EVALUACIÓN DEL PROCESO DE SEGURIDAD DIGITAL EN EMPRESAS DEL SECTOR ELÉCTRICO EN COLOMBIA

RAÚL ALEJANDRO TRIGOS ANGARITA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS
, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CUCÚTA
2023

EVALUACIÓN DEL PROCESO DE SEGURIDAD DIGITAL EN EMPRESAS DEL SECTOR ELÉCTRICO EN COLOMBIA

RAÚL ALEJANDRO TRIGOS ANGARITA

Proyecto de grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

EDGAR ROBERTO DULCE VILLARREAL
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CÚCUTA
2023

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad _____, Fecha sustentación _____

DEDICATORIA

A mi madre Nelly Angarita, quien me orienta en alcanzar uno a uno mis objetivos académicos, su respaldo incondicional siempre fortalecerá mis cualidades.

A mi padre Raúl Trigos, quien me apoya en diversos aspectos para materializar mis metas, su carácter y disciplina han sido parte integral de mí.

A Nelly Arias, por motivarme y guiarme en mi carrera profesional, gracias por acompañarme en los momentos más especiales de mi vida.

AGRADECIMIENTOS

Agradezco a cada uno de los directores y tutores de la Especialización en Seguridad Informática, a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, gracias por su comprensión y aporte académico.

A Jover Alonso Cabrales Pineda y Constanza Eugenia Quintero Calderón por su asesoría, motivación y el apoyo suministrado para el desarrollo del presente proyecto aplicado, la oportunidad que me brindaron y la experiencia adquirida.

CONTENIDO

pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ACCIÓN CORRECTIVA: Acción para eliminar la(s) causa(s) de una no conformidad y evitar que vuelva a ocurrir.

ACTIVO CRÍTICO: Instalaciones, sistemas o dispositivo que, si es destruido, degradado o puesto indisponible, afecte la confiablidad u operatividad del sistema eléctrico. Acorde con las recomendaciones del Comité Tecnológico del CNO para la definición de activos críticos que comprometan la seguridad de operación del SIN.

ALTA DIRECCIÓN: Persona o grupo de personas que dirigen y controlan una organización al más alto nivel.

AMENAZA: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

ASUMIR RIESGOS: Estrategia de Administración de Riesgos consistente en no desarrollar ninguna acción tendiente a su control. Aceptación del riesgo en su condición actual.

ATAQUE: Tentativa de destruir, exponer, alterar, inhabilitar, robar o acceder sin autorización o hacer un uso no autorizado de un activo.

AUDITORIA: Proceso sistemático, independiente y documentado para obtener evidencias de la auditoria (registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de la auditoria y que son verificables) y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría.

AUTENTICACIÓN: Asegurar que una característica declarada de una entidad es correcta.

AUTENTICIDAD: Propiedad de que una entidad es lo que dice ser.

CAUSA: Condición de origen interno o externo que genera la posibilidad de que se presente un riesgo.

CIBER-ACTIVO: Dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota.

CIBER-ACTIVO CRÍTICO: Dispositivo para la operación confiable de activos críticos que usa un protocolo enrutable para comunicarse afuera del perímetro de seguridad electrónica o utiliza un protocolo enrutable con un centro de control o es accesible por marcación. Son dispositivos electrónicos programables, software, sistemas y personas que a través de ellos se pueden afectar los activos críticos en su confiabilidad u operatividad de los procesos y servicios.

CIBERESPACIO: Es una red interdependiente de infraestructuras de información y comunicaciones, que incluye internet, redes de telecomunicaciones, sistemas informáticos, y procesos y controles embebidos.

CIBER-RESILIENCIA: Cuando un sistema es capaz de soportar todo tipo de presiones sin cambiar su comportamiento, entonces es robusto. Cuando un sistema no es capaz de soportar más presiones, pero puede integrar cambios para disminuirlas y puede seguir adelante, entonces es ciber-resiliente.

CIBERSEGURIDAD: Actividad o proceso, habilidad o capacidad, o estado en el que la información y los sistemas de comunicación e información que contienen, están protegidos o pueden defenderse contra daños, usos o modificaciones no autorizadas.

COMPETENCIA: Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

CONFIABILIDAD: Propiedad de la consistencia del comportamiento deseado y los resultados.

CONFIDENCIALIDAD: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

CONFORMIDAD: Cumplimiento de un requisito.

CONSECUENCIA: Efecto principal de un riesgo que es considerado al momento de realizar la valoración de acuerdo con el objeto de impacto afectado.

CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN: Procesos y procedimientos para asegurar la continuidad de las operaciones relacionadas con la seguridad de la información.

CONTROL: Acción que tiende a prevenir y/o mitigar o potenciar los riesgos. Se pueden clasificar en preventivos o correctivos de acuerdo con su función.

CONTROL DE ACCESO: Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos (2.63) de negocio y de seguridad.

CORRECCIÓN: Acción tomada para eliminar una no conformidad detectada.

DISPONIBILIDAD: Propiedad de ser accesible y utilizable a demanda por una entidad autorizada.

EFECTO: Resultado de la materialización del riesgo para el nivel de gestión analizado.

EFICACIA: Grado en el que se realizan las actividades planificadas y se alcanzan los resultados planificados.

ESCENARIO DE RIESGO: Descripción detallada del riesgo, según como se materializa el evento en un determinado nivel de gestión y de acuerdo al conjunto de circunstancias que lo rodean.

ESQUEMA DE MONITOREO: Secuencia de acciones necesarias para la medición y análisis de la evolución de los riesgos a partir de la implementación de acciones para su mitigación.

EVENTO: Presencia o cambio de un conjunto particular de circunstancias.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, una falla en los controles o una situación previa desconocida hasta el momento y que puede ser relevante para la seguridad.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: Procesos para la detección, reporte, evaluación, respuesta, tratamiento, y aprendizaje de incidentes de seguridad de la información.

GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

INCIDENTE CIBERNÉTICO: Significa cualquier violación o amenaza inminente implícita o explícita de la política de seguridad de la información y ciberseguridad del Asegurado, cualquier evento que compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad) o cualquier evento o serie de eventos

indeseados o inesperados de ciberseguridad que tengan una probabilidad significativa de comprometer la operación de la infraestructura crítica de la operación.

INCIDENTE DE CIBERSEGURIDAD: Cualquier acto malicioso o evento sospechoso que compromete o intenta comprometer la seguridad física o electrónica de un Ciber Activo Crítico o su perímetro.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento único o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.

INTEGRIDAD: Propiedad de exactitud y completitud.

MATRIZ DE RIESGOS: Representación en forma gráfica del nivel de los riesgos identificados y evaluados en su probabilidad y consecuencia, teniendo en cuenta los controles existentes en el momento de la evaluación. En esta matriz se identifican cuatro zonas rojas (extremo), naranja (alto), amarilla (tolerable) y verde (aceptable), que representan los niveles de aceptabilidad definido.

MEJORA CONTINUA: Actividad recurrente para mejorar el desempeño.

NIVEL DE RIESGO: Magnitud de un riesgo expresada en términos de la consecuencia y la probabilidad. En términos prácticos se calcula como el producto entre probabilidad y consecuencia.

NO CONFORMIDAD: Incumplimiento de un requisito.

NO REPUDIO: Capacidad para corroborar que es cierta la reivindicación de que ocurrió un evento o una acción y las entidades que lo originaron.

OBJETIVO DE CONTROL: Declaración que describe lo que se quiere lograr como resultado de la implementación de controles.

OBJETO DE IMPACTO: Elemento del entorno interno o externo que puede afectarse si llegara a materializarse un riesgo, cuya afectación podría comprometer el cumplimiento de los objetivos organizacionales y el cumplimiento de los compromisos asumidos con los diferentes grupos de interés, por lo cual debe ser valorado y protegido.

PARTE INTERESADA: Persona u organización que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad.

PERÍMETRO DE SEGURIDAD ELECTRÓNICA: Es la frontera lógica con acceso controlado, que rodea una red dentro de la cual están conectados los Ciber Activos Críticos.

PERÍMETRO DE SEGURIDAD FÍSICA: Es la frontera física con acceso controlado, completamente contenida (seis paredes) que rodea cuartos de control, cuartos de comunicaciones. centros de operación y otros sitios que alojan Ciber Activos Críticos. Puntos de acceso al (los) perímetro(s) de Seguridad Electrónica: Incluye todos los terminales de comunicación externamente conectados (por ejemplo: módems de marcación) que conecten con cualquier dispositivo dentro del Perímetro de Seguridad Electrónica.

PLAN DE RECUPERACIÓN DE DESASTRES (DRP): Proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos. Esto también debería incluir proyectos para enfrentarse a la pérdida inesperada o repentina de personal clave, aunque esto no sea cubierto en este artículo, el propósito es la protección de datos.

POLÍTICA: Intenciones y dirección de una organización, como las expresa formalmente su alta dirección.

PROBABILIDAD: Medida de la posibilidad de que algo suceda en determinadas circunstancias de modo, espacio y tiempo. Se representa por una medida adimensional entre “0” (certeza de no-ocurrencia) y “1” (certeza de ocurrencia).

PROCESO: Conjunto de actividades secuenciales e interrelacionadas, orientadas a la consecución de un resultado en el que se agrega valor a un insumo y se suministra un producto o servicio a otro proceso o a cualquiera de los grupos de interés definidos por la empresa, en especial, al cliente final para satisfacer una necesidad. Un proceso agrupa las actividades con las cuales es posible realizar el producto o servicio objeto de éste.

PUNTOS DE ACCESO AL (LOS) PERÍMETRO(S) DE SEGURIDAD ELECTRÓNICA: Incluye todos los terminales de comunicación externamente conectados (por ejemplo: módems de marcación) que conecten con cualquier dispositivo dentro del Perímetro de Seguridad Electrónica.

REQUISITO: Necesidad o expectativa que está establecida, generalmente implícita u obligatoria.

RESILIENCIA: La resiliencia se refiere al proceso de, capacidad para, o resultado de una adaptación exitosa a pesar de circunstancias desafiantes o amenazantes”.

RIESGO: Posibilidad de que se materialice un evento que pueda generar afectación sobre un objeto de impacto.

RIESGO DE SEGURIDAD DIGITAL: Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.

SEGURIDAD DE LA INFORMACIÓN: Es la preservación de la confidencialidad, integridad y disponibilidad de la información.

SISTEMA DE GESTIÓN: Conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos.

VULNERABILIDAD: Debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

RESUMEN

Los generadores y operadores del sistema eléctrico nacional de Colombia se encuentran integrando tecnologías digitales avanzadas para automatizar y controlar las funciones físicas de las infraestructuras criticas para mejorar el rendimiento interconectando los dispositivos digitales de control y medida a una red de datos que puede estar expuesta a amenazas cibernéticas.

Las empresas del sector eléctrico en Colombia han desarrollado estrategias de seguridad de la información y ciberseguridad que buscan desarrollar las capacidades de: gestión de la ciberseguridad, conciencia situacional, respuesta a incidentes y ciber defensa, gestionar la identidad y control de acceso, definir nuevas estrategias de ciberseguridad y una nueva gestión de ciberseguridad orientada al riesgo. Por lo tanto, el proceso de seguridad digital debe ser constantemente evaluado y actualmente carece de la definición de un plan para garantizar la mejora continua del proceso.

El presente proyecto, tiene como propósito evaluar el proceso de seguridad digital definido en el sistema de gestión integral de una empresa del sector eléctrico en Colombia. Inicialmente se identificará el estado actual del proceso, mediante la verificación de los planes de tratamiento los mecanismos de la operación y controles de la seguridad digital. Teniendo en cuenta lo anterior, se aplicará el modelo de madurez de la capacidad cibernética C2M2 para evaluar el proceso de seguridad digital y finalmente definir un plan de manera apropiada para garantizar la mejora continua del proceso.

ABSTRACT

Generators and operators of Colombia's national electrical system are integrating advanced digital technologies to automate and control the physical functions of critical infrastructure to improve performance by interconnecting digital control and measurement devices to a data network that may be exposed to threats. cybernetics.

Companies in the electricity sector in Colombia have developed information security and cybersecurity strategies that seek to develop the capabilities of: cybersecurity management, situational awareness, incident response and cyber defense, manage identity and access control, define new strategies cybersecurity and a new risk-oriented cybersecurity management. Therefore, the digital security process must be constantly evaluated and currently lacks the definition of a plan to guarantee continuous improvement of the process.

The purpose of this project is to evaluate the digital security process defined in the comprehensive management system of a company in the electricity sector in Colombia. Initially, the current state of the process will be identified by verifying the treatment plans, operation mechanisms and digital security controls. Taking into account the above, the C2M2 cyber capability maturity model will be applied to evaluate the digital security process and finally define a plan appropriately to ensure continuous improvement of the process.

INTRODUCCIÓN

Las amenazas cibernéticas continúan en constante aumento, lo que las convierte en uno de los riesgos operativos más apremiantes que enfrentan las empresas modernas. Tanto la seguridad nacional como la salud económica dependen en gran medida del funcionamiento confiable de la infraestructura crítica y de la continuidad de operaciones de organizaciones de diversos sectores ante dichas amenazas. En este contexto, el Modelo de Madurez de Capacidades de Ciberseguridad (C2M2) emerge como un recurso valioso que puede asistir a las empresas del sector eléctrico en Colombia para evaluar y mejora de sus programas de ciberseguridad, fortaleciendo, así, su capacidad para mantener operaciones ininterrumpidas.

El C2M2 se enfoca en la implementación y gestión de prácticas de ciberseguridad relacionadas con activos de tecnología de la información (TI), tecnología operativa (TO) y activos de información, considerando también el contexto operativo.

En el presente proyecto, se aplicará el Modelo de Madurez de la Capacidad Cibernética (C2M2) en una empresa del sector eléctrico en Colombia para medir la seguridad digital. El proceso se iniciará con la recopilación de documentación de su Sistema de Gestión Integral (SGI), que incluirá la guía de cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI), los procesos de seguridad digital y la estructura administrativa.

La evaluación de la capacidad cibernética se llevará a cabo utilizando la herramienta HTML del modelo C2M2, disponible de forma gratuita en la página web del Programa C2M2. Durante la preparación del taller de autoevaluación C2M2, se tendrán en cuenta los roles existentes en la estructura administrativa y se recopilará el material de apoyo más actualizado del modelo C2M2. Se evaluarán las 356 prácticas propuestas en el modelo, utilizando opciones de respuesta que incluirán "No implementada", "Implementada parcialmente", "Implementada en gran medida" y "Totalmente Implementada".

Una vez que se haya completado el análisis de las brechas de seguridad mediante los indicadores de nivel de madurez (MIL), se procederá a priorizar las iniciativas y proyectos en un plan de tratamiento.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Las empresas del sector eléctrico en Colombia están sometidas al régimen general de los servicios públicos domiciliarios y ejerce actividades dentro del ámbito del derecho privado como empresario mercantil.

Según la Cámara Colombiana de Informática y Telecomunicaciones (CCIT)[1], desde el Tanque de Análisis y Creatividad de las TIC (TicTac) y su programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE) consideran relevante la adopción de estrategias de ciberseguridad por parte de las compañías, que estén enfocadas a la protección del usuario, debido a que el ciberdelito se ha convertido en una de las actividades criminales de mayor crecimiento en Colombia durante los últimos tres años; impulsado por eventos como la pandemia COVID-19 y el incremento del comercio electrónico que alcanzó el 59.4% en las transacciones durante el periodo de cuarentena obligatoria y del 35% durante el 2021 con ventas estimadas en 37 billones de pesos al finalizar el año según cifras de la Cámara de Comercio electrónico de Colombia CCCE.

Considerando lo anteriormente mencionado, las empresas del sector eléctrico en Colombia generalmente disponen de un Sistema de Gestión Integrado (SGI) que incluye un proceso de Seguridad Digital, con el propósito de documentar y formalizar sus procedimientos relacionados a la operación de la seguridad digital. Constantemente este proceso es actualizado con el fin de adaptarse a los objetivos estratégicos de las empresas y considerando las nuevas tendencias en ciberseguridad.

1.2 FORMULACIÓN DEL PROBLEMA

El entorno digital en las empresas industriales conlleva riesgos y amenazas que deben ser evaluados para tomar decisiones efectivas. En Colombia, las empresas eléctricas necesitan validar su seguridad digital y desarrollar un plan de mejora continua, surgiendo la siguiente necesidad.

¿Como se puede garantizar la eficiencia y eficacia de los controles de seguridad a partir de una evaluación del proceso de seguridad digital?

[1] CCIT. Tendencias Cibercrimen Colombia 2021 – 2022: Nuevas amenazas al comercio electrónico. {En línea}. {2021}. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf.

2 JUSTIFICACIÓN

El proceso de seguridad digital debe aportar al cumplimiento de los objetivos estratégicos de las empresas del sector eléctrico en Colombia, adicionalmente debe alinearse las acciones y/o controles propuestos con las iniciativas estratégicas que han definido como: Sostenibilidad, transmisión y distribución de energía, las directivas del talento humano y tecnología, los retos generales, la estrategia de crecimiento y la estrategia de transformación cultural, entre otros. Por lo tanto, evaluar el proceso de seguridad digital permitirá analizar las lecciones aprendidas y definir un plan de mejora continua que permitirá ajustar las necesidades para garantizar la continuidad de los servicios TI/TO y así disponer de las herramientas y la información necesaria para alcanzar los objetivos estratégicos.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Evaluar el proceso de seguridad digital en una empresa del sector eléctrico en Colombia, aplicando el modelo de madurez de la capacidad cibernética C2M2 para la adopción de una mejora continua.

3.2 OBJETIVOS ESPECÍFICOS

- Examinar el estado actual del proceso de seguridad digital en una empresa del sector eléctrico en Colombia a partir de una revisión de su sistema de gestión integrado.

- Inspeccionar los planes de tratamiento, los mecanismos de la operación y controles de la seguridad digital implementados en una empresa del sector eléctrico en Colombia para determinar su eficiencia y efectividad.

- Adoptar el modelo de madurez de la capacidad cibernética C2M2 para evaluar el proceso de seguridad digital en una empresa del sector eléctrico en Colombia.

- Medir el proceso de seguridad digital en una empresa del sector eléctrico en Colombia a partir de los instrumentos de evaluación C2M2 para determinar el estado actual de la seguridad digital y promover el mejoramiento continuo del proceso.

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

Las empresas Colombianas cada vez más implementan soluciones digitales y la información resultante de sus procesos es un activo de gran valor que es necesario salvaguardar y generar mecanismos de control que permitan garantizar los principios de confidencialidad, disponibilidad, integridad y no repudio, no obstante, los balances generados por entidades de seguridad como Fortinet, muestran que en Colombia se percibe una mayor tasa de intentos de ataques cibernéticos, en contraste se identifica un bajo porcentaje de empresas que invierte recursos en seguridad, y en muchos casos la inversión que se hace resulta ser inadecuada para enfrentar los desafíos actuales. En el año 2017, Citrix publicó un estudio que presenta cifras preocupantes sobre la implementación de mecanismos de seguridad, donde en un total de 48% de las empresas encuestadas, no tienen desarrollado, ni en borrador, unas políticas de seguridad. Del mismo modo, un 70% mencionó contar con herramientas de seguridad obsoletas y que no brindan el nivel requerido ante las amenazas actuales[2].

