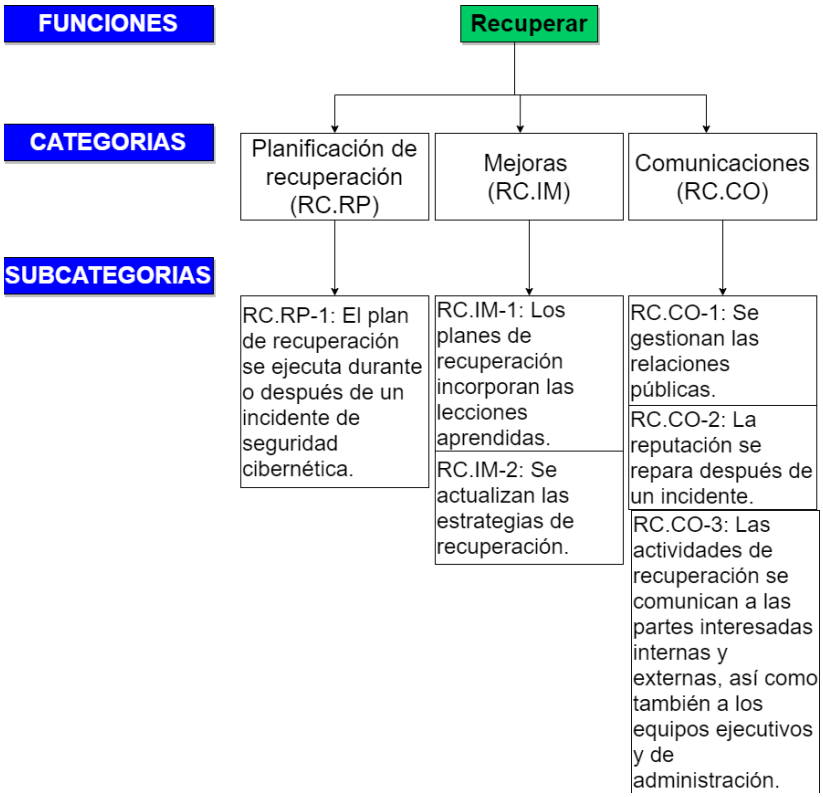


Figura A9: Función Recuperar-subcategorías
Elaboración propia

Niveles de implementación

Este componente se utiliza para proporcionar contexto acerca de cómo la organización percibe los riesgos y que procesos tiene establecidos para la administración del riesgo. Los niveles de implementación están definidos en tres áreas: procesos de administración de riesgo, programa de administración de riesgo integrado, y participación externa, el siguiente resumen se basa en Administración del Riesgo de Ciberseguridad de Brumfield y Haugli (Brumfield, Cynthia. Haugli 2022).

Nivel 1: Parcial: el riesgo se gestiona de acuerdo a las necesidades, a veces, manera reactiva. Existe una conciencia limitada del riesgo de seguridad cibernética a nivel organizacional no abarca toda la organización. Es posible que la organización no tenga los procesos implementados para participar en coordinación o colaboración con otras entidades externas.

Nivel 2: Informado sobre los riesgos: la gerencia aprueba las prácticas de administración de riesgos, pero es posible que no sea una política para toda la organización. Hay conciencia del riesgo de ciberseguridad a nivel de la organización. Aun así, no se ha establecido un enfoque para toda la organización, y la organización comprende el ecosistema más amplio, pero no ha formalizado su participación en él.

Nivel 3: Repetible – Las prácticas de administración del riego de la organización son aprobadas y adoptadas formalmente como política. Hay un enfoque en toda la organización para la administración de riesgos. La organización colabora y recibe información de socios en el ecosistema más amplio.

Nivel 4: Adaptativo: La organización adapta sus prácticas de ciberseguridad a partir de las lecciones aprendidas. La gestión de riesgos de ciberseguridad utiliza políticas, procedimientos y procesos informados sobre riesgos y es parte de la cultura organizacional y la organización comparte información activamente con los socios.

En la figura A11, se representan de manera gráfica los niveles de implementación y su relación con las tres áreas que los definen.

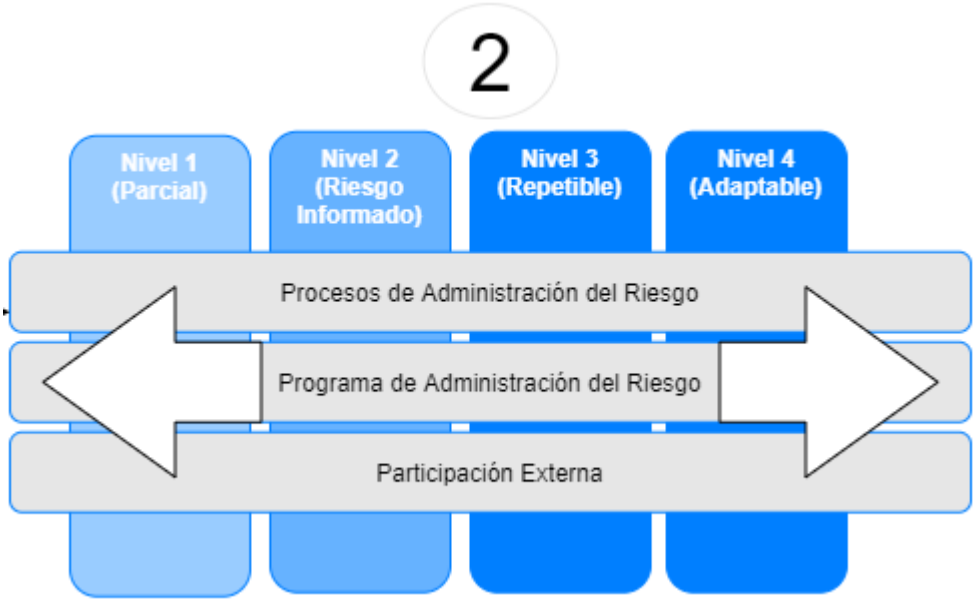


Figura A10: Niveles de implementación. Traducido, adaptado de Administración de Riesgos de Ciberseguridad
(Brumfield, Cynthia. Haugli 2022)

Los perfiles

En el componente perfiles se puede ver como la organización esta alineada en la implementación de los estándares, prácticas del componente núcleo. El perfil se utiliza para conocer el estado actual de alineación con el NIST CSF v1.1.