Considerando lo mencionado anteriormente, se identifica una diversificación de la tecnología y simultáneamente un aumento constante del cibercrimen, mientras que las empresas siguen estando muy rezagadas a lo requerido para proteger su información. Con el propósito de conseguir un nivel aceptable de seguridad en una empresa del sector eléctrico en Colombia, es indispensable disponer de un conjunto de procedimientos que permitan generar control de seguridad en los diferentes activos y ciber-activos, que pueden ser clasificados en cuatro (4) tipos: seguridad en la conectividad de las Tecnologías de la Información (TI), seguridad en la conectividad de las Tecnologías de la Operación, la seguridad de hardware y la seguridad de software.

4.1.1 Seguridad en la conectividad TI

Existen diversas vulnerabilidades que se pueden aprovechar debido a la ausencia de seguridad en la red, como la interceptación o escucha ilegal de información, la propagación de virus, software espía y robo de identidad.

Los controles de seguridad eficientes en la red de datos son todos aquellos que incluyen un conjunto de soluciones entre software y hardware, entre los que se

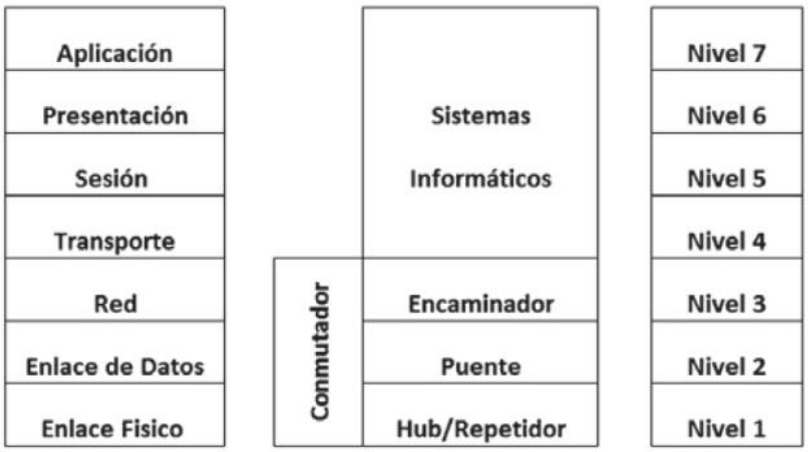
[2] ANGULO, Susana. Empresas fallan en sus sistemas de seguridad informática. {En línea}. {27 de febrero de 2017}. Disponible en: https://www.enter.co/especiales/empresas-del-futuro/segun-estudio-empresas-fallan-en-sus-sistemas-de-seguridad-informatica/.

pueden resaltar el antivirus, firewall, Sistema de Prevención de Intrusos (IPS), Sistema de Detección de Intruso (IDS) y el uso de redes VPN.

Los controles deben cobijar los ciber-activos relacionados a las redes de datos, conformadas por una serie de dispositivos físicos, que tienen una mayor o menor capacidad de control mediante programación software, pero no dejan de ser dispositivos, con un objetivo concreto en la red, los cuales son[3]:

- Canales de comunicación y cableados típicos: par trenzado, fibra óptica y la comunicación inalámbrica.
- Repetidores.
- Hubs o concentradores.
- Conmutadores o switches
- Encaminadores o router
- Maquinas utilizadas por los usuarios, especialmente servidores.

Figura 1. Niveles OSI de dispositivos en sistemas de comunicaciones



Fuente: Díaz, G., Alzórriz, I., Sancristóbla, E., & Castro, M. (2014). Procesos y herramientas para la seguridad de redes. Universidad Nacional de Educación a Distancia. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/48736?

4.1.2 Seguridad en la conectividad TO

Comprende los mecanismos de control que protegen los ICS, por sus siglas en ingles Industrial Control System, es decir, Sistemas de Control Industrial. Según

[3] Díaz, G., Alzórriz, I., Sancristóbla, E., & Castro, M. (2014). Procesos y herramientas para la seguridad de redes. Universidad Nacional de Educación a Distancia. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/48736?

Lorenzo[4], hace referencia a un concepto asociado a una variedad de sistemas de control utilizados en los procesos industriales. Estos sistemas pueden contener desde unos pocos controladores hasta una gran cantidad de sistemas distribuidos con miles de elementos interconectados. También, existen una variedad de ICS como HMI, PLC o SCADA[5].

ISA 95 define los siguientes 5 niveles para clasificar los componentes de este tipo de sistemas.

- **Nivel 0**: Procesos de producción físico.
- **Nivel 1**: Sensores, los cuales pueden ser manipulan y actúan sobre el proceso de producción.
- **Nivel 2**: Monitorización, supervisión y control de los procesos.
- **Nivel 3**: Control de flujos u órdenes para crear los productos finales, mantenimiento de registros y optimización del proceso de producción.
- **Nivel 4**: Destinado a la alta gestión con procesos como logística y económicos facilitando información a la dirección ejecutiva.

Figura 2. Clasificación de los ICS

Fuente: LORENZO GONZÁLEZ, D. Herramienta para auditorías de seguridad en entornos industriales y SCADA. Logroño, 2020. Trabajo de investigación (Máster universitario en seguridad informática). Universidad Internacional de la Rioja. ESIT.

[4] LORENZO GONZÁLEZ, D. Herramienta para auditorías de seguridad en entornos industriales y SCADA. Logroño, 2020. Trabajo de investigación (Máster universitario en seguridad informática). Universidad Internacional de la Rioja. ESIT.
[5] STOUFFER, K.; PILLITTERI, V.; LIGHTMAN, S.; ABRAMS, A.; HAHN, A. Guide to Industrial Control Systems (ICS) Security. United States: NIST Special Publication 800-82, 2015.

4.1.3 Seguridad de hardware

Se relaciona con todos los mecanismos de control implementados para garantizar que los dispositivos físicos de un sistema informático permanezcan seguros ante las posibles amenazas. El análisis del hardware es indispensable para detectar vulnerabilidades en los mismos, la seguridad de hardware puede ser activa o pasiva.

- Seguridad activa: Incluye todos los mecanismos que se encuentran destinados a la protección de los dispositivos, como los sistemas de alimentación interrumpida.
- Seguridad pasiva: Son los controles implementados para entrar a funcionar justo en el momento que se presenta una amenaza, es decir, esto ocurre cuando la amenaza superó todos los controles activos[6].

4.1.4 Seguridad de software

Corresponde a la protección de aplicaciones instaladas en los diferentes dispositivos y que pueden ser blanco de ataques debido a las múltiples vulnerabilidades que usualmente presentan. Se debe considerar que el software es parte fundamental de cualquier empresa en el cumplimiento de sus objetivos estratégicos y se encargan de gestionar la información más relevante para alcanzar sus metas.

Entre los controles a nivel de software, encontramos la solución de antivirus, mantener actualizados los aplicativos en la última versión de los parches, las actualizaciones del sistema operativo y el control de cada uno de los nuevos aplicativos que se deseen instalar[7].

4.1.5 Mecanismos de seguridad

Los mecanismos de seguridad implementados en una empresa para proteger sus activos y ciber-activos, pueden ser clasificados en seguridad física y seguridad lógica, esto permite definir metodologías de control de acceso apropiada para generar un control seguro.

---

[6] NAKED SECURITY. Seguridad activa y seguridad pasiva en equipos informáticos. {En línea}. {14 de septiembre de 2012}. Disponible en: https://news.sophos.com/es-es/2012/09/14/seguridad-activa-y-seguridad-pasiva-en-equipos-informaticos/.

[7] UNIVERSIDAD INTERNACIONAL DE VALENCIA. Tres tipos de seguridad informática que debes conocer. {En línea}. {10 de octubre de 2016}. Disponible en: https://www.universidadviu.com/es/actualidad/nuestros-expertos/tres-tipos-de-seguridad-informatica-que-debes-conocer.

A continuación, se mencionan algunos tipos de controles de acceso que pueden ser implementados en las organizaciones. Estos mecanismos se eligen en función de las necesidades particulares de cada organización o del nivel de seguridad deseado[8].

- Controles de acceso físicos

    - Por huella dactilar: El reconocimiento de la huella dactilar es un control de acceso biométrico que se basa en el hecho de que no existen dos huellas dactilares iguales. Es uno de los sistemas más habituales y se puede usar tanto para acceder a instalaciones como a equipos informáticos o sistemas electrónicos.
    - Reconocimiento facial: El reconocimiento facial o el ocular son otros sistemas de identificación biométricos. Se basan en un software que analiza los rasgos de la cara de una persona y comprueba si coinciden con los de alguna entrada de su base de datos.
    - Tarjeta identificativa: Otro de los métodos de control de accesos y presencia es a través de las tarjetas identificativas. Normalmente estas tarjetas se insertan en terminales que identifican al usuario y almacenan diversa información, por ejemplo, la hora de entrada y salida del trabajador.

- Controles de acceso lógicos

    - Active Directory (AD): Es una base de datos y un conjunto de servicios que conectan a los usuarios con los recursos de red que necesitan para realizar su trabajo. En particular, se aseguran de que cada persona sea quien dice ser (autenticación), generalmente al verificar el ID de usuario y la contraseña que ingresa, y le permite acceder solo a los datos que tiene permitido usar (autorización).
    - Consola de seguridad: Es una plataforma de software extensible y centralizada que le permite administrar y hacer cumplir políticas de seguridad. Detecta las amenazas y proteger los puntos de enlace en su red.
    - Firewall: Un firewall es la parte de un sistema informático o red destinada a prevenir el acceso no autorizado, al mismo tiempo que facilita las comunicaciones autorizadas. Estos pueden ser implementados tanto a nivel de hardware como de software.
    - IPS/IDS: Es un dispositivo de seguridad, con la capacidad de bloquear o denegar el tráfico en función de las coincidencias positivas de una regla o la firma[9].

[8] GRUPO ATICO34. Control de acceso: Definición, objetivos y tipos. {En línea}. {Consultado el 19 de febrero de 2022}. Disponible en: https://protecciondatos-lopd.com/empresas/control-de-acceso/#Tipos_de_controles_de_acceso.

[9] SEGU-INFO. Detección de intrusiones en tiempo real. {En línea}. {20 de mayo de 2022}. Disponible en: http://www.segu-info.com.ar/proteccion/deteccion.htm.

4.2 MARCO CONCEPTUAL

Con el propósito de evaluar apropiadamente el proceso de seguridad digital en una empresa del sector eléctrico en Colombia, es fundamental apropiar un conjunto de conceptos básicos que permitan comprender los argumentos del presente proyecto aplicado.

4.2.1 Seguridad de la información

Es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la confidencialidad, integridad y disponibilidad de la información[10]. La confidencialidad nos garantiza que la información sólo podrá ser accedida o consultada por las personas autorizadas, mientras que la integridad se fundamenta en asegurar que la información recibida y almacenada sea legitima entre el emisor y receptor, finalmente la disponibilidad busca garantizar que la información pueda ser accesible, aplicando planes de contingencia para lograr restablecer la información ante cualquier eventualidad. En la actualidad se menciona el “No repudio” como otro componente de la seguridad de la información, el cual hace referencia a garantizar que el intercambio de la información entre los participantes fueron exactamente los autorizados y no se generó interceptación de un actor no autorizado.

4.2.2 Seguridad informática

Es una rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida[11]. Corresponde a los procedimientos implementados para fortalecer la seguridad de los recursos tanto físicos como lógicos de un sistema informático con el propósito de evitar que se comprometa la autenticidad, garantizando que accedan a la información solo el personal autorizado[12].

4.2.3 Seguridad digital

[10] ESCRIVÁ GASCÓ, G. Seguridad informática. España: Macmillan Iberia, 2013. 8p.
[11] GÓMEZ VIEITES, Á. Seguridad informática: básico. España: Ecoe Ediciones, 2010. 15p – 55p.
[12] CANDELARIO SAMPER, J.; RODRÍGUEZ BOLAÑO, M. Seguridad informática en el siglo XXI: Una perspectiva jurídica tecnológica enfocada hacia las organizaciones Nacionales y Mundiales. En: Revista Especializada en Ingeniería, Universidad Nacional Abierta y a Distancia. {En línea}. {18 de abril de 2014}. Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1441/1760.

Es la disciplina que se encarga de proteger la información en los servicios e infraestructura TI, aplicando controles basados en la prevención, detección y recuperación[13].

Figura 3. Controles de seguridad

Fuente: ÁLVAREZ, M. G.; PÉREZ, G. P. Seguridad informática para empresas y particulares. España: McGraw-Hill, 2004. 20p – 41p.

4.2.3 Controles de seguridad

Medidas de protección que se implementan para prevenir y/o mitigar los riesgos. Se pueden clasificar en preventivos o correctivos de acuerdo a su función, estas acciones, buscan reducir el impacto de diferentes eventos sobre los activos y ciber-activos de la operación del negocio, protegiéndola contra posibles pérdidas[14].

4.2.4 Activo

Se refiere a cualquier información o elemento de valor que posee la empresa, como son las Instalaciones físicas (edificio, sede, piso, etc.), infraestructura informática (servidores, bases de datos aplicaciones, entre otros), sistemas (eléctrico, aire acondicionado, etc.), o servicios de TI que, si son destruidos, degradados o puestos indisponibles, pueden afectar la confiabilidad u operatividad de los procesos y servicios[15].

[13] ÁLVAREZ, M. G.; PÉREZ, G. P. Seguridad informática para empresas y particulares. España: McGraw-Hill, 2004. 20p – 41p.
[14] NIST. Security and privacy controls for federal information systems and organizations. United States: NIST Special Publication 800-53, 2013.
[15] NIST. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. Estados Unidos: Instituto Nacional de Estándares y Tecnología, 2018. 1p – 44p.

4.2.5 Amenaza

Causa potencial de un incidente no deseado, situación que se puede presentar en la entidad dañando un activo de información, mediante la explotación de una vulnerabilidad[16].

4.2.6 Vulnerabilidad en la seguridad

Cualquier tipo de defecto de hardware o software que los usuarios malintencionados intentan explotar. Las vulnerabilidades de software, generalmente son causadas por errores en el sistema operativo o el código fuente de una aplicación. Las vulnerabilidades de hardware, hacen referencia a debilidades de seguridad causadas por fallas de diseño en los componentes y dispositivos informáticos, se limitan generalmente a modelos de dispositivos específicos y se explotan comúnmente con ataques dirigidos[17].

4.2.7 Ataque

Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema, generalmente programa escrito para aprovechar una vulnerabilidad de seguridad conocida[18].

4.2.8 Problemas de control de acceso

Uso incorrecto de las prácticas que administran el control físico de equipos, datos o aplicaciones[19].

4.2.9 Malware

Cualquier código informático que se puede utilizar para robar datos, evitar los controles de acceso o dañar o comprometer un sistema.

---

[16] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. NTC-ISO/IEC 27001:2013 Tecnología de la información, Técnicas de seguridad, Sistemas de gestión de la seguridad de la información, Requisitos. Bogotá. INCONTEC, 2013.

[17] LONG, J. Penetration Tester's Open Source Toolkit. United States: Syngress, 2006. 5p – 50p.

[18] OEA; AWS. Marco de Ciberseguridad NIST: Un abordaje integral de la Ciberseguridad. {En línea}. {28 de agosto de 2019}. Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf.

[19] QUINTERO, J. Introducción a los Sistemas de Control de Acceso. Bogotá, Colombia: Universidad Nacional Abierta y a Distancia, 2020.

4.2.10 Virus

Código ejecutable malintencionado que se adjunta a programas legítimos. Usualmente, los virus requieren la activación del usuario final y pueden ser relativamente inofensivos o muy destructivos. Con frecuencia se esparcen por las unidades USB, los medios ópticos, los recursos de red compartidos o los correos electrónicos[20].

4.2.11 Ingeniería social

Es una manera de obtener acceso a recursos que manipulan a las personas para que ejecuten acciones o divulguen información confidencial. Los atacantes intentan explotar nuestra predisposición para ayudar o nuestras debilidades[21].

4.2.12 Seguridad física

Un tipo de medida de seguridad que restringe el acceso a los armarios de red, las ubicaciones de servidores y la extinción de incendios.

4.3 MARCO LEGAL

Conforme al presente proyecto aplicado, contiene menciones de delitos informáticos en Colombia y que se encuentran tipificados en la Ley 1273 de 2009. Como argumenta Gonzalez [22], a través de esta ley se adiciona al código penal un nuevo bien jurídico denominado “De la protección de la información y de los datos”. La ley contiene dos capítulos y diez artículos mencionados en la siguiente tabla:

Tabla 1. Ley 1273 de 2009

Capitulo	Articulo	Descripción
1. De los atentados contra la confidencialidad, la	269A. Acceso Abusivo a un Sistema Informático.	Acceder total o parcialmente a un sistema informático sin autorización,

[20] LÓPEZ, M. Y. Los virus informáticos: Una amenaza para la sociedad. Cuba: Editorial Universitaria, 2009. 1p – 31p.
[21] PAREDES, F. C. I. Hacking. Argentina: El Cid Editor, 2009. 4p – 29p.
[22] GONZALEZ, J. Estudio del estado actual de la seguridad informática en las organizaciones de Colombia. Buga, 2020. Proyecto de grado (especialización en seguridad informática). Universidad Nacional Abierta y a Distancia. Escuela de ciencias básicas, tecnología e ingeniería.

Capitulo	Articulo	Descripción
integridad y la disponibilidad de los datos y de los sistemas informáticos.		aunque este cuente o no con medidas de seguridad.
	269B: Obstaculización llegítima de Sistema Informático o Red de Telecomunicación.	Este delito aplica a toda persona que genere un obstáculo para el acceso normal a un sistema información.
	269C: Interceptación de Datos Informáticos.	Aplica a cualquier interceptación de datos informático incluyendo interceptaciones a emisiones electromagnéticas.
	269D: Daño Informático.	Aplica a la persona que destruya sin autorización datos informáticos.
	269E: Uso de Software Malicioso.	Aplica a cualquier actividad relacionada con el uso de software malicioso, esto incluye actividades como el desarrollo o distribución.
	269F: Violación de Datos Personales	Cualquier actividad que implique la obtención sin autorización de datos personales con beneficio sea propia o de un tercero.
	269G: Suplantación de Sitios WEB para Capturar Datos	Aplica a cualquier actividad con la suplantación y engaño de personas con el fin de obtener información.
	269H: Circunstancias de Agravación Punitiva.	Menciona algunas causales de agravación de las penas, dependiendo la actividad final realizada o la propiedad del bien afectado.
2. De los Atentados informáticos y otras infracciones	269I: Hurto por Medios Informáticos y Semejantes	Toda actividad en la que se supere cualquier medida de seguridad bien sea manipulando un sistema de seguridad o suplantando a una persona.
	269J: Transferencia No Consentida de Activos	Realizar la manipulación y/o transferencia no autorizada de un activo y que esto sea en perjuicio de un tercero.

Fuente: GONZALEZ, J. Estudio del estado actual de la seguridad informática en las organizaciones de Colombia. Buga, 2020. Proyecto de grado (especialización en seguridad informática). Universidad Nacional Abierta y a Distancia. Escuela de ciencias básicas, tecnología e ingeniería.

El proceso de Seguridad Digital en las empresas del sector eléctrico en Colombia se relaciona a la ley 1712 de 2014 correspondiente a la transparencia y derecho de acceso a la información pública nacional, mediante el decreto 103 de 2015[23] se reglamenta parcialmente la ley y se dictan otras disposiciones. En el artículo 4º del decreto, hace referencia a la publicación de información en sección particular del sitio web oficial, aclarando que de conformidad con las condiciones establecidas en el artículo 5° de la Ley 1712 de 2014, deben publicar en el sitio web oficial, en una sección particular identificada con el nombre de “Transparencia y acceso a información pública”, la siguiente información:

a. La información mínima requerida a publicar según los artículos 9°, 10º y 11º de la Ley 1712 de 2014. Cuando la información se encuentre publicada en otra sección del sitio web o en un sistema de información del Estado, es necesario identificar la información que reposa en estos y habilitar los enlaces para permitir el acceso a la misma.
b. El registro de activos de información.
c. El índice de información clasificada y reservada.
d. El esquema de publicación de información.
e. El programa de gestión documental.
f. Las tablas de retención documental.
g. El informe de solicitudes de acceso a la información señalado en el artículo 52 del presente decreto.
h. Los costos de reproducción de la información pública, con su respectiva motivación.

En el artículo 27º del decreto 103 de 2015, hace referencia al responsable de la calificación de reserva de la información pública por razones de defensa y seguridad nacional, seguridad pública o relaciones internacionales.

[23] PRESIDENCIA DE LA REPÚBLICA. Decreto 103 de 2015: Diario Oficial 49400. {En línea}. {20 de enero de 2015}. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60556.

Entre otras normas jurídicas relacionadas al proceso de seguridad digital, podemos mencionar la Ley 527 de 1999[24], Ley 600 de 2000[25], Decreto 1078 de 2015[26], Decreto 1413 de 2017[27], Decreto 1704 de 2012[28], Decreto 2364 de 2012[29], Decreto 2573 de 2014[30], Decreto 415 de 2016[31], Resolución 0-2369 de 2016[32], Resolución 0312 de 2019[33], Acuerdo 1347 de 2020[34], CONPES 3701 de 2011[35], CONPES 3854 de 2016[36] y CONPES 3995 de 2020[37].

---

[24] CONGRESO DE LA REPÚBLICA. Ley 527 de 1999: Diario Oficial 43673. {En línea}. {21 de agosto de 1999}. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276.

[25] CONGRESO DE LA REPÚBLICA. Ley 600 de 2000: Diario Oficial 52130. {En línea}. {18 de agosto de 2022}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0600_2000_pr006.html.

[26] PRESIDENCIA DE LA REPÚBLICA. Decreto 1078 de 2015: Diario Oficial 49523. {En línea}. {26 de mayo de 2015}. Disponible en: https://normograma.mintic.gov.co/mintic/docs/decreto_1078_2015.htm.

[27] PRESIDENCIA DE LA REPÚBLICA. Decreto 1413 de 2017: Diario Oficial 50336. {En línea}. {25 de agosto de 2017}. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83253.

[28] PRESIDENCIA DE LA REPÚBLICA. Decreto 1704 de 2012: Diario Oficial 48523. {En línea}. {15 de agosto de 2012}. Disponible en: https://normograma.mintic.gov.co/mintic/docs/decreto_1704_2012.htm.

[29] PRESIDENCIA DE LA REPÚBLICA. Decreto 2364 de 2012: Diario Oficial 48622. {En línea}. {22 de noviembre de 2012}. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=50583.

[30] PRESIDENCIA DE LA REPÚBLICA. Decreto 2573 de 2014: Diario Oficial 49363. {En línea}. {12 de diciembre de 2014}. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=60596.

[31] PRESIDENCIA DE LA REPÚBLICA. Decreto 415 de 2016: Diario Oficial No. 49808. {En línea}. {07 de marzo de 2016}. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=65564.

[32] FISCALÍA GENERAL DE LA NACIÓN. Resolución 0-2369 de 2016: Diario Oficial 49933. {En línea}. {13 de Julio de 2016}. Disponible en: https://normograma.info/crc/docs/pdf/resolucion_fiscalia_2369_2016.pdf.

[33] MINISTERIO DE TRABAJO. Resolución 0312 de 2019: Diario Oficial 50872. {En línea}. {19 de febrero de 2019}. Disponible en: https://id.presidencia.gov.co/Documents/190219_Resolucion0312EstandaresMinimosSeguridadSalud.pdf.

[34] CONSEJO NACIONAL DE OPERACIÓN (CNO). Acuerdo 1347 de 2020. {En línea}. {16 de septiembre de 2020}. Disponible en: https://www.cno.org.co/content/acuerdo-1347-por-el-cual-se-aprueba-la-actualizacion-de-la-guia-de-ciberseguridad.

[35] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Lineamientos de política para ciberseguridad y ciberdefensa: CONPES 3701 de 2011. {En línea}. {14 de julio de 2011}. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3701.pdf.

[36] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Política Nacional de Seguridad Digital: CONPES 3854 de 2016. {En línea}. {11 de abril de 2016}. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

[37] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Política nacional de confianza y seguridad digital: CONPES 3995 de 2020. {En línea}. {1 de julio de 2020}. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf.

Tabla 2. Normas jurídicas relacionadas al proceso seguridad digital

Norma	Descripción	Alcance
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.	Define el concepto de firma digital y entidad de certificación.
Ley 600 de 2000	Por la cual se expide el Código de Procedimiento Penal.	Denuncia, investigación, gestión de la prueba pericial, peritaje, cadena custodia.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.	Políticas y lineamientos de Tecnologías de la Información.
Decreto 1413 de 2017	Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078d de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.	Ciudadanos digitales.
Decreto 1704 de 2012	Por medio del cual se reglamenta el artículo 52 de la Ley 1453 de 2011, se deroga el Decreto 075 de 2006 y se dictan otras disposiciones.	Gobierno en línea.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.	Denuncia, investigación, gestión de la prueba pericial, peritaje, cadena custodia.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.	Gobierno en línea.
Decreto 415 de 2016	Definición de los lineamientos para el fortalecimiento institucional en materia de	Lineamientos para el fortalecimiento institucional.

Norma	Descripción	Alcance
	Tecnologías de la Información y las Comunicaciones.	
Resolución 0-2369 de 2016	Por medio de la cual se adopta el Manual de procedimientos para cadena de custodia y se deroga la Resolución 0-1874 de 21 de junio de 2016.	Procedimiento manejo de evidencias en cadenas de custodia
Resolución 0312 de 2019	Por la cual se definen los Estándares Mínimos del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST.	Establecer los estándares Mínimos del Sistema de gestión de Seguridad y Salud en el trabajo SG-SST para las personas naturales y jurídicas señaladas en el articulo2° de este acto Administrativo.
Acuerdo 1347 de 2020	Por el cual se aprueba la actualización de la Guía de Ciberseguridad.	Guía de ciberseguridad.
CONPES 3701 de 2011	Lineamientos de política en ciberseguridad y ciberdefensa, orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.	Lineamientos de política para ciberseguridad y ciberdefensa.
CONPES 3854 de 2016	Política nacional de seguridad digital.	Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.
CONPES 3995 de 2020	Política nacional de confianza y seguridad digital.	Confianza y seguridad digital.

Fuente: Propia

5 DISEÑO METODOLÓGICO

La metodología de la investigación implica la aplicación de una serie de reglas y estrategias que especifican como se puede profundizar un problema y se concreta en un proceso sistemático que comprende acciones, actividades y tareas[38].

El enfoque metodológico es de naturaleza cualitativa, enfatizándose en los datos, la riqueza interpretativa, la contextualización del ambiente o entorno, los detalles y las experiencias únicas.

Se pretende realizar un análisis cualitativo, sobre la información obtenida del proceso de seguridad digital implementado en una empresa del sector eléctrico en Colombia. El estudio se fundamenta en un proceso inductivo, donde se logra explorar, describir y generar perspectivas teóricas.

Conforme al objeto de estudio, la población está definida por el conjunto de interesados que interactúan en el proceso de seguridad digita definido en el sistema de gestión integral de una empresa del sector eléctrico en Colombia.

Se aplicará distintos instrumentos de recolección de información, tales como: revisión documental y entrevistas.

Los métodos para la consecución de los objetivos son los siguientes:

- Revisión electrónica del proceso de seguridad digital en una empresa del sector eléctrico en Colombia.
- Revisión bibliográfica.
- Integración de referencias.
- Analizar lecciones aprendidas.
- Hacer evaluaciones de eficiencia y eficacia de los controles de seguridad.
- Definir el plan de mejoramiento para el proceso de seguridad digital.

[38] PALELLA, S.; MARTINS, F. Metodología de la Investigación Cuantitativa. Caracas: FEDUPEL, 2006.

6 DESARROLLO DE LOS OBJETIVOS

6.1 PROCESO DE SEGURIDAD DIGITAL EN EMPRESAS DEL SECTOR ELÉCTRICO EN COLOMBIA

Examinando el Sistema de Gestion Integral de una empresa del sector eléctrico en Colombia, se identifica el proceso de Seguridad Digital cómo parte del macroproceso Gestión de Tecnología e Información.

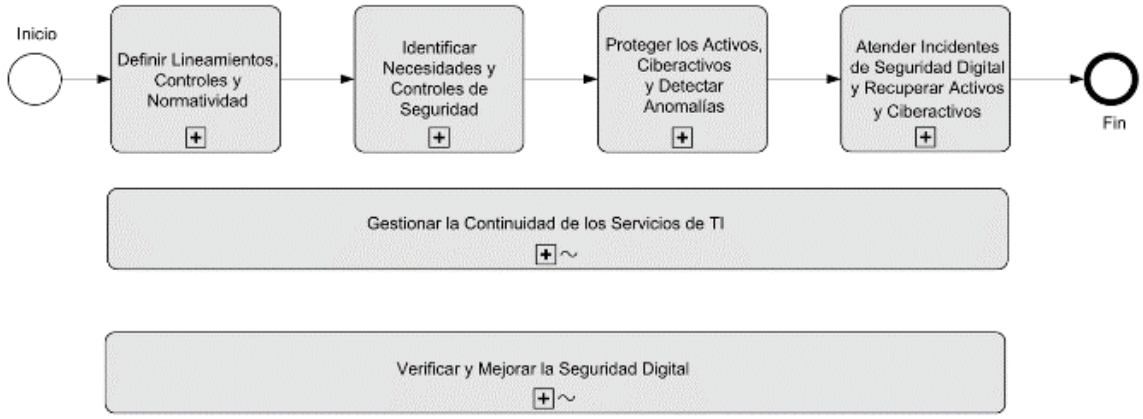
6.1.1 Descripción del proceso

El proceso se encarga de poner en operación la Gestión de Seguridad Digital y Continuidad, tomando como referencia la normatividad nacional e internacional, para los activos de información y ciber-activos definidos en el alcance del sistema de gestión de seguridad de la información, en busca de minimizar los riesgos de seguridad que amenacen la confidencialidad, integridad y continuidad de los servicios de TI, mediante la implementación de controles de seguridad requeridos para mitigar los riesgos de ataques cibernéticos y proteger los activos organizacionales como: Información crítica, activos críticos de operación y ciber-activos. El proceso está compuesto las siguientes actividades[39].

- Definir lineamientos, controles y normatividad.
- Identificar necesidades y controles de seguridad.
- Proteger los activos, ciber-activos y detectar anomalías.
- Atender incidentes de seguridad digital y recuperar activos y ciber-activos.
- Gestionar la continuidad de los servicios de TI.
- Verificar y mejorar la seguridad digital.

[39] GÓMEZ, F. L.; FERNÁNDEZ, R. P. P. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el esquema nacional de seguridad. España: AENOR, 2018. 57p – 132p.

Figura 4. Proceso Seguridad Digital



Fuente: Propia

6.1.2 Objetivo del proceso

Desarrollar, mantener y evolucionar las capacidades de seguridad de la información y ciberseguridad (gobierno, identificación, prevención, detección, protección, defensa y recuperación), con el propósito de habilitar una operación sostenible y segura en la prestación de los servicios y proteger la información crítica para los diferentes grupos de interés[40].

6.1.3 Alcance del proceso

Definir lineamientos, controles y normatividad. Con el propósito de verificar, mantener y mejorar la seguridad digital.

6.1.4 Procedimientos

- Definir lineamientos, controles y normatividad

Comprende la definición o actualización de la estrategia, arquitectura, gobierno, la estructura, las necesidades y requisitos de seguridad digital, así como los planes de implementación, el marco normativo aplicable y los planes de sensibilización y capacitación del proceso de seguridad digital.
El objetivo es definir y actualizar la estrategia, arquitectura, gobierno, la estructura, las necesidades y requisitos de seguridad digital, así como los planes de

[40] FERNÁNDEZ, S. C. M.; PIATTINI, V. M. Modelo para el gobierno de las TIC basado en las normas ISO. España: AENOR, 2012. 83p – 88p.

implementación, el marco normativo aplicable y los planes de sensibilización y capacitación del proceso de seguridad digital.

- Identificar necesidades y controles de seguridad

Identificación de los riesgos y controles de seguridad digital mediante la aplicación de la metodología definida para administrar los riesgos en los procesos y proyectos, así como realizar las capacitaciones y entrenamiento en seguridad digital.
El objetivo es el de identificar las necesidades de seguridad digital mediante la aplicación de una metodología definida para administrar el riesgo en los procesos y proyectos con el fin de definir los controles de seguridad digital[41].

- Proteger los activos, ciber-activos y detectar anomalías

Identificación y protección de los activos, ciber-activos e instalaciones físicas críticos ante las amenazas y vulnerabilidades de seguridad de la información y ciberseguridad.
El objetivo es el de identificar e implementar los controles de seguridad digital apropiados para minimizar los riesgos detectados en los servicios de infraestructura críticos.

- Atender incidentes de seguridad digital y recuperar activos y ciber-activos

Este procedimiento define la ejecución de las acciones para atender los incidentes de segundo nivel en temas de seguridad digital, la restauración de las capacidades tecnológicas afectadas, así como, documentación y divulgación de las lecciones aprendidas.
El objetivo es definir e implementar las actividades adecuadas para reaccionar frente a un incidente de ciberseguridad identificado y mitigar su impacto, mediante la atención del mismo o de la aplicación de planes de resiliencia que permitan restaurar las capacidades que se hayan visto afectadas por el evento[42].

- Gestionar la continuidad de los servicios de TI

El procedimiento comprende el análisis de los impactos de los servicios de tecnología críticos ante incidentes de seguridad digital con el fin de formular las estrategias necesarias para la operación de los mismos, esta actividad incluye la verificación periódica del plan de recuperación para la mejora continua.

[41] CHICANO, T. E. Gestión de servicios en el sistema informático. España: IC Editorial, 2015. 22p – 27p.
[42] CHICANO, T. E. Gestión de incidentes de seguridad informática. España: IC Editorial, 2015. 9p – 17p, 151p – 187p.

El objetivo es definir las estrategias de continuidad de los servicios de tecnología basado en un análisis de impacto de los mismos con el fin de gestionar los niveles de resiliencia mínimos para la operación de los servicios de TI[43].

- Verificar y mejorar la seguridad digital

El procedimiento comprende la evaluación de la implementación de las estrategias de seguridad digital, en el cumplimiento de la eficacia de los mecanismos de la operación y controles de la seguridad digital, teniendo en cuenta las métricas y planes definidos en la vigencia.
El objetivo es el de verificar y evaluar el cumplimiento de las medidas de Seguridad Digital, sus resultados y el cumplimiento de los ANS de los servicios de TI, para identificar planes de mejoramiento que se generen como resultado de la evaluación desempeño del proceso.

6.2 MECANISMOS DE LA OPERACIÓN Y SEGURIDAD DIGITAL EN EMPRESAS DEL SECTOR ELÉCTRICO EN COLOMBIA

Con el propósito de definir el tratamiento de controles para la seguridad de información y ciber-activos críticos en los procesos o proyectos de una empresa del sector eléctrico en Colombia, fueron valorados los riegos que impactan los objetivos estratégicos.

6.2.1 Análisis de riesgos

La matriz de riesgos o tablero de calor es un instrumento que permite clasificar los riesgos identificados según su nivel de riesgo. Permite visualizar la ubicación espacial de los mismos y priorizar los riesgos para hacer más efectiva la gestión.

A continuación, en se explica las zonas del mapa de calor y las acciones que se recomiendan tomar en cada una de ellas.

[43] MINTIC. Seguridad y privacidad de la información: Guía para la gestión y clasificación de incidentes de seguridad de la información. Ministerio de Tecnologías de la Información y las Comunicaciones, 2009. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.

Figura 5. Matriz de calificación de riesgos

PROBABILIDAD		CONSECUENCIA				
		Mínima	Menor	Moderada	Mayor	Máxima
		1	2	4	8	16
Muy alta	5	5	10	20	40	80
Alta	4	4	8	16	32	64
Media	3	3	6	12	24	48
Baja	2	2	4	8	16	32
Muy baja	1	1	2	4	8	16

Fuente: Propia

- Riesgo externo (zona roja): Riesgos de máxima prioridad que requieren acciones inmediatas. Si la implementación de controles requiere inversión, se deberá realizar un análisis económico para determinar la viabilidad de aplicación. Este tipo de riesgos debe ser monitoreado permanentemente.

- Riesgo alto (zona naranja): Riesgos de alta prioridad que requieren de acciones que pueden ser ejecutadas a corto plazo. Si la implementación de controles requiere inversión, se deberá realizar un análisis económico para determinar la viabilidad de aplicación. Este tipo de riesgos deben ser monitoreados permanentemente.

- Riesgo tolerable (zona amarilla): Riesgos de prioridad moderada que requieren acciones que pueden ser ejecutadas a mediano plazo. Generalmente no debe requerir inversión y su aplicación debe ser aprobada por el responsable del proceso de análisis.

- Riesgo aceptable (zona verde): Riesgos de baja prioridad que no es necesario realizar acciones adicionales o que el control actual existente mantiene los niveles de riesgos en los aceptados por la organización.

6.2.2 Determinación del valor total del activo de información y/o ciber-activo

A partir de los valores establecidos en cada una de las características por parte de los responsables de los procesos, se determina el valor total del activo de información, el cuál sería el valor más alto que haya obtenido el activo en las

valoraciones realizadas. Este valor permite establecer de manera práctica una escala de valorización única comparable para la totalidad de los activos de información, independientemente de los dueños de procesos y de las características afectadas.

De acuerdo con la escala de valoración de la metodología, la siguiente tabla muestra un ejemplo de posibles valores de características y el valor total del activo de información y/o ciber-activo.

Figura 6. Escala de valoración

Confidencialidad	Integridad	Disponibilidad	Valor total del activo
Catastrófica	Catastrófica	Catastrófica	Catastrófica
Catastrófica	Catastrófica	Moderada	Catastrófica
Moderada	Mayor	Moderada	Mayor
Insignificante	Catastrófica	Insignificante	Catastrófica
Menor	Menor	Mayor	Mayor
Mayor	Insignificante	Mayor	Mayor

Fuente: Propia

6.2.3 Definición de riesgos

Tabla 3. Definición de riesgos

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
R1	Uso de equipos no autorizados, dispositivos móviles no autorizados, accesos lógicos no autorizados o conexiones no autorizadas.	Falta de proceso disciplinario en caso de incidentes de seguridad y privacidad. Falta de reglas de negocio para el correcto uso de las telecomunicaciones y mensajería. Inadecuada seguridad física. Desconocimiento, negligencia o curiosidad. Falta o fallas en la producción de reportes de gestión. Ausencia de procedimientos, documentación o inadecuada transferencia de conocimiento. Falta de monitoreo de logs de seguridad. Falta de controles para el monitoreo de la red. Falta de revisiones gerenciales periódicas. No se bloquean las estaciones de trabajo desatendidas. Política de uso aceptable insuficiente. No hay mecanismos de monitoreo para dispositivos móviles que acceden el correo corporativo. Falta de políticas de uso de dispositivos móviles Falta o ausencia de reglas, procedimientos o guías de seguridad y privacidad. Falta de protección de tráfico sensible.	Indisponibilidad del servicio de conectividad. Indisponibilidad del servicio de conectividad de TO. Indisponibilidad de los servicios de TI. Demora en la gestión de la operación del servicio de energía. Fuga de información sensible.	**40**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
		Accesos sin restricciones. Falta de concientización en reglas y procedimientos. Disposición o reúso de medios sin borrado seguro apropiado. Falta de procedimientos o procesos para identificar y gestionar registros y activos críticos. Mecanismos inadecuados de destrucción. Falta de supervisión en los trabajos de aseo. Falta de procesos de disposición de información.		
R2	Suplantación (IP Address Spoofing, Man in middle attack, Replay attack, DDoS, DNS poisioning, Trojan Horses).	Fallos conocidos de software. Servicios innecesarios habilitados. Líneas de comunicación no protegidas. Fallos en la configuración y actualización del antivirus. Deficiencias en la arquitectura de seguridad. Falta de controles criptográficos o controles de red. Transmisión de contraseñas en texto plano. Políticas inadecuadas de firewall. Falta de concientización. Falta de líneas bases de seguridad. Falta de monitoreo de logs de seguridad. Falta de controles para el monitoreo de la red. Falta de identificación y autenticación para el emisor y receptor. Falta de protección de conexiones a redes públicas. Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de procedimientos para identificación y evaluación de riesgos. Falta de mecanismos de monitoreo de brechas de seguridad y privacidad. Falta de procedimientos para el reporte de debilidades de seguridad y privacidad. Uso de software no autorizado. Falta de prácticas de desarrollo seguro. Falta de seguimiento logs y correlación de eventos. Obsolescencia tecnológica.	Suplantación de identidad para acceso a los servicios de TO. Indisponibilidad del servicio de conectividad de TO. Indisponibilidad de los servicios de TI. Fuga de información sensible. Perdida o fuga de información sensible que puede poner en riesgo la operación del Centro de Control. Fallo en los equipos del Centro de Control o de los elementos de control de la red eléctrica por ataques DDoS.	**40**
R3	Fallos en los procesos de continuidad generando perdidas en las capacidades de recuperación.	Falta de consistencia y prácticas de planes de continuidad. Políticas inadecuadas o inconsistentes de continuidad. Fallo en el cumplimiento de tiempos de recuperación objetivo (RTO), puntos de recuperación objetivo (RPO) en caso de desastre. Falta o inadecuada estrategia de recuperación. Falta de procesos de evaluación de riesgo o prácticas de continuidad del proveedor. Falta de mecanismos de evaluación de las pruebas o planes de continuidad.	Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Indisponibilidad de la infraestructura tecnológica necesaria para la operación del centro de control. Indisponibilidad de los enlaces de comunicaciones. Demora en la recuperación de los servicios de energía. Desplazamiento de personal operativo a las subestaciones para maniobrar los dispositivos electrónicos.	**32**
R4	Incumplimiento Contractual.	Incumplimiento de requerimientos legales o legislativos. Obligaciones contractuales no identificadas. Falta de coordinación entre las áreas. Riesgos contractuales no identificados. Falta de monitoreo de cláusulas contractuales. Desconocimiento de las políticas de retención de	Dificultad en el reemplazo de cargos en el Centro de Control por vacaciones, incapacidades, etc. y demoras en los tiempos de atención al soporte por parte de los contratistas.	**32**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
		información. Falta de procedimientos para establecer mecanismos de protección de propiedad intelectual. Falta de acompañamiento legal en las nuevas iniciativas.	Dificultad en el reemplazo de cargos del personal de subestaciones y líneas por vacaciones, incapacidades, etc. y demoras en los tiempos de atención al soporte por parte de los contratistas. Indisponibilidad de los servicios de soporte o de comunicaciones contratados con terceros.	
R5	Terrorismo.	Ubicación inadecuada de equipos. Falta disposiciones sobre seguridad y privacidad en los contratos con terceros. Falta de procedimientos para el reporte de debilidades de seguridad y privacidad. Falta de supervisión en los trabajos de aseo. Falta de protección de conexiones a redes públicas. Falta de planes de continuidad. Procedimientos de reclutamiento o terminación inadecuados. Falta de protecciones y controles físicos.	Indisponibilidad de los sistemas de información que soportan la operación del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Daño de equipos. Demoras en la operación de la red eléctrica. Destrucción de las instalaciones del Centro de Control. Demora en la recuperación de los servicios de energía. Desplazamiento de personal operativo a las subestaciones para maniobrar los dispositivos electrónicos.	**32**
R6	Intrusiones e interrupciones en la plataforma SCADA.	Falta de prácticas seguras de los proveedores o terceros. Deficiencias en los controles de accesos para proveedores o terceros. Contraseñas compartidas. Deficiencia en las cláusulas o contratos con terceros. Falta de concientización de mecanismos de ataque a ingeniería social. Falta de conocimiento de la criticidad de la información. Desconocimiento. Retiro o renuncia del empleado. Falta de mecanismos de control de intrusiones en la red. Contraseñas por defecto.	Indisponibilidad del servicio SACADA. Demora en la recuperación de los servicios de energía. Indisponibilidad para maniobrar los dispositivos electrónicos del servicio de energía eléctrica. Fuga de información sensible.	**32**
R7	Amenazas de usuario final (Spam, Phishing, Spear Phishing, Spoofing, Virus, Worms, Malware, BotNet, Criptomineria, Macros infectadas, Ransomware).	Falta de concientización. Fallos conocidos de software. Servicios innecesarios habilitados. Líneas de comunicación no protegidas. Falta de controles criptográficos o controles de red. Ausencia de revisiones técnicas. Fallos en la configuración y actualización del antivirus. Deficiencias en la arquitectura de seguridad. Transmisión de contraseñas en texto plano. Políticas inadecuadas de Firewall. Falta de monitoreo de logs de seguridad.	Demora en la atención de requerimientos. Latencia en la red de datos. Indisponibilidad del servicio de telecomunicaciones. Indisponibilidad de acceso a los dispositivos electrónicos de las subestaciones por malware en los equipos de los operadores del Centro de Control o de los técnicos	**32**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
		Falta de controles para el monitoreo de la red. Falta de identificación y autenticación para el emisor y receptor. Falta de actualización de antivirus. Falta de líneas bases de seguridad. Falta de protección de conexiones a redes públicas. Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de procedimientos para identificación y evaluación de riesgos. Falta de mecanismos de monitoreo de brechas de seguridad y privacidad. Falta de procedimientos para el reporte de debilidades de seguridad y privacidad. Uso de software no autorizado. ingeniería Social.	de subestaciones y líneas o contratistas.	
R8	Ataques a sitios y aplicaciones Web.	Fallos conocidos de software. Servicios innecesarios habilitados. Líneas de comunicación no protegidas. Fallos en la configuración y actualización Antivirus. Deficiencias en la arquitectura de seguridad. Falta de controles criptográficos o controles de red. Transmisión de contraseñas en texto plano. Políticas inadecuadas de Firewall. Falta de líneas bases de seguridad. Falta de monitoreo de logs de seguridad. Falta de controles para el monitoreo de la red. Falta de identificación y autenticación para el emisor y receptor. Falta de protección de conexiones a redes públicas. Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de procedimientos para identificación y evaluación de riesgos. Falta de mecanismos de monitoreo de brechas de seguridad y privacidad. Falta de procedimientos para el reporte de debilidades de seguridad y privacidad. Uso de software no autorizado. Falta de prácticas de desarrollo seguro. Falta de seguimiento logs y correlación de eventos. Obsolescencia tecnológica.	Indisponibilidad de gestión de los equipos de comunicaciones. Indisponibilidad de acceso a la gestión de las aplicaciones y/o gestión de dispositivos de las subestaciones eléctricas y del centro de control.	**32**
R9	Eventos políticos (paro, asonada, golpe de estado).	Falta de contacto con las autoridades. Falta de planes de continuidad.	Indisponibilidad de la red de comunicaciones por daño de equipos o enlaces de comunicaciones. Indisponibilidad de los sistemas de información que soportan la operación del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Daño de equipos. Demoras en la operación de la red eléctrica. Destrucción de las	**32**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
			instalaciones del Centro de Control.	
R10	Hacktivismo.	Fallos conocidos de software. Servicios innecesarios habilitados. Líneas de comunicación no protegidas. Falta de controles criptográficos o controles de red. Ausencia de revisiones técnicas. Fallos en la configuración y actualización de antivirus. Deficiencias en la arquitectura de seguridad. Falta de líneas bases de seguridad. Falta de controles de acceso a internet. Transmisión de contraseñas en texto plano. Políticas inadecuadas de firewall. Falta de monitoreo de logs de seguridad. Falta de controles para el monitoreo de la red. Falta de identificación y autenticación para el emisor y receptor. Falta de protección de conexiones a redes públicas. Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de procedimientos para identificación y evaluación de riesgos. Falta de mecanismos de monitoreo de brechas de seguridad y privacidad. Falta de procedimientos para el reporte de debilidades de seguridad y privacidad. Uso de software no autorizado. Problemas de Diseño.	Indisponibilidad de la información para ser registrada en los sistemas de información. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos de las subestaciones. Fallo de equipos. Maniobras en componentes electrónicos de la red eléctrica. Indisponibilidad de los sistemas de información que soportan la operación del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Fallo de equipos. Indisponibilidad de gestión de los equipos de comunicaciones. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI.	**24**
R11	Amenazas avanzadas persistentes (Interceptación de Conexiones o sesiones, APT, Session Hijacking, Spoofing, Eavesdropping, Compromised Key).	Fallos conocidos de software. Servicios innecesarios habilitados. Deficiencias en la arquitectura de seguridad. Falta de protección de tráfico sensible. Líneas de comunicación no protegidas. Falta de controles criptográficos o controles de red. Transmisión de contraseñas en texto plano. Políticas inadecuadas de Firewall. Falta de líneas bases de seguridad. Falta de monitoreo de logs de seguridad. Falta de controles para el monitoreo de la red. Falta de identificación y autenticación para el emisor y receptor. Falta de protección de conexiones a redes públicas. Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de procedimientos para identificación y evaluación de riesgos. Falta de mecanismos de monitoreo de brechas de seguridad y privacidad. Falta de procedimientos para el reporte de debilidades de seguridad y privacidad. Uso de software no autorizado. Falta de prácticas de desarrollo seguro.	Perdida o fuga de información sensible que puede poner en riesgo la operación de la red eléctrica. Indisponibilidad de gestión de los equipos de comunicaciones. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Perdida o fuga de información sensible que puede poner en riesgo la operación del Centro de Control.	**24**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
		Falta de seguimiento logs y correlación de eventos Obsolescencia tecnológica.		
R12	Intrusión en el sistema.	Fallos conocidos de software. Servicios innecesarios habilitados. Líneas de comunicación no protegidas. Falta de controles criptográficos o controles de red. Ausencia de revisiones técnicas. Fallos en la configuración y actualización de antivirus. Deficiencias en la arquitectura de seguridad. Falta de líneas bases de seguridad. Falta de controles de acceso a internet. Transmisión de contraseñas en texto plano. Políticas inadecuadas de firewall. Falta de monitoreo de logs de seguridad. Falta de controles para el monitoreo de la red. Falta de identificación y autenticación para el emisor y receptor. Falta de protección de conexiones a redes públicas. Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de procedimientos para identificación y evaluación de riesgos. Falta de mecanismos de monitoreo de brechas de seguridad y privacidad. Falta de procedimientos para el reporte de debilidades de seguridad y privacidad. Uso de software no autorizado. Falta de prácticas de desarrollo seguro. Falta de seguimiento logs y correlación de eventos. Obsolescencia tecnológica.	Perdida o fuga de información sensible que puede poner en riesgo la operación de la red eléctrica. Manipulación del funcionamiento del Sistema SCADA. Maniobras no autorizadas en componentes electrónicos. Se podría generar ataques de denegación de servicio a los equipos de comunicaciones. Indisponibilidad del servicio de conectividad de TO. Indisponibilidad de los servicios de TI. Fuga de información sensible.	**24**
R13	Robo o fuga de Información.	Ausencia o incorrecta clasificación de información. Controles inapropiados en medios removibles. Dependencia de terceros para el manejo de información. Desconocimiento, negligencia o curiosidad. Empaque inadecuado de registros de información física. Falta de auditoría y control interno. Falta de concientización. Falta de concientización en reglas y procedimientos. Falta de control de activos fuera de las instalaciones. Falta de controles para la copia de información. Falta de líneas bases de seguridad. Falta de mecanismos de autorización en locaciones de procesamiento de información. Falta de mecanismos de monitoreo de brechas de seguridad y privacidad. Falta de políticas de contraseñas o módulos de seguridad. Falta de políticas de uso de dispositivos móviles. Falta de procedimiento de registro de supervisión. Falta de procedimientos de registro y baja de usuarios. Falta de procedimientos formales de control de documentación. Falta de procedimientos o procesos para identificar y	Indisponibilidad de gestión de los equipos de comunicaciones. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI y TO. Pérdida de información.	**24**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
		gestionar registros y activos críticos. Falta de procedimientos para clasificar información. Falta de procedimientos para el reporte de debilidades de seguridad y privacidad. Falta de proceso disciplinario en caso de incidentes de seguridad y privacidad. Falta de proceso formal para la revisión de privilegios de acceso. Falta de procesos de disposición de información. Falta de protección en el almacenamiento. Falta de recursos para inversión en controles de seguridad. Falta de reglas de negocio de escritorio limpio. Falta de revisiones gerenciales periódicas. Falta de supervisión en los trabajos de aseo. Falta disposiciones sobre seguridad y privacidad en los contratos con empleados y terceros. Falta disposiciones sobre seguridad y privacidad en los contratos con terceros. Falta o ausencia de reglas, procedimientos o guías de seguridad y privacidad. Inadecuada seguridad física. Insatisfacción del Empleado. Insuficiente entrenamiento en seguridad y privacidad. Mecanismos inadecuados de destrucción. Obligaciones contractuales no identificadas.		
R14	Manipulación física: Robo, daño, perdida de documentos / medios / equipos.	Accesos mal definidos sobre plataformas y aplicativos. Ausencia de procedimientos, documentación o inadecuada transferencia de conocimiento. Ausencia o incorrecta clasificación de información. Controles inapropiados en medios removibles. Dependencia de terceros para el transporte de registros. Desconocimiento, negligencia o curiosidad. Empaque inadecuado de registros de información física. Falta de control de activos fuera de las instalaciones. Falta de controles para la copia de información. Falta de esquemas de reemplazo periódico. Falta de mecanismos de autorización en locaciones de procesamiento de información. Falta de mecanismos de monitoreo de brechas de seguridad y privacidad. Falta de políticas de uso de dispositivos móviles. Falta de procedimientos o procesos para identificar y gestionar registros y activos críticos. Falta de procedimientos para el reporte de debilidades de seguridad y privacidad. Falta de proceso disciplinario en caso de incidentes de seguridad y privacidad. Falta de procesos de disposición de información. Falta de protección en el almacenamiento. Falta de reglas de negocio de escritorio limpio. Falta de revisiones gerenciales periódicas. Falta de supervisión en los trabajos de aseo. Inadecuada seguridad física. Inadecuados procedimientos de control de acceso físico. Insatisfacción del empleado. locación en zona sensible a radiación	Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Pérdida económica por afectación de equipos de comunicación. Pérdida de información sensible. Indisponibilidad del servicio de conectividad de TO. Indisponibilidad de los servicios de TI. Demora en la gestión de la operación del servicio de energía. Fuga de información sensible. Reemplazo de equipos afectados.	**24**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
		electromagnética. Mantenimiento insuficiente. Mecanismos inadecuados de destrucción. Procedimientos de reclutamiento o terminación inadecuados. Zona sensible a humedad o polvo. Zona sensible a variaciones de voltaje.		
R15	Abuso de privilegios (Insider Threat) o actuaciones malintencionadas.	Falta de protección en las tablas de contraseñas. Deficiencias en la gestión de contraseñas Falta de identificación y autenticación para el emisor y receptor. No se bloquean las estaciones de trabajo desatendidas. Falta de Auditoria. Accesos mal definidos sobre plataformas y aplicativos. Falta de concientización. Falta de proceso disciplinario en caso de incidentes de seguridad y privacidad. Falta de procedimientos de registro y baja de usuarios. Falta de proceso formal para la revisión de privilegios de acceso. Falta de separación de ambientes de producción, pruebas y desarrollo. Falta de pruebas de seguridad en el software. Falta de políticas de contraseñas o módulos de seguridad. Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de líneas bases de seguridad. Falta de auditoria periódicas. Falta de procedimientos para identificación y evaluación de riesgos. Falta de logs. Insatisfacción del empleado. Falta de mecanismos de identificación y autenticación. Ausencia de revisiones técnicas. Deficiencia en las políticas de contratación y controles. Deficiencia en la asignación de privilegios.	Indisponibilidad del servicio de conectividad. Ataques de DDoS a los RTU o IDE a través de las WorkStations. Fuga de información. Afectación del funcionamiento de los equipos de comunicaciones degradando el servicio y afectando la oportunidad de la gestión de la red eléctrica.	**24**
R16	Fallos de telecomunicaciones.	Problemas de cableado. Punto único de fallo. Falta de un proveedor alterno. Falta de planes de continuidad. Falta o fallo de respaldos. Falta o fallo en los equipos de monitoreo. Falta de mecanismos de monitoreo. Líneas de comunicación no protegidas. Ubicación inadecuada de equipos. Falta de SLAs.	Indisponibilidad de gestión de los equipos de comunicaciones. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Indisponibilidad de la gestión de los equipos remotos generando demoras en el restablecimiento y operación de la red eléctrica. Indisponibilidad de los enlaces de comunicaciones. Demora en la recuperación de los servicios de energía. Desplazamiento de personal	**24**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
			operativo a las subestaciones para maniobrar los dispositivos electrónicos.	
R17	Fallo o pérdida de energía.	Zona sensible a variaciones de voltaje. Inestabilidad eléctrica. Ausencia de mecanismos de polo a tierra. Ausencia de Unidades de Respaldo de Potencia. Falta de un proveedor alterno. Falta de planes de continuidad. Falta o fallo en los equipos de monitoreo. Falta o fallo de respaldos. Falta de mecanismos de monitoreo. Ubicación inadecuada de equipos. Falta de acuerdos de cumplimiento. Falta de SLAs.	Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Indisponibilidad de los sistemas de información que soportan la operación del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Indisponibilidad para la gestión del servicio de conectividad TO. Pérdida económica por afectación de equipos de comunicación.	**24**
R18	Fallo suministro de agua o fallo de aire acondicionado.	Falta o fallo en los equipos de monitoreo. Falta de mecanismos de monitoreo. Falta de un proveedor alterno. Falta o fallo de respaldos. Ubicación inadecuada de equipos. Falta de acuerdos de cumplimiento. Falta de SLAs.	Degradación en el servicio de conectividad. Recalentamiento de equipos de comunicaciones. Latencia en la red de telecomunicaciones TO.	**24**
R19	Fuego.	Falta de concientización en seguridad y privacidad. Falta de contacto con las autoridades. Falta de entrenamiento en elementos de respuesta contra incendio. Falta de planes de continuidad. Falta de protecciones y controles físicos. Inadecuada seguridad física. Ausencia de mecanismos de polo a tierra. Desconocimiento, negligencia o curiosidad. Zona sensible a variaciones de voltaje. Ubicación inadecuada de equipos.	Indisponibilidad de los sistemas de información que soportan la operación del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Daño de equipos. Demoras en la operación de la red eléctrica. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Demora en la recuperación de los servicios de energía. Desplazamiento de personal operativo a las subestaciones para maniobrar los dispositivos electrónicos. Reemplazo de los equipos de comunicaciones. Afectación de vidas humanas. Pérdida económica por	**24**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
			afectación de equipos de comunicación.	
R20	Robo de identidad.	Falta de concientización. Fallos conocidos de software. Servicios innecesarios habilitados. Líneas de comunicación no protegidas. Falta de controles criptográficos o controles de red. Ausencia de revisiones técnicas. Fallos en la configuración y actualización de antivirus. Deficiencias en la arquitectura de seguridad. Falta de líneas bases de seguridad. Falta de controles de acceso a internet. Transmisión de contraseñas en texto plano. Políticas inadecuadas de firewall. Falta de monitoreo de logs de seguridad. Falta de controles para el monitoreo de la red. Falta de identificación y autenticación para el emisor y receptor. Falta de protección de conexiones a redes públicas. Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de procedimientos para identificación y evaluación de riesgos. Falta de mecanismos de monitoreo de brechas de seguridad y privacidad. Falta de procedimientos para el reporte de debilidades de seguridad y privacidad. Uso de software no autorizado. Falta de prácticas de desarrollo seguro. Falta de seguimiento logs y correlación de eventos. Obsolescencia tecnológica.	Suplantación de identidad para acceso a los servicios de TO. Indisponibilidad del servicio de conectividad de TO. Indisponibilidad de los servicios de TI. Fuga de información sensible. Perdida o fuga de información sensible que puede poner en riesgo la operación del Centro de Control. Acceso no autorizado al Sistema SCADA.	**24**
R21	Suplantación de identidad.	Falta de concientización. Fallos conocidos de software. Servicios innecesarios habilitados. Líneas de comunicación no protegidas. Falta de controles criptográficos o controles de red. Ausencia de revisiones técnicas. Fallos en la configuración y actualización de antivirus. Deficiencias en la arquitectura de seguridad. Falta de líneas bases de seguridad. Falta de controles de acceso a internet. Transmisión de contraseñas en texto plano. Políticas inadecuadas de firewall. Falta de monitoreo de logs de seguridad. Falta de controles para el monitoreo de la red. Falta de identificación y autenticación para el emisor y receptor. Falta de protección de conexiones a redes públicas. Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de procedimientos para identificación y evaluación de riesgos. Falta de mecanismos de monitoreo de brechas de seguridad y privacidad. Falta de procedimientos para el reporte de debilidades de seguridad y privacidad.	Perdida o fuga de información sensible que puede poner en riesgo la operación del servicio de energía eléctrica. Acceso no autorizado al Sistema SCADA. Acceso no autorizado a componentes electrónicos de las subestaciones.	**20**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
		Uso de software no autorizado. Falta de prácticas de desarrollo seguro. Falta de seguimiento logs y correlación de eventos. Obsolescencia tecnológica.		
R22	Fenómenos naturales (pulsos electromagnéticos, radiación, terremoto, fenómenos climáticos, polvo, corrosión, pandemia).	Zona sensible a humedad o polvo. Zona sensible a variaciones de temperatura. locación en zona sensible a radiación electromagnética. Ubicación inadecuada de equipos. Falta o fallo en los equipos de monitoreo. Falta de mecanismos de monitoreo. locación en zona sísmica. Falta de contacto con las autoridades. Falta de planes de continuidad. Falta de condiciones y ambiente saludables. Falta de planes de continuidad. Insuficiencia de recursos. Falta de compromiso gerencial en temas de seguridad y privacidad. Erupción volcánica.	Indisponibilidad de los sistemas de información que soportan la operación del sistema eléctrico y del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Daño de equipos. Demoras en la operación de la red eléctrica. Destrucción de las instalaciones de la subestación. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Demora en la recuperación de los servicios de energía. Reemplazo de los equipos de comunicaciones. Desplazamiento de personal operativo a las subestaciones para maniobrar los dispositivos electrónicos. Pérdida económica por afectación de equipos de comunicación.	**20**
R23	Disponibilidad de personal.	Falta de reglas y procedimientos para la salida de empleados. Políticas de recursos humanos inadecuadas. Falta de coordinación entre las áreas. Insuficiencia de recursos. Falta de SLAs definidos con proveedores. Responsabilidades no documentadas. Falta de gestión de recursos críticos. Falta de planes de continuidad. Falta de condiciones y ambiente saludables. Insatisfacción del empleado.	Falta de personal para operación del servicio de energía eléctrica. Sobrecarga laboral en trabajadores del centro de control. Falta de personal para soporte y operación de la red de telecomunicaciones de TO.	**20**
R24	Falta de apoyo de la alta dirección.	Falta de concientización. Falta de apoyo corporativo. Falta de presupuesto. Falta de gobierno. Falta de auditoría. Falta de un marco de control.	Falta de recursos para la operación del sistema eléctrico. Falta de recursos para soporte y operación de la red de telecomunicaciones de TO. Degradación en el servicio de conectividad.	**20**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
R25	Demanda por incumplimiento en la protección de la privacidad de los datos.	Falta de conocimiento de la información personal. Falta de conocimiento en las consecuencias del compromiso a los datos sensibles. Controles inadecuados para la protección de la privacidad de información. Falta de protecciones para la privacidad de datos. Falta mecanismos para la atención de solicitudes sobre protección de datos personales.	Sanciones por manejo indebido de datos personales.	**20**
R26	Incidentes nucleares o químicos.	Falta de contacto con las autoridades. Falta de planes de continuidad. Inadecuados procedimientos de control de acceso físico. Inadecuada seguridad física.	Daños en componentes electrónicos por incendio producido por baterías de las UPS. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Pérdida económica por afectación de equipos de comunicación. Ausencia de energía por afectación de baterías para energía regulada. Indisponibilidad para la gestión del servicio de conectividad TO. Pérdida económica por afectación de equipos de comunicación.	**16**
R27	Espionaje Industrial.	Falta de prácticas seguras de los proveedores o terceros. Deficiencias en los controles de accesos para proveedores o terceros. Contraseñas compartidas. Falta de concientización. Deficiencia en las cláusulas o contratos con terceros. Falta de concientización de mecanismos de ataque a ingeniería social. Falta de conocimiento de la criticidad de la información. Desconocimiento. Retiro o renuncia del empleado. Falta de mecanismos de control de intrusiones en la red. Falta de protecciones y controles físicos. Contraseñas por defecto.	Perdida o fuga de información sensible que puede poner en riesgo la operación del sistema eléctrico y del Centro de Control. Indisponibilidad de gestión de los equipos de comunicaciones. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Pérdida de información. Indisponibilidad del servicio de conectividad de TO. Indisponibilidad de los servicios de TI. Fuga de información sensible.	**16**
R28	Exposición a residuos peligrosos.	Falta de respuesta a emergencias. Falta de mecanismos de segregación de residuos. Manejo inapropiado de materiales peligrosos.	Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Pérdida económica por afectación de equipos de comunicación.	**16**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
R29	Reglas, políticas y procedimientos obsoletos o inexistentes.	Falta de revisiones periódicas. Falta de prácticas seguras de archivado. Falta de política en materia de seguridad de la información.	Baja reputación.	**16**
R30	Fallo de equipos.	Ubicación inadecuada de equipos. Servicios inadecuados de terceros. Servicios de mantenimiento inadecuados. Falta de procesos de control de cambios. Falta de acuerdos de cumplimiento. Falta de planes de continuidad. Punto único de fallo. Fallo en las copias de respaldo. No hay cifrado sobre los respaldos de la plataforma. Ausencia de Unidades de Respaldo de Potencia. Falta o fallo de respaldos. Falta de mecanismos de monitoreo. Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de líneas bases de seguridad. Desconocimiento, negligencia o curiosidad. Falta de supervisión en los trabajos de aseo. Inadecuados procedimientos de control de acceso físico. Falta de procedimientos para clasificar información. Falta de procedimientos o procesos para identificar y gestionar registros y activos críticos.	Indisponibilidad de gestión de los equipos de comunicaciones. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Indisponibilidad de los sistemas de información que soportan la operación del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Daño de equipos. Demoras en la operación de la red eléctrica.	**16**
R31	Presencia de infraestructura no autorizada (Rogue IT, IoT, IIoT).	Acceso no restringido a sistemas o redes corporativas. Logs y registros de auditoria inadecuados. Falta de mecanismos de revisión de antecedentes para personal crítico. Falta de concientización.	Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Indisponibilidad de los sistemas de información que soportan la operación del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Indisponibilidad del servicio de conectividad de TO. Indisponibilidad de los servicios de TI. Demora en la gestión de la operación del servicio de energía.	**16**
R32	Afectación a la Integridad por manipulación física o lógica de los equipos o ciber-activos.	Falta de controles criptográficos o controles de red. Falta de controles para el monitoreo de la red. Líneas de comunicación no protegidas. Desconocimiento, negligencia o curiosidad. Ausencia de procedimientos, documentación o inadecuada transferencia de conocimiento. Políticas inadecuadas de firewall. Fallos de acceso lógico.	Indisponibilidad de gestión de los equipos de comunicaciones. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Pérdida económica por daños en equipos de comunicación. Información inconsistente de los dispositivos	**16**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
			electrónicos para la operación de la red eléctrica. Operación errada de la red eléctrica causando accidentes.	
R33	Accesos físicos no autorizados.	Fallos de Diseños. Fallo en los controles perimetrales. Problemas de autorización. Fallo de monitoreo.	Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Pérdida de información sensible. Pérdida o fuga de información sensible que puede poner en riesgo la operación del Centro de Control. Manipulación del funcionamiento del Sistema SCADA. Indisponibilidad del servicio SACADA. Demora en la recuperación de los servicios de energía. Desplazamiento de personal operativo a las subestaciones. para maniobrar los dispositivos electrónicos.	**16**
R34	Procesamiento ilegal de datos.	Accesos mal definidos sobre plataformas y aplicativos. Falta de mecanismos de identificación y autenticación. Desconocimiento, negligencia o curiosidad. Ausencia de procedimientos, documentación o inadecuada transferencia de conocimiento. Falta de mecanismos de monitoreo. Falta de concientización en reglas y procedimientos. Falta de procedimientos o procesos para identificar y gestionar registros y activos críticos. Ausencia o incorrecta clasificación de información. Falta de procedimientos para clasificar información. Falta disposiciones sobre seguridad y privacidad en los contratos con terceros. Falta de proceso formal para la revisión de privilegios de acceso. Falta de líneas bases de seguridad. Insatisfacción del empleado. Falta de procedimientos formales de control de documentación. Falta de procedimiento de registro de supervisión. Falta de procedimientos para el monitoreo de centros de procesamiento de datos.	Sanciones por manejo indebido de datos personales. Demora en la atención de incidentes y solicitudes Baja reputación. Fuga de información sensible.	**16**
R35	Manipulación indebida de hardware.	Falta de mecanismos de monitoreo. Desconocimiento, negligencia o curiosidad. Falta de supervisión en los trabajos de aseo. Inadecuados procedimientos de control de acceso físico. Falta de concientización en reglas y procedimientos.	Afectación del funcionamiento de los equipos de comunicaciones degradando el servicio y afectando la oportunidad de la gestión de la red	**16**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
		Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de Logs. Falta de procedimientos para clasificar información. Falta de procedimientos o procesos para identificar y gestionar registros y activos críticos. Falta de mecanismos de monitoreo. Falta de controles para la descarga o uso de software. Desconocimiento, negligencia o curiosidad. Falta de concientización en reglas y procedimientos. Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de procedimientos o procesos para identificar y gestionar registros y activos críticos. Falta de copias de respaldo.	eléctrica. Indisponibilidad de los enlaces de comunicaciones. Indisponibilidad de los sistemas de información que soportan la operación del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Daño de equipos. Demoras en la operación de la red eléctrica. Indisponibilidad de gestión de los equipos de comunicaciones. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Pérdida económica por daños en equipos de comunicación.	
R36	Obsolescencia tecnológica, fallos de configuración, ausencia parches.	Mantenimiento insuficiente. Falta de personal. Servicios inadecuados de terceros. Servicios de mantenimiento inadecuados. Falta de SLAs. Falta de acuerdos de cumplimiento. Falta de procesos de control de cambios. Falta de mecanismos de monitoreo. Dependencia del proveedor. Perdida de respaldo técnico del proveedor.	Afectación del funcionamiento de los equipos de comunicaciones degradando el servicio y afectando la oportunidad de la gestión de la red eléctrica. Fuga de información. múltiples vulnerabilidades en equipos de comunicaciones. Indisponibilidad de los sistemas de información que soportan la operación del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Daño de equipos. Demoras en la operación de la red eléctrica. Degradación en el servicio de conectividad.	**16**
R37	Soborno, estafa, corrupción.	Desconocimiento del empleado o falta de ética. Falta de revisiones y auditoria. Jurisdicción internacional. Falta de procesos disciplinarios.	Ejecución de actividades ilícitas por parte de los trabajadores del Centro de Control. Baja reputación. Sabotaje en componentes del servicio de comunicaciones de la red TO.	**12**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
R38	Fallos a la integridad de la información.	Falta de controles criptográficos o controles de red. Falta de controles para el monitoreo de la red. Líneas de comunicación no protegidas. Desconocimiento, negligencia o curiosidad. Ausencia de procedimientos, documentación o inadecuada transferencia de conocimiento. Políticas inadecuadas de firewall.	Información inconsistente de los dispositivos electrónicos para la operación de la red eléctrica. Baja reputación. Indisponibilidad de los servicios de TI. Sabotaje en componentes del servicio de comunicaciones de la red TO.	**12**
R39	Error humano.	Ausencia de procedimientos, documentación o inadecuada transferencia de conocimiento. Uso incorrecto de software o hardware. Falta de control eficiente de cambios de configuración. Falta de detallar responsabilidades de seguridad y privacidad en la descripción de los cargos. Falta de logs de acciones administrativas. Interfaces de usuario complejas. Falta de líneas base de seguridad. Desconocimiento, negligencia o curiosidad.	Indisponibilidad de gestión de los equipos de comunicaciones. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Indisponibilidad de los sistemas de información que soportan la operación del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Daño de equipos. Demoras en la operación de la red eléctrica. Destrucción de las instalaciones del centro de Control. Afectación del funcionamiento de los equipos de comunicaciones degradando el servicio y afectando la oportunidad de la gestión de la red eléctrica.	**12**
R40	Negligencia.	Falta de logs. Falta de mecanismos de identificación y autentificación. Falta de detallar responsabilidades de seguridad y privacidad en la descripción de los cargos. Falta de mecanismos de control de no-repudio. políticas de recursos humanos inadecuadas. Falta de auditoría y control interno. Falta de auditoría. Incapacidad para la recolección de evidencia. Falta de auditoria periódicas. Falta de líneas base de seguridad. Falta de monitoreo de logs de seguridad.	Indisponibilidad de gestión de los equipos de comunicaciones. Indisponibilidad del servicio de conectividad. Indisponibilidad de los servicios de TI. Indisponibilidad de los sistemas de información que soportan la operación del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Daño de equipos. Demoras en la operación de la red eléctrica.	**12**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
			Destrucción de las instalaciones del centro de Control. Afectación del funcionamiento de los equipos de comunicaciones degradando el servicio y afectando la oportunidad de la gestión de la red eléctrica.	
R41	Fallo en conectividad Internet.	Falta de un proveedor alterno. Falta de planes de continuidad. Falta de controles de acceso a internet. Falta o fallo de respaldos. Punto único de fallo. Ubicación inadecuada de equipos. Falta de SLAs. Problemas de cableado.	Baja reputación. Indisponibilidad de los servicios de TI. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control.	**12**
R42	Resistencia al cambio.	Incertidumbre.	Sabotaje en la operación del servicio de energía eléctrica. Demoras en la operación de la red eléctrica. Sabotaje en componentes del servicio de comunicaciones de la red TO. Demora en la atención de incidentes y solicitudes. Baja reputación.	**12**
R43	Corrupción o perdida de datos.	Accesos mal definidos sobre plataformas y aplicativos. Falta de mecanismos de identificación y autenticación. Desconocimiento, negligencia o curiosidad. Fallos en la configuración y actualización de antivirus. Ausencia de procedimientos, documentación o inadecuada transferencia de conocimiento. Falta de mecanismos de monitoreo. Falta de concientización en reglas y procedimientos. Falta de procedimientos o procesos para identificar y gestionar registros y activos críticos. Ausencia o incorrecta clasificación de información. Falta de procedimientos para clasificar información. Falta disposiciones sobre seguridad y privacidad en los contratos con terceros. Falta de proceso formal para la revisión de privilegios de acceso. Insatisfacción del empleado. Falta de procedimientos formales de control de documentación. Falta de procedimiento de registro de supervisión. Falta de procedimientos para el monitoreo de centros de procesamiento de datos. Falta de líneas bases de seguridad.	Perdida o fuga de información sensible que puede poner en riesgo la operación del Centro de Control. Sabotaje en componentes del servicio de comunicaciones de la red TO. Baja reputación. Indisponibilidad de los servicios de TI.	**12**
R44	Inaccesibilidad a la instalación de operación o producción.	Falta de un proveedor alterno. Falta de planes de continuidad.	Demora en la atención de requerimientos. Latencia en la red de datos. Indisponibilidad del servicio de telecomunicaciones. Indisponibilidad de los	**12**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
			sistemas de información que soportan la operación del Centro de Control. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que hacen parte del centro de control. Demoras en la operación de la red eléctrica. Indisponibilidad de acceso a los equipos de cómputo o componentes electrónicos que soportan la operación del sistema eléctrico. Daño de equipos. Demoras en la operación de la red eléctrica. Destrucción de las instalaciones de la subestación.	
R45	Problemas de diseño de software.	Falta de un efectivo control de cambios. Falta de procedimientos para entrada a producción de nuevos aplicativos. Falta de mecanismos de control de cambios. Falta o ausencia de reglas, procedimientos o guías de seguridad y privacidad. Falta de líneas bases de seguridad. Configuraciones inadecuadas. Fechas Incorrectas. Ausencia de mecanismos de pruebas de seguridad. Falta de información. Falta de experiencia o entrenamiento. Falta de implementación de mejores prácticas. Exceso de información. Validación impropia de entradas.	Indisponibilidad de acceso a los sistemas de información que soportan el Centro de Control. Demora en la atención de incidentes y solicitudes. Baja reputación. Indisponibilidad de acceso a los sistemas de información que soportan el Centro de Control.	**8**
R46	Abuso de propiedad intelectual.	Internet sin control. Falta de concientización. Falta de reglas de negocio o políticas. Falta de acuerdos de confidencialidad.	Demora en la atención de incidentes y solicitudes. Baja reputación. Descarga de software no licenciado que genere problemas legales para CENS.	**8**
R47	Uso de software o licencias ilegales, copias fraudulentas de software.	Problemas de distribución de actualizaciones. Falta de procedimientos para establecer mecanismos de protección de propiedad intelectual. Falta de proceso disciplinario en caso de incidentes de seguridad y privacidad. Desconocimiento, negligencia o curiosidad. Ausencia de procedimientos, documentación o inadecuada transferencia de conocimiento. Falta de controles para el monitoreo de la red. Falta de revisiones gerenciales periódicas. Falta de procedimientos para el reporte de debilidades de seguridad y privacidad.	Baja reputación.	**8**

Código del riesgo	Nombre de riesgo	Causas	Efecto	Nivel del Riesgo (P*C)
R48	Robo de propiedad intelectual.	Internet sin control. Falta de controles técnicos (DLP). Deficiencia en el control de licenciamiento. Uso de aplicativos P2P.	Baja reputación.	**8**
R49	Daños a la reputación por clientes insatisfechos.	Falta de personalización. Competencia. Mecanismos inapropiados de escalamiento. Retrasos en la entrega de servicios. Falta de disponibilidad en canales de servicio. Altos tiempos de solución. Repetición de incidentes. Falta en la revisión de los servicios. Problemas de diseño. Deficiencias de calidad en el servicio.	Marchas de las comunidades por incumplimiento en la prestación del servicio. Campañas de desprestigio por la oportunidad del servicio prestado.	**6**

Fuente: Propia

6.2.4 Definición de Iniciativas

Una vez aplicada la metodología de gestión de riesgos definida por el proceso Gestión Integral de Riesgos, se debe indican y catalogan las iniciativas de tratamientos de riesgos bajo el marco de la norma ISO 27001. Por lo tanto, se presenta en la siguiente tabla el resultado del análisis de riesgos de seguridad digital del año 2021.

Tabla 4. Resultado Análisis de Riesgos

Iniciativa	Descripción	Riesgos a mitigar
Aspectos organizativos de la seguridad de la información.	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad digital dentro de la organización incluyendo los procesos de alcance inicial, incluye acciones orientadas a la adopción del proceso de seguridad digital y Continuidad Servicios TI, definición de roles y responsabilidades y los mecanismos de comunicación con los grupos de interés	R15, R24, R27, R29, R47, R49
Seguridad ligada a los recursos humanos.	Esta iniciativa busca asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	R7, R9, R10, R13, R14, R20, R23, R34, R37, R39, R40, R46, R48
Concienciación, capacitación y formación en seguridad de la información.	Esta iniciativa busca establecer un programa de toma de conciencia en seguridad de la información y ciberseguridad con operación anual, en línea con las políticas y procedimientos pertinentes de seguridad digital, teniendo en cuenta la información de la organización que se va a proteger, y los controles que se han implementado para proteger la información y los activos críticos. El plan	R2, R7, R10, R13, R14, R15, R20, R25, R37, R39, R40, R42

Iniciativa	Descripción	Riesgos a mitigar
	de sensibilización incluirá varias actividades para la toma de conciencia, tales como campañas y la elaboración de folletos y boletines de noticias entre otros.	
Control de acceso a las redes y servicios asociados.	Esta iniciativa busca limitar el acceso a información y a instalaciones de procesamiento de información y operación de los ciber activos por medio de la implementación de controles de red y servicios, lógicos o físicos, basados en los requisitos de los negocios y de la seguridad digital. Esta iniciativa es particularmente importante para conexiones de red o aplicaciones de negocios críticas o sensibles para usuarios en sitios de alto riesgo.	R6, R8, R12, R15, R32, R38, R41, R43
Gestión de contraseñas de usuarios.	Esta iniciativa está orientada a la implementación de controles de seguridad para definir las técnicas de autenticación adecuada para corroborar la identidad declarada de los usuarios que se conectan a los servicios y a las redes de la organización. Se definen en esta iniciativa mecanismos de verificación de la identidad y autenticación fuerte, así como métodos de autenticación alternativos a las contraseñas, tales como medios criptográficos, tarjetas inteligentes, toquens o medios biométricos.	R2, R6, R12, R15, R32, R38, R43
Áreas seguras.	Prevenir el acceso físico no autorizado el daño y la interferencia a la información y la operación de los ciber activos, así como a las instalaciones de procesamiento y operación de información y activos críticos para la operación del negocio mediante la definición de controles que buscan proteger áreas que contengan información sensible o crítica, e instalaciones de manejo y operación de información.	R5, R12, R13, R14, R18, R19, R26, R28, R33
Equipo informático de usuarios desatendidos.	Esta iniciativa está orientada a definir los mecanismos de control para definir la protección apropiada a los equipos desatendidos, notificando a los usuarios sobre sus responsabilidades.	R1, R27, R30, R32, R35, R43
Controles contra el código malicioso.	Esta iniciativa busca que se implementen los controles de red o de estación de trabajo para asegurarse que la información, los activos críticos y las instalaciones de procesamiento de información están protegidas contra códigos maliciosos. Se busca también implementar mecanismos de alerta temprana sobre comportamientos anormales en la red de datos relacionados con códigos maliciosos.	R7, R27, R32, R43
Gestión de la seguridad en las redes.	La finalidad de esta iniciativa es asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de soporte mediante la implementación de controles para asegurar la seguridad de la información en las redes, y la protección de servicios relacionados contra accesos no autorizados.	R6, R8, R12, R15, R16, R27, R31, R41, R43
Seguridad en los procesos de desarrollo y soporte.	Esta iniciativa busca asegurar de que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información y aplicaciones corporativas, bien sean desarrolladas internamente o contratadas externamente. Incluyendo	R3, R8, R11, R12, R27, R45

Iniciativa	Descripción	Riesgos a mitigar
	controles relacionados con el ciclo del desarrollo de software.	
Gestión de la prestación del servicio por proveedores.	Asegurar la protección de los archivos y ciber activos de la organización que sean accesibles o gestionados por proveedores mediante la definición e implementación de controles normativos y de cumplimiento por las partes responsables.	R4, R27, R38, R44, R47
Gestión de incidentes de seguridad de la información y mejoras.	Mediante la formalización de esta iniciativa se busca asegurar un enfoque unificado y eficaz para la gestión de incidentes de seguridad de la información, incluida la monitorización y comunicación sobre eventos de seguridad, registros acerca de actividades del usuario, excepciones, fallas de los activos de información y/o ciber activos críticos para la operación del servicio de energía. Se busca adicionalmente contar con un procesamiento centralizado para toda la gestión de seguridad mediante la operación tercerizada de un Security Operation Center SOC por sus siglas en inglés.	R3, R11, R43
Documentación de procesamiento de operación.	Mediante la ejecución de esta iniciativa se busca realizar la documentación operativa necesarias para asegurar las operaciones correctas y seguras de los servicios de TI y de los activos de información y ciber activos que soportan la operación de la organización.	R11, R17, R43, R47
Planificación de la continuidad de la seguridad de la información.	Esta iniciativa busca determinar los requisitos de la seguridad digital en situaciones adversas, por ejemplo, durante una crisis o desastre para establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido. Se incluye dentro de las actividades de esta iniciativa el ciclo de gestión de la continuidad de los servicios de tecnología de la información y la operación.	R3, R17, R19, R22, R26, R36, R44
Protección de los registros de la organización.	Se busca definir los mecanismos de control para proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de la información empresarial; de acuerdo con los requisitos legales, de reglamentación, contractuales y de negocio para asegurar la privacidad y la protección de la información de datos personales y empresariales.	R3, R19, R22, R26

Fuente: Propia

6.2.5 Declaración de aplicabilidad (SOA)

La presente información corresponde a la declaración de controles existentes, no existentes y propuestos para el SGSI en una de las empresas del sector eléctrico en Colombia. Adicionalmente en ella se encuentran justificada la exclusión de algunos de los controles y se muestra el motivo de selección de los controles aplicables, entre los motivos de selección se pueden encontrar: resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo, requisitos legales o reglamentos, obligaciones contractuales y necesidades

empresariales en materia de seguridad de la información según la siguiente nomenclatura:

L: Requerimiento regulatorio.
C: Obligación contractual.
N: Requerimiento del negocio.
R: Análisis de riesgos.

Tabla 5. Declaración de aplicabilidad y el estado de los controles de seguridad de la información

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
A.5	**POLÍTICAS DE SEGURIDAD**							
A.5.1	**Directrices de la Dirección en seguridad de la información**							
A.5.1.1	Conjunto de políticas para la seguridad de la información.	Política de seguridad documentada y divulgada.			X			
A.5.1.2	Revisión de las políticas para la seguridad de la información	No hallada	Aspectos organizativos de la seguridad de la información				X	X
A.6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**							
A.6.1	**Organización interna**							
A.6.1.1	Asignación de responsabilidades para la seguridad de la información	No hallada	Aspectos organizativos de la seguridad de la información					X
A.6.1.2	Segregación de tareas	Adoptando las configuraciones de seguridad se han segregado las tareas en los sistemas de información en uso y se dispone de una matriz de incompatibilidades por sistema al momento de asignar permisos de usuarios.	Aspectos organizativos de la seguridad de la información					X
A.6.1.3	Contacto con las autoridades	Se ha definido el comité de crisis desde donde se interactúa con las autoridades municipales y departamentales.	Aspectos organizativos de la seguridad de la información					X
A.6.1.4	Contacto con grupos de interés	No hallada	Aspectos organizativos de la seguridad de la información					X
A.6.1.5	Seguridad de la información en la gestión de proyectos	No hallada	Aspectos organizativos de la seguridad de la información					X
A.6.2	**Dispositivos para movilidad y teletrabajo**							
A.6.2.1	Política de uso de dispositivos para movilidad	No hallada		Actualmente la gestión de dispositivos				

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
				móviles como celulares está gestionada por la USSA, TI solo gestiona las terminales portátiles para toma de lecturas.				
A.6.2.2	Teletrabajo	No hallada		La política de teletrabajo aún no ha sido aprobada, por tanto no se definen reglas de negocio para este dominio				
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**							
A.7.1	**Antes de la contratación**							
A.7.1.1	Investigación de antecedentes	Se cuenta con mecanismo documentado, formalizado y aplicado de selección de personal. En él se validan los datos de los aspirantes a vinculación. Sin incluir contratistas	Seguridad ligada a los recursos humanos			X	X	X
A.7.1.2	Términos y condiciones de contratación	Como parte de los términos y condiciones laborales, se incluye las cláusulas de confidencialidad. Sin incluir cumplimiento a políticas de seguridad de la información dispone del código de ética	Seguridad ligada a los recursos humanos			X	X	X
A.7.2	**Durante la contratación**							
A.7.2.1	Administración de las responsabilidades	Se ejecutan sólo controles técnicos para aplicar la seguridad de la información				X		
A.7.2.2	Concienciación, capacitación y entrenamiento en seguridad de la información	En las inducciones de nuevo personal se ha definido en la agenda de TI el tema: *Portafolio servicios de tecnología de información. *Política de tecnología de información. *Seguridad de la información. *Buenas prácticas en el uso de Internet y correo electrónico.	Concienciación, capacitación y entrenamiento en seguridad de la información				X	X

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
A.7.2.3	Proceso disciplinario	Cuenta con mecanismo de control disciplinario documentado y aplicado acorde a la ley, sin claridad en los cumplimientos de seguridad de la información	Documentación de mecanismo de control disciplinario				X	
A.7.3	**Cese o cambio de puesto de trabajo**							
A.7.3.1	Cese o cambio de puesto de trabajo	Se tienen definidos procedimientos para el termino o cambio de empleo, sin contemplar claramente los activos de información.					X	
A.8	**GESTIÓN DE ACTIVOS**							
A.8.1	**Responsabilidad sobre los activos**							
A.8.1.1	Inventario de activos	Se han realizado inventario de activos de información para los procesos de TI, Operación Integrada, Facturación, Seguridad física, Cartera y Atención clientes.	Aspectos organizativos de la seguridad de la información.				X	
A.8.1.2	Propiedad de los activos	No hallada	Aspectos organizativos de la seguridad de la información				X	
A.8.1.3	Uso aceptable de los activos	Metodología de inventario de activos de información	Metodología de inventario de activos de información				X	
A.8.1.4	Devolución de activos	Se tiene implementado un procedimiento para el reintegro de equipos	Implementar un procedimiento para el reintegro de equipos				X	
A.8.2	**Clasificación de la información**							
A.8.2.1	Directrices de clasificación	Metodología de inventario de activos de información. Inventario de activos de información procesos de TI, seguridad física y centros de control de energía.	Metodología de inventario de activos de información. Inventario de activos de información.				X	
A.8.2.2	Etiquetado y manejo de la información	Documento metodología de inventario de activos de información	Metodología de inventario de activos de información				X	
A.8.2.3	Manejo de activos	Se cuenta con algunos procedimientos para el retiro de equipos de la institución. No se cuenta con controles eficientes y efectivos para su cumplimiento	Aspectos organizativos de la seguridad de la información				X	
A.8.3	**Manejo de los soportes de almacenamiento**							

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
A.8.3.1	Administración de medios extraíbles	No hallada		El servicio de respaldo se realiza mediante un contratista en el cual se delega la gestión del manejo de soportes de almacenamiento		X	X	X
A.8.3.2	Eliminación de soportes	No hallada		El servicio de respaldo se realiza mediante un contratista en el cual se delega la gestión del manejo de soportes de almacenamiento		X	X	X
A.8.3.3	Soportes físicos en tránsito	No hallada		El servicio de respaldo se realiza mediante un contratista en el cual se delega la gestión del manejo de soportes de almacenamiento		X	X	X
A.9	**CONTROL DE ACCESOS**							
A.9.1	**Requisitos de negocio para el control de accesos**							
A.9.1.1	Política de control de accesos	No hallada	Aspectos organizativos de la seguridad de la información				X	
A.9.1.2	Control de acceso a las redes y servicios asociados	Se implementó la segmentación de redes y el bloqueo de tráfico entre redes mediante firewall. Se cuenta con un procedimiento para otorgar permisos de acceso a los servicios de TI mediante plantilla de Accesos TI.	Aspectos organizativos de la seguridad de la información				X	
A.9.2	**Gestión de acceso de usuario**							
A.9.2.1	Gestión de altas/bajas en el registro de usuarios	Se cuenta con el procedimiento de accesos para los servicios de TI, adicionalmente se realiza actualización de novedades enviadas por GHO mediante sistema de información Mercurio. Se realiza depuración de cuentas de usuario de dominio mensualmente.	Aspectos organizativos de la seguridad de la información				X	

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	Se cuenta con el procedimiento de accesos para los servicios de TI, adicionalmente se realiza actualización de novedades enviadas por GHO mediante sistema de información Mercurio. Se realiza depuración de cuentas de usuario de dominio mensualmente.	Aspectos organizativos de la seguridad de la información				X	
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	Se cuenta con el procedimiento de accesos para los servicios de TI, adicionalmente se realiza actualización de novedades enviadas por GHO mediante sistema de información Mercurio. Se realiza depuración de cuentas de usuario de dominio mensualmente.	Aspectos organizativos de la seguridad de la información				X	
A.9.2.4	Administración de la información confidencial de la autenticación de usuarios	Documento de líneas base de seguridad, El procedimiento no se aplica a la totalidad de los servicios de TI.	Documento de líneas base de seguridad				X	
A.9.2.5	Revisión de los derechos de acceso de los usuarios	Se realizan auditorias que incluyen la revisión de los derechos de acceso a discreción del auditor.	Auditorias que incluyan la revisión de los derechos de acceso a discreción del auditor.				X	
A.9.2.6	Retirada o adaptación de los derechos de acceso	Se tienen definidos procedimientos para el termino o cambio de empleo, sin contemplar claramente los activos de información.	Procedimientos para el termino o cambio de empleo.				X	
A.9.3	**Responsabilidades del usuario**							
A.9.3.1	Uso de información confidencial para la autenticación	Documento de líneas base de seguridad	Aspectos organizativos de la seguridad de la información				X	
A.9.4	**Control de acceso a sistemas y aplicaciones**							
A.9.4.1	Restricción del acceso a la información	Los sistemas de información poseen menús que permiten la ejecución de aplicaciones por usuario. No se controla cual información puede ser consultada por quién.					X	

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
A.9.4.2	Procedimientos seguros de inicio de sesión	Documento de líneas base de seguridad					X	
A.9.4.3	Gestión de contraseñas de usuario	La administración de las contraseñas se realiza mediante GPO que aplica a todos los usuarios del dominio cumpliendo con los requisitos de password	Concienciación, capacitación y entrenamiento en seguridad de la información				X	
A.9.4.4	Restricción en el uso de herramientas de administración de sistemas	Mediante GPO se restringe la instalación de aplicaciones a las cuentas de usuario, pero si la herramienta se puede instalar en una ubicación diferente a c:\windows, si se permite instalar.					X	
A.9.4.5	Control de acceso al código fuente de los programas	Documento de seguridad procesos seguridad y soporte					X	
A.10	**CIFRADO**							
A.10.1	**Controles criptográficos**							
A.10.1.1	Política de uso de los controles criptográficos	Documento de seguridad Controles criptográficos	Gestión de contraseñas de usuario				X	X
A.10.1.2	Gestión de claves	Documento de seguridad Controles criptográficos	Gestión de contraseñas de usuario				X	X
A.11	**SEGURIDAD FÍSICA Y AMBIENTAL**							
A.11.1	**Áreas seguras**							
A.11.1.1	Perímetro de seguridad física.	Se han definido las áreas seguras donde se ubican los equipos de comunicaciones y los servidores.	Áreas seguras				X	X
A.11.1.2	Controles físicos de entrada	El proceso de seguridad física tiene definidos y administra controles físicos de acceso a las instalaciones mediante el sistema integrado de seguridad electrónica.	Áreas seguras				X	X
A.11.1.3	Seguridad de oficinas, despachos y recursos	El proceso de seguridad física tiene definidos y administra controles físicos de acceso a las instalaciones mediante el sistema integrado de seguridad electrónica.	Áreas seguras				X	X
A.11.1.4	Protección contra las amenazas externas y ambientales	Se cuenta con un plan básico de emergencias definidos por el equipo de salud y seguridad en el trabajo donde se incluyen acciones a	Áreas seguras				X	X

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
		tomar si se presentan terremotos, incendios, inundaciones, asonadas, etc.						
A.11.1.5	El trabajo en áreas seguras	Se cuentan con buenas prácticas para trabajar en áreas seguras, sin que se encuentre debidamente formalizados y documentados	Áreas seguras				X	X
A.11.1.6	Áreas de acceso público, carga y descarga	Se cuentan con mecanismos de seguridad en áreas de acceso público como: Vigilancia, cámaras, puertas etc.	Áreas seguras				X	X
***A.11.2**	**Seguridad de los equipos**							
A.11.2.1	Ubicación y protección de equipos	Se cuenta con centro de cómputo y equipos de comunicaciones alojados en gabinetes con llave.	Áreas seguras					X
A.11.2.2	Medidas de protección para fallas en el fluido eléctrico.	Se cuenta con circuitos eléctricos regulados protegidos con UPS. El centro de cómputo principal adicionalmente cuenta con alimentación de planta eléctrica.	Áreas seguras					X
A.11.2.3	Seguridad del cableado	Se cuenta con canastillas, canaletas, centros de cableado protegidos y construidos bajo normas técnicas.	Áreas seguras					X
A.11.2.4	Mantenimiento de los equipos	No se halla	Contratos de soporte para los equipos de comunicaciones y los servidores del centro de cómputo. Proceso de gestión de cambio como regulador de las intervenciones de los dispositivos.					X
A.11.2.5	Salida de activos fuera de las dependencias de la empresa	El departamento técnico solo gestiona la salida de equipos desde la mesa de servicios fuera de las instalaciones mediante formato de orden de salida. No se controla la salida de los equipos de los usuarios finales.	Áreas seguras					X
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	No se halla	Generar una póliza contra robo para los					X

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
			equipos de los trabajadores.					
A.11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento	No se halla	Procedimiento para el reintegro de equipos, donde se debe formatear los equipos que ingresan al almacén o al stock. Procedimiento para medios de almacenamiento.					X
A.11.2.8	Equipo informático de usuario desatendido	Mediante política del dominio se bloquea la pantalla del computador por inactividad de todos los equipos. Las aplicaciones usadas tienen mecanismo de cierre automático de sesión por inactividad. No se encuentra documentado.	Áreas seguras					X
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	No se halla	Documento de líneas base de seguridad					X
A.12	**SEGURIDAD EN LAS OPERACIONES**							
A.12.1	**Responsabilidades y procedimientos de operación**							
A.12.1.1	Documentación de procedimientos de operación	No se halla	Documentación de procedimientos de operación				X	
A.12.1.2	Gestión de cambios	No se halla	Proceso de gestión de cambios implementado y en ejecución.				X	
A.12.1.3	Gestión de capacidades	No hallada		El proceso de gestión de capacidad de los servicios de TI no ha sido implementado.				
A.12.1.4	Separación de entornos de desarrollo, prueba y producción	Cuenta con un 57% de 21 aplicaciones con entorno separado de desarrollo y producción. No se cuenta con entorno de pruebas.					X	
A.12.2	**Protección contra código malicioso**							
A.12.2.1	Controles contra el código malicioso	Cuenta con una solución antivirus para todos los equipos de la organización.					X	X
A.12.3	**Copias de seguridad**							
A.12.3.1	Copias de seguridad de la información	Cuenta con procedimiento de backup para los sistemas de información críticos.					X	

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
A.12.4	**Registro de actividad y supervisión**							
A.12.4.1	Registro y gestión de eventos de actividad	No se halla	Gestión de incidentes de seguridad de la información y mejoras				X	
A.12.4.2	Protección de los registros de información (logs de auditoría)	No se halla	Gestión de incidentes de seguridad de la información y mejoras				X	
A.12.4.3	Registros de actividad del administrador y operador del sistema	No se halla	Gestión de incidentes de seguridad de la información y mejoras				X	
A.12.4.4	Sincronización de relojes	No se halla	Documentar y aplicar política de directorio activo NTP para la sincronización de relojes.				X	
A.12.5	**Control del software en producción**							
A.12.5.1	Instalación del software en sistemas en producción	No se halla	Proceso de gestión de cambios y gestión de la configuración para regular la instalación de aplicaciones y definir las pruebas necesarias para su puesta en producción.				X	
A.12.6	**Gestión de la vulnerabilidad técnica**							
A.12.6.1	Gestión de las vulnerabilidades técnicas	No se halla	Implementar la práctica de actualizaciones automáticas usando WSUS				X	X
A.12.6.2	Restricciones en la instalación de software	Políticas de directorio activo se controla instalación de software.	Disponer de una política que no permite la instalación de aplicaciones que modifiquen el funcionamiento del sistema operativo.				X	
A.12.7	**Consideraciones de las auditorías de los sistemas de información**							
A.12.7.1	Controles de auditoría de los sistemas de información	No se halla	Realizar auditorías periódicamente.				X	
A.13	**SEGURIDAD EN LAS TELECOMUNICACIONES**							
A.13.1	**Gestión de la seguridad en las redes**							
A.13.1.1	Controles de red	Dispone de una solución de comunicaciones con segmentación de redes, adicionalmente posee una solución Firewall incorporada en el Router.	Gestión de la seguridad en las redes				X	

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
A.13.1.2	Mecanismos de seguridad asociados a servicios en red	No se halla	Dispone de un servidor Radius para autenticación en equipos de comunicación.				X	
A.13.1.3	Segregación de redes	Se ha configurado segmentación de redes, se aplicó la práctica de deshabilitar puertos de red sin usar					X	
A.13.2	**Intercambio de información con partes externas**							
A.13.2.1	Políticas y procedimientos de intercambio de información	No se halla	Definir reglas de negocio para el manejo de la información. Metodología de inventario de activos de información. Documento de requerimientos de seguridad sistemas de información.		X		X	
A.13.2.2	Acuerdos de intercambio	No se halla	Definición de reglas de negocio para el manejo de la información		X		X	
A.13.2.3	Mensajería electrónica	No se halla	Definición de reglas de negocio para el manejo de la información. Documento de uso honesto de correo electrónico				X	
A.13.2.4	Acuerdos de confidencialidad y secreto	Cláusulas de confidencialidad definidas de forma básica en los contratos con terceros			X		X	
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**							
A.14.1	**Requisitos de seguridad de los sistemas de información**							
A.14.1.1	Análisis y especificación de los requisitos de seguridad	No se halla	Realizar socialización de las mejores prácticas de seguridad en desarrollo de sistemas de información.				X	
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas	No se halla	Seguridad en los procesos de desarrollo y soporte				X	
A.14.1.3	Protección de las transacciones de los servicios de aplicación	No se halla	Seguridad en los procesos de desarrollo y soporte				X	
A.14.2	**Seguridad en los procesos de desarrollo y soporte**							
A.14.2.1	Política de desarrollo seguro de software	No se halla	Seguridad en los procesos de desarrollo y soporte				X	

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
A.14.2.2	Procedimientos de control de cambios en los sistemas	No se halla	Documento de seguridad Gestión de vulnerabilidades técnicas. Proceso de gestión de cambios				X	
A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	No se halla	Proceso de gestión de cambios define una fase de pruebas las cuales son realizadas ante el desarrollo de cualquier cambio en los servicios de TI.				X	X
A.14.2.4	Restricciones a los cambios en los paquetes de software	No hallada	Seguridad en los procesos de desarrollo y soporte				X	X
A.14.2.5	Uso de principios de ingeniería en protección de sistemas	No hallada	Seguridad en los procesos de desarrollo y soporte				X	X
A.14.2.6	Seguridad en entornos de desarrollo	No se halla.	Contar con ambientes de desarrollo y producción separados.				X	X
A.14.2.7	Externalización del desarrollo de software	Actualmente tiene tercerizado el desarrollo de la página web sin aplicar lineamientos establecidos en un procedimiento formal.					X	X
A.14.2.8	Pruebas de la seguridad del sistema	No hallada	Seguridad en los procesos de desarrollo y soporte				X	
A.14.2.9	Pruebas de aceptación del sistema	No hallada	Seguridad en los procesos de desarrollo y soporte				X	
A.14.3	**Datos de prueba**							
A.14.3.1	Protección de los datos utilizados en pruebas	No hallada	Seguridad en los procesos de desarrollo y soporte					X
A.15	**RELACIONES CON PROVEEDORES**							
A.15.1	**Seguridad de la información en las relaciones con proveedores**							
A.15.1.1	Política de seguridad de la información para proveedores	No hallada			X		X	
A.15.1.2	Tratamiento del riesgo dentro de acuerdos con proveedores	No hallada			X		X	
A.15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones	No hallada			X		X	
A.15.2								
A.15.2.1	Supervisión y revisión de los servicios prestados por terceros	No hallada			X		X	

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
A.15.2.2	Gestión de cambios en los servicios prestados por terceros	No hallada			X		X	
A.16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**							
A.16.1	**Gestión de incidentes de seguridad de la información y mejoras**							
A.16.1.1	Responsabilidades y procedimientos	Se cuenta con un procedimiento para el manejo de cadena de custodia	Gestión de incidentes de seguridad de la información y mejoras				X	X
A.16.1.2	Notificación de los eventos de seguridad de la información	Se han realizado informes de eventos de seguridad bajo un método no formal	Gestión de incidentes de seguridad de la información y mejoras				X	X
A.16.1.3	Notificación de puntos débiles de la seguridad	No se halla	Realizar prueba de vulnerabilidad.				X	X
A.16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones	No se halla	Gestión de incidentes de seguridad de la información y mejoras				X	X
A.16.1.5	Respuesta a los incidentes de seguridad	No hallada	Gestión de incidentes de seguridad de la información y mejoras				X	X
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	No hallada	Gestión de incidentes de seguridad de la información y mejoras				X	X
A.16.1.7	Recopilación de evidencias	No hallada	Gestión de incidentes de seguridad de la información y mejoras				X	X
A.17	**GESTIÓN DE LA CONTINUIDAD DE NEGOCIO**							
A.17.1	**Continuidad de la seguridad de la información**							
A.17.1.1	Planificación de la continuidad de la seguridad de la información	No hallada	Planificación de la continuidad de la seguridad de la información				X	X
A.17.1.2	Implantación de la continuidad de la seguridad de la información	No hallada	Planificación de la continuidad de la seguridad de la información				X	X
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No hallada	Planificación de la continuidad de la seguridad de la información				X	X
A.17.2	**Redundancias**							
A.17.2.1	Disponibilidad de instalaciones para el procesamiento de la información	No hallada	Planificación de la continuidad de la seguridad de la información				X	
A.18	**CUMPLIMIENTO**							
A.18.1	**Cumplimiento de los requisitos legales y contractuales**							
A.18.1.1	Identificación de la legislación aplicable y requerimientos contractuales.	No se halla	Procedimientos con un Normograma donde se define la normatividad aplicable a los procesos de TI.				X	

Sección	Información control de seguridad	Controles existentes	Controles propuestos	Justificación para excluir control	Razón de la selección			
					L	C	N	R
A.18.1.2	Derechos de propiedad intelectual (DPI)	No se halla	Protección de los registros de la organización				X	
A.18.1.3	Protección de los registros de la organización	No se halla	Protección de los registros de la organización				X	
A.18.1.4	Protección de datos y privacidad de la información personal	No se halla	Norma de datos personales				X	
A.18.1.5	Regulación de los controles criptográficos	No se halla	Protección de los registros de la organización				X	
A.18.2	**Revisiones de la seguridad de la información**							
A.18.2.1	Revisión independiente de la seguridad de la información	No se halla	Aspectos organizativos de la seguridad de la información				X	
A.18.2.2	Cumplimiento de las políticas y normas de seguridad	No se halla	Auditorias que incluyan la revisión de los derechos de acceso a discreción del auditor.				X	
A.18.2.3	Comprobación del cumplimiento	No se halla	Auditorias que incluyan la revisión de los derechos de acceso a discreción del auditor.				X	

Fuente: Propia

6.3 MODELO DE MADUREZ DE LA CAPACIDAD CIBERNÉTICA C2M2

El C2M2 se centra en la implementación y gestión de las prácticas de ciberseguridad asociadas con los activos de información, tecnología de la información (TI) y tecnología de operaciones (OT). Está diseñado para usarse como una metodología y herramienta de autoevaluación, para que las empresas del sector eléctrico en Colombia midan y mejoren sus procesos de seguridad digital. Además, se puede utilizar para guiar el desarrollo de nuevos procedimientos que contribuyan a fortalecer la seguridad de sus activos y ciber-activos[44].

6.3.1 Objetivo del modelo C2M2

El propósito del modelo es fortalecer las capacidades de ciberseguridad en las empresas del sector eléctrico en Colombia. Permitiendo evaluar y comparar de

[44] US DEPARTMENT OF ENERGY. Cybersecurity Capability Maturity Model (C2M2) Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

manera efectiva y consistente el proceso de seguridad digital, logrando así, priorizar acciones e inversiones para mejorar sus capacidades de ciberseguridad.

El desafío, es desarrollar capacidades en ciberseguridad para la gestión de amenazas en las empresas del sector eléctrico en Colombia.

Su enfoque, es el de desarrollar un modelo de madurez y una encuesta de autoevaluación para medir las capacidades de ciberseguridad.

El resultado, es el de elaborar un modelo escalable ajustado a las necesidades de las empresas del sector eléctrico en Colombia.

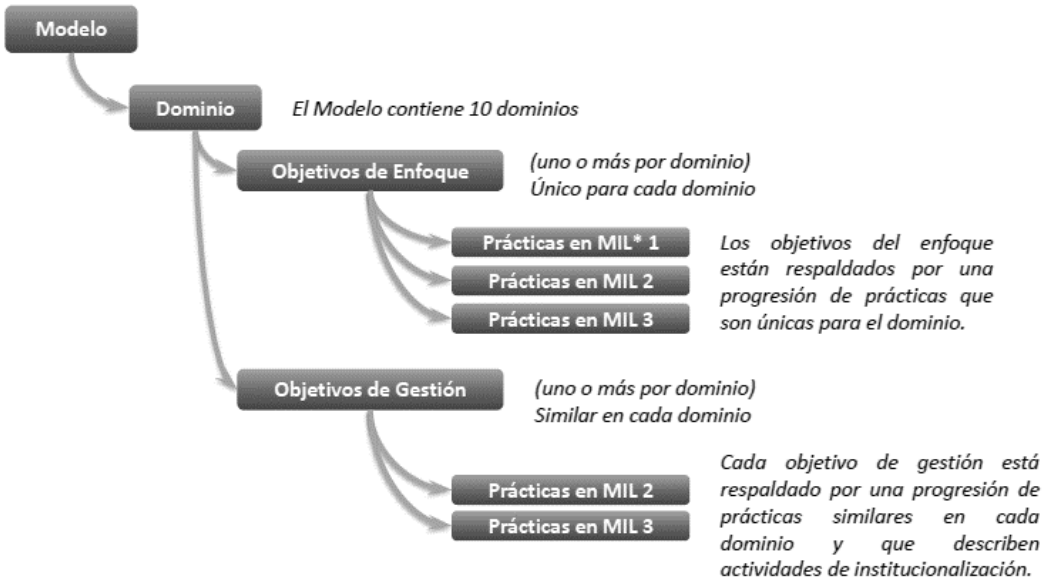
6.3.2 Arquitectura del modelo C2M2

El C2M2 incluye 342 prácticas de ciberseguridad, que se agrupan en 10 dominios. Estas prácticas representan las actividades que una organización puede realizar para establecer y madurar la capacidad en el dominio.

Las prácticas dentro de cada dominio están organizadas en objetivos, que representan logros que respaldan el dominio.

Cada uno de los objetivos de un dominio comprende un conjunto de prácticas, las cuales son ordenadas por niveles de indicadores de madurez o MIL por sus siglas en ingles. La Figura 7 resume los elementos de cada dominio.

Figura 7. **Arquitectura del modelo C2M2**



Fuente: US DEPARTMENT OF ENERGY. Cybersecurity Capability Maturity Model (C2M2) Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

Los dominions, son agrupaciones lógicas de prácticas de ciberseguridad. Cada dominio tiene una sigla a la que se hace referencia en la herramienta de evaluación, como se puede observar en la Figura 8.

Figura 8. Dominios del modelo C2M2

Fuente: US DEPARTMENT OF ENERGY. Cybersecurity Capability Maturity Model (C2M2) Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

Cada dominio está asociado a unos objetivos específicos, como se puede observar en la Figura 9.

Figura 9. Objetivos de los dominios del modelo C2M2

Dominios	Objetivos
RM - Gestión de Riesgos	Establecer una estrategia de gestión del riesgo de ciberseguridad
	Gestión del riesgo de ciberseguridad
	Actividades de gestión
ACM - Gestión de configuración y cambios de Activos	Gestión de inventario de activos
	Gestión de configuración de activos
	Gestión de cambios en activos
	Actividades de gestión
IAM - Gestión de Identidad y Acceso	Establecer y mantener identidades
	Control de acceso
	Actividades de gestión
TVM - Gestión de vulnerabilidades y amenazas	Identificar y responder a las amenazas
	Reducir vulnerabilidades de seguridad
	Actividades de gestión
SA - Conciencia situacional	Realizar el registro
	Realizar monitoreo
	Establecer y mantener una imagen operativa común
	Actividades de gestión
ISC - Intercambio de Información y comunicaciones	Compartir información de ciberseguridad
	Actividades de gestión
IR - Respuesta a Incidentes y Continuidad de la operación	Detectar eventos de ciberseguridad
	Escalar eventos de ciberseguridad y declarar incidentes
	Responder a incidentes y escalar eventos de ciberseguridad
	Plan de continuidad
	Actividades de gestión
EDM - Cadena de Suministro y gestión de dependencias externas	Identificar las dependencias
	Gestión de riesgos de la dependencia
	Actividades de gestión
WM - Gestión de la fuerza de trabajo	Asignar responsabilidades de ciberseguridad
	Controlar el ciclo de vida de la fuerza de trabajo
	Desarrollar la fuerza de trabajo en ciberseguridad
	Incrementar la conciencia en ciberseguridad
	Actividades de gestión
CPM - Gestión del programa de ciberseguridad	Establecer la estrategia del programa de ciberseguridad
	Patrocinador del programa de ciberseguridad
	Establecer y mantener la arquitectura de ciberseguridad
	Realizar desarrollo de software seguro
	Actividades de gestión

Fuente: US DEPARTMENT OF ENERGY. Cybersecurity Capability Maturity Model (C2M2) Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

En la Figura 10 se describen los indicadores de nivel de madurez.

Figura 10. Indicadores de nivel de madurez

Nivel	Nombre	Descripción
MIL0	No realizado	• No se ha iniciado trabajo en el dominio
MIL1	Iniciado	• Se desarrollan prácticas iniciales, pero por defecto
MIL2	Realizado	• Prácticas documentadas • Las partes interesadas están involucradas • Existen recursos adecuados para las prácticas • Se usan estándares y guías para la implementación de las prácticas • Las prácticas son más completas o avanzadas que en el nivel 1 (MIL1)
MIL3	Gestionado	• Las actividades del dominio son guiadas por políticas y gobernanza. • Las actividades son revisadas periódicamente para validar cumplimiento con las políticas. • La responsabilidad y la autoridad para las prácticas están claramente asignadas al personal con habilidades y conocimientos adecuados • Las prácticas son más completas o avanzadas que en el nivel 2 (MIL2)

Fuente: US DEPARTMENT OF ENERGY. Cybersecurity Capability Maturity Model (C2M2) Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

6.3.3 Adoptando el modelo C2M2

El modelo de madurez de la capacidad cibernética (C2M2)[45] está diseñado para que las empresas del sector eléctrico en Colombia puedan evaluar de manera coherente sus capacidades en ciberseguridad, comunicar sus niveles de capacidad de manera significativa e informar sobre la priorización de sus inversiones en este ámbito. La Tabla 6 resume un posible enfoque con cuatro (4) procedimientos para la aplicación del modelo.

Tabla 6. Etapas para utilizar el modelo C2M2

Procedimientos	Entradas	Salidas
Realizar la evaluación	• Autoevaluación de C2M2. • Conocimiento de políticas y procedimientos. • Entendimiento C2M2.	Reporte de autoevaluación de C2M2.
Analizar e identificar brechas	• Reporte de autoevaluación de C2M2. • Objetivos organizacionales. • Impactos en la infraestructura crítica.	Listado de brechas.

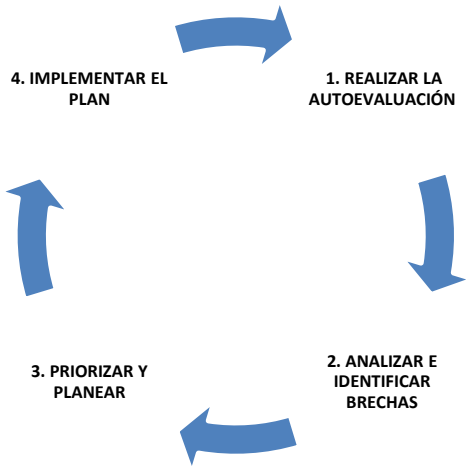
[45] US DEPARTMENT OF ENERGY. Cybersecurity Capability Maturity Model (C2M2) Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

Procedimientos	Entradas	Salidas
	• Trabajos realizados en la organización.	
Priorizar y planear	• Listado de brechas y consecuencias potenciales. • Restricciones organizacionales.	Plan priorizado de implementación.
Implementar el plan	• Plan priorizado de implementación.	Gestión del plan de implementación.

Fuente: US DEPARTMENT OF ENERGY. Cybersecurity Capability Maturity Model (C2M2) Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

En este proceso, la empresa del sector eléctrico lleva a cabo una autoevaluación basada en el modelo, utiliza los resultados de esta autoevaluación para identificar las brechas en sus capacidades de ciberseguridad, prioriza estas brechas y desarrolla planes para abordarlas. Posteriormente, se procede a implementar estos planes de acción. Conforme se implementan los planes, los objetivos pueden cambiar y el entorno de riesgo puede evolucionar, por lo que este proceso se repite de forma iterativa como se observa en la Figura 18.

Figura 11. Ciclo del modelo C2M2



Fuente: US DEPARTMENT OF ENERGY. Cybersecurity Capability Maturity Model (C2M2) Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

6.4 MEDICIÓN DEL PROCESO DE SEGURIDAD DIGITAL EN EMPRESAS DEL SECTOR ELÉCTRICO EN COLOMBIA

Normalmente, una autoevaluación del modelo de madurez de la capacidad de ciberseguridad (C2M2) se lleva a cabo en un taller presencial que dura un día completo o en una serie de sesiones virtuales de 60 a 90 minutos. Los participantes clave en el taller deben ser individuos que tengan un entendimiento sólido de cómo la empresa del sector eléctrico implementa las prácticas de ciberseguridad. Los participantes del taller cuentan con diversas fuentes de información para respaldar su labor, incluyendo la definición del proceso de seguridad digital, el sistema de gestión de seguridad de la información, la declaración de aplicabilidad y la gestión de riesgos. Estos recursos se apoyan en los numerales 6.1 y 6.2 del caso práctico, que se aplica en una empresa del sector eléctrico en Colombia. La definición del proceso de seguridad digital proporciona una comprensión sólida de los procedimientos relacionados con la seguridad digital, mientras que el sistema de gestión de seguridad de la información se centra en la gestión integral de la seguridad de la información. La declaración de aplicabilidad es fundamental para identificar y priorizar las medidas de seguridad necesarias en un contexto específico, y la gestión de riesgos ofrece directrices para identificar, evaluar y mitigar posibles amenazas. En conjunto, estas fuentes de información son esenciales para el desarrollo efectivo del proyecto.

El método para realizar la medición del proceso de seguridad digital aplicando C2M2 sigue las fases de una autoevaluación típica, que son las siguientes[46]:

- Preparación.
- Realización de la autoevaluación.
- Seguimiento.

6.4.1 Preparación

En esta fase se abordó las actividades de planificación y preparación que deben llevarse a cabo en la autoevaluación del C2M2.

a) Obtención de la última versión de los materiales de C2M2

[46] US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

Quienes participen en la planificación de la autoevaluación deben tener la última versión de la documentación enumerada en la Tabla 7. Estos materiales y recursos adicionales se pueden descargar u obtener de la página web del Programa C2M2[47].

Tabla 7. Materiales clave de autoevaluación de C2M2

Titulo	Descripción
Cybersecurity Capability Maturity Model V2.1	El modelo, incluidas las secciones introductorias ("Introducción", "Antecedentes", "Conceptos básicos", etc.)
Self-Evaluation Guide	Guía a los usuarios para planificar y facilitar un taller de autoevaluación con participantes clave en su organización.
Self-Evaluation Tools	Existen diversas herramientas de software gratuitas y comerciales para llevar a cabo y calificar una evaluación de C2M2, incluyendo una herramienta gratuita de C2M2 ofrecida por el Departamento de Energía, que está disponible en dos plataformas: una basada en PDF y otra en HTML. Estas herramientas ofrecen características interactivas y texto de ayuda, permiten a los usuarios registrar los resultados de manera segura y generan automáticamente un informe detallado y gráfico. En ambos formatos de herramienta, todos los datos del usuario permanecen en los dispositivos del usuario.
Self-Evaluation Report	El informe, generado por la Herramienta de Autoevaluación del DOE C2M2 V2.0 (o un informe equivalente generado por otra herramienta), documenta los resultados de la autoevaluación. No es necesario obtener este documento por separado, ya que forma parte de las herramientas de autoevaluación mencionadas anteriormente.
Self-Evaluation Workshop Kickoff Presentation	La presentación se puede utilizar para iniciar un taller de autoevaluación de C2M2. La presentación ofrece una visión general del modelo, ayuda a los participantes a comprender el alcance de la autoevaluación y facilita la comprensión de las respuestas y otros elementos de la autoevaluación.
C2M2 Overview Presentation	La presentación ofrece una visión general de alto nivel de C2M2 que se puede utilizar durante presentaciones a ejecutivos y otros interesados para informarles sobre qué es C2M2 y cómo se puede aprovechar en la organización.
Self-Evaluation Cheat Sheet	La guía resumida de dos páginas contiene información condensada de C2M2 para ser utilizada como referencia por los participantes del taller durante una autoevaluación de C2M2.

Fuente: US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

[47] US DEPARTMENT OF ENERGY. Cybersecurity Capability Maturity Model (C2M2): Additional Resources. {En línea}. {10 de junio de 2022}. Disponible en: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

b) Asignar roles claves en el taller de autoevaluación

La autoevaluación de C2M2 requiere la participación de miembros de la empresa del sector eléctrico que desempeñan una variedad de roles. Los roles y responsabilidades involucrados en un taller típico de autoevaluación de C2M2 se describen en la Tabla 8.

Tabla 8. Roles claves del taller de autoevaluación C2M2

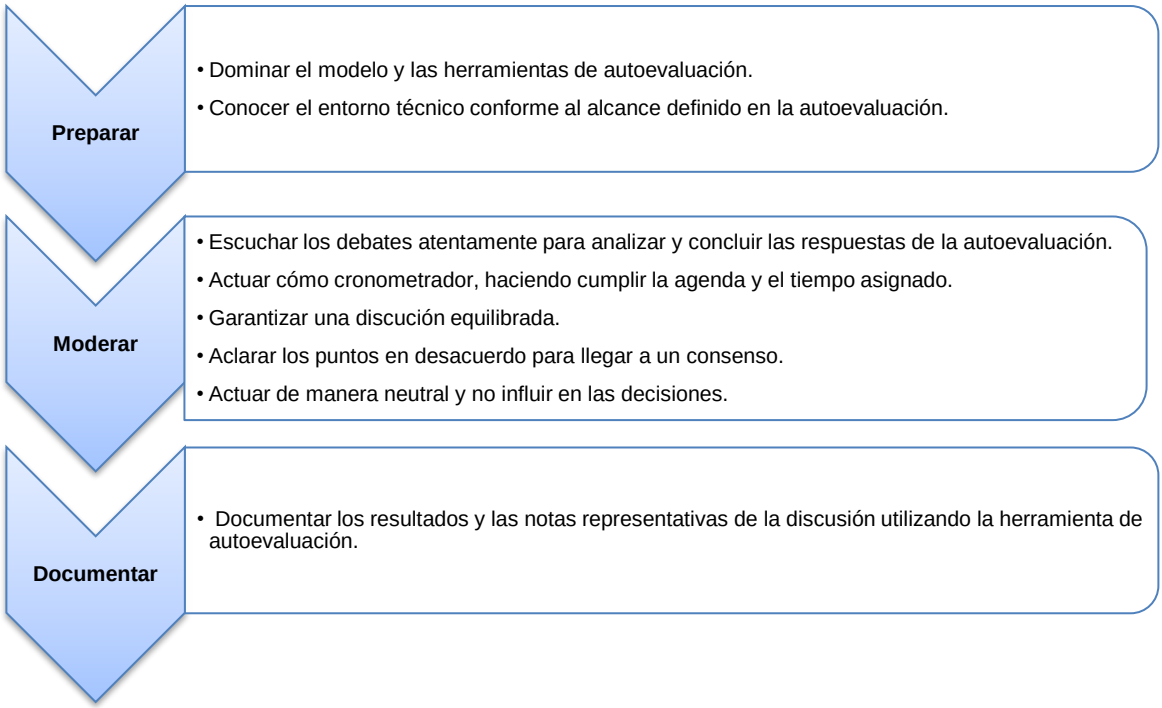
Titulo	Descripción
Organizador	El organizador tiene la responsabilidad general de preparar a la empresa del sector eléctrico para la autoevaluación C2M2 y garantizar su éxito. El rol de organizador, las habilidades requeridas y las responsabilidades son similares a los de un gerente de proyecto.
Facilitador	El facilitador es responsable de planificar y facilitar el taller de autoevaluación del C2M2. El facilitador debe estar familiarizado con todos los materiales enumerados en la Tabla 7 antes del taller de autoevaluación.
Patrocinador	El patrocinador demuestra el compromiso de la alta dirección de la empresa para utilizar la autoevaluación C2M2 y ayuda a garantizar la participación de los miembros del personal necesarios para obtener resultados significativos.
Expertos en la Materia (SMEs)	Los expertos en la materia (SMEs) evalúan las capacidades actuales de ciberseguridad de la organización en relación con las prácticas del dominio C2M2 y la función que se evalúa.
Observadores	Los observadores pueden beneficiarse de la facilitación, pero es posible que no sean necesarios para el desarrollo de respuestas durante la autoevaluación. Se debe notificar al facilitador, patrocinador y participantes sobre cualquier observador potencial.
Escribano	Se debe asignar a una persona para capturar respuestas, notas y propuestas. Un escribano permite al facilitador y a los SMEs centrarse en los debates de autoevaluación sin la necesidad de detenerse a tomar notas.
Personal de apoyo	En colaboración con el patrocinador y el organizador, el facilitador debe identificar a todas las demás personas cuyo apoyo sea necesario durante las tres fases del taller de autoevaluación C2M2.
Participantes	Todas las personas cuya presencia y participación son necesarias durante el taller de autoevaluación (por ejemplo, el patrocinador, el facilitador, los expertos en la materia) se denominan participantes. El patrocinador debe animar a todos los participantes a estar presentes durante toda la duración del taller.

Fuente: US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

c) Selección de un facilitador

La elección de un facilitador eficaz es fundamental. El facilitador es una persona que ayuda a los participantes del taller de autoevaluación a mantener discusiones productivas, llegar a consensos, documentar decisiones y resultados. El facilitador contribuye a planificar una agenda de taller efectiva y asegura que las discusiones se mantengan en tiempo y en el camino correcto[48]. En la Figura 12 se observa las principales funciones del facilitador.

Figura 12. Funciones del facilitador



Fuente: US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

El facilitador debe poseer un profundo conocimiento y experiencia con el C2M2, lo que le permite definir el alcance de la autoevaluación y responder a preguntas tanto durante la autoevaluación como en el seguimiento. Además, el facilitador debe tener competencia técnica suficiente para participar en debates sobre los aspectos técnicos de la implementación de las prácticas C2M2. Para preparar a los participantes, los facilitadores pueden proporcionar copias del C2M2 y organizar reuniones presenciales o virtuales en las que brinden información general sobre el C2M2.

[48] US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

d) Realizar una reunión de preparación para la autoevaluación

Antes de programar la fecha del taller de autoevaluación, el organizador coordinó una reunión con el patrocinador, el facilitador y, posiblemente, otros participantes clave para la preparación de la autoevaluación. Para la presentación de esta reunión se recomienda utilizar la plantilla “C2M2 Overview Presentation” del material referenciado en la Tabla 7. Los objetivos de esta reunión (o reuniones) incluyen los siguientes aspectos[49]:

- Introducir al patrocinador y otros participantes clave al C2M2.
- Obtener un sólido y visible respaldo ejecutivo para el proceso de autoevaluación del C2M2 y el taller relacionado.
- Discutir las expectativas del patrocinador en cuanto a la logística del proceso de autoevaluación, incluyendo las tres fases del proceso, los recursos necesarios, el marco de tiempo involucrado, las funciones y responsabilidades del personal.
- Explorar las expectativas del patrocinador sobre cómo se planea utilizar los resultados de la autoevaluación del C2M2.
- En el caso de que el facilitador sea un externo a la empresa, presentarlo al entorno operativo de la empresa y a los factores comerciales que impactan en sus esfuerzos de ciberseguridad.
- Definir el alcance de la autoevaluación. En caso de que la empresa ya tenga definido un alcance el SGSI, este mismo puede ser adoptado. El término función se utiliza en el modelo para referirse a la parte de la empresa que está dentro del alcance de cada autoevaluación, por lo tanto, es importante aclarar si se evaluaran las prácticas en ciberseguridad en toda la empresa o en dependencias específicas.
- Identificar a los participantes necesarios para el taller de autoevaluación. En el documento “Self-Evaluation Guide”, numeral 1.4.2, Identify Workshop Participants, enumeran el personal relevante que puede participar en la autoevaluación C2M2, pero para efectos prácticos, se recomienda identificar los lideres de procesos y trabajadores que interactúen con las actividades de los 10 dominios C2M2 que serán evaluados.
- Establecer el cronograma y horario del taller de autoevaluación de manera óptima para la participación. En la primera reunión, debe incluir la introducción del modelo C2M2, se recomienda utilizar la plantilla “Self-Evaluation Workshop Kickoff Presentation” del material referenciado en la Tabla 7. Conforme a la

[49] US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

disponibilidad de los participantes claves identificados, se recomienda programar las reuniones por los dominios C2M2 que serán evaluados. La figura 13 es una representación teórica de cómo los dominios C2M2 podrían dividirse en un conjunto de cinco reuniones de talleres virtuales. Para el presente proyecto aplicado, se programaron reuniones semanales, abarcando dos dominios por semana.

Figura 13. Ejemplo de cronograma de un taller virtual de autoevaluación C2M2

Fuente: US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

- Determinar si el taller se llevará a cabo de forma presencial o virtual y, si es presencial, definir la ubicación.
- Decidir si se establecerán objetivos y, en caso afirmativo, cómo y cuándo se hará (según lo descrito en el Apéndice D, Establecimiento de Objetivos, del documento “Self-Evaluation Guide” referenciado en la Tabla 7).
- Si se realizan autoevaluaciones para múltiples funciones en la misma organización, decidir si se consolidarán las puntuaciones y cómo se llevará a cabo dicho proceso (según se detalla en el Apéndice E, Guía de Puntuación para Organizaciones Multifunción, del documento “Self-Evaluation Guide” referenciado en la Tabla 7).

e) Gestionar la logística del taller.

Para llevar a cabo un taller de autoevaluación de manera eficiente, es necesario realizar una extensa preparación logística en los días y semanas previos al evento. Esto abarca la planificación, la definición de la agenda y la capacitación de los participantes, así como la organización de la sala. Además, se deben llevar a cabo tareas posteriores al taller durante la semana siguiente. La gestión de toda la

logística del taller requiere una colaboración efectiva entre el organizador, el facilitador y el personal de apoyo[50].
En el Apéndice A, del documento “Self-Evaluation Guide” referenciado en la Tabla 7 se incluye una lista de verificación de tareas específicas para la logística del taller de autoevaluación, no es necesario seguir esta guía al pie de la letra, para el proyecto aplicado se consideraron las tareas básicas cómo la programación de reuniones virtuales y suministrar previamente el material de apoyo.

6.4.2 Realización de la autoevaluación

En esta segunda fase del taller, se describen las actividades desarrolladas en la empresa del sector electico en Colombia para ejecutar apropiadamente la autoevaluación del modelo C2M2.

a) Iniciar el taller

El taller se inicializó con comentarios de la alta dirección, ya que estos comentarios subrayan la importancia de la autoevaluación C2M2 para la organización, destacan los impulsores comerciales relacionados con la ciberseguridad y enfatizan la necesidad de una participación de los asistentes al taller. Luego, el facilitador socializa la presentación inicial del taller de autoevaluación (Self-Evaluation Workshop Kickoff Presentation), que se ha preparado previamente. Es útil recordar a los participantes que el propósito de la autoevaluación es proporcionar una visión actual de la madurez de las prácticas de ciberseguridad de la empresa del sector eléctrico. La Tabla 9 incluye varios temas que pueden requerir un énfasis especial al comenzar el taller, y la presentación inicial del taller de autoevaluación incluye diapositivas relacionadas con estos temas.

Tabla 9. Temas de discusión al inicio del taller

Tema	Discusión
Alcance acordado	Asegúrese de recordar a los participantes que la autoevaluación se enfoca en una parte específica de la empresa y confirme que comprenden claramente el alcance.
Activos relacionados con la función del alcance	Estos son los activos de TI, TO e información que respaldan la función y aquellos dentro de la función que pueden ser aprovechados para alcanzar un objetivo de amenaza.

[50] US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

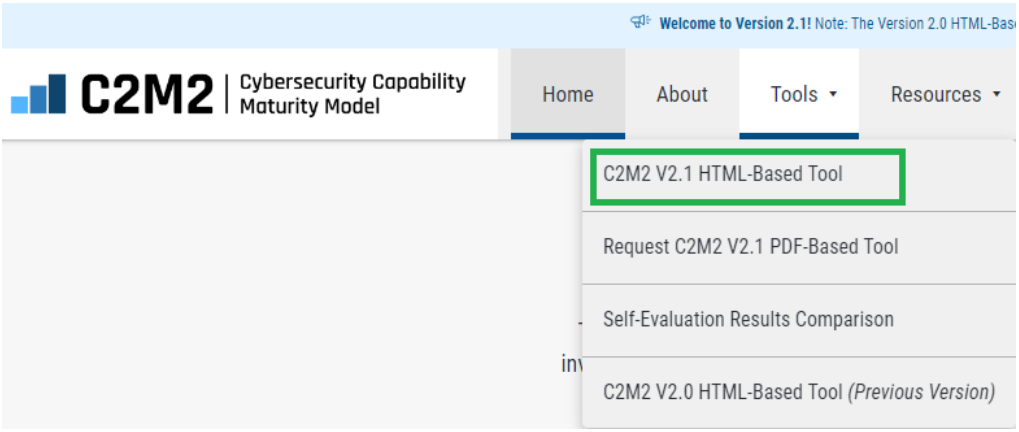
Tema	Discusión
Abordar las actividades previstas para el futuro	Al evaluar posibles respuestas, los participantes deben centrarse en las prácticas implementadas en el día del taller, excluyendo las actividades planificadas o en curso. Este proceso brinda una oportunidad para tomar nota de proyectos planificados o en curso. Posteriormente, se puede considerar actualizar la autoevaluación una vez que estos proyectos se completen. Además, no se deben considerar prácticas que no se hayan llevado a cabo durante un período prolongado de tiempo. Por ejemplo, si se considera que un plan de recuperación ante desastres de la organización está tan desactualizado que resulta inútil, no debe incluirse en la evaluación.
Escala de respuesta de cuatro opciones	Los participantes usan una escala de cuatro opciones para evaluar la implementación de cada práctica en la organización. Se recomienda revisar con los participantes el significado de las cuatro opciones de respuesta; “No implementada”, “Implementada parcialmente”, “Implementada en gran medida” y “Totalmente Implementada”.
Actividades de seguimiento	El facilitador establece expectativas y roles de los participantes en el taller, resaltando la integración de la encuesta en el programa de ciberseguridad de la empresa. Se hace hincapié en que los pasos futuros se basarán en los riesgos y la madurez. La autoevaluación C2M2 debería estimular conversaciones sobre riesgos y permitir a las empresas planificar revisiones periódicas de su programa de ciberseguridad para rastrear el progreso y validar los objetivos. También se indican los roles de los participantes en las actividades de seguimiento.

Fuente: US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

b) Facilitar el taller

La herramienta utilizada para aplicar la autoevaluación en la empresa del sector eléctrico en Colombia es la que se encuentra disponible de manera gratuita en la página web del programa C2M2, accediendo a “Tools” y luego a la opción “C2M2 V2.1 HTML-Based Tool” con se puede observar en la Figura 14 o mediante la URL: https://c2m2.doe.gov/c2m2-assessment.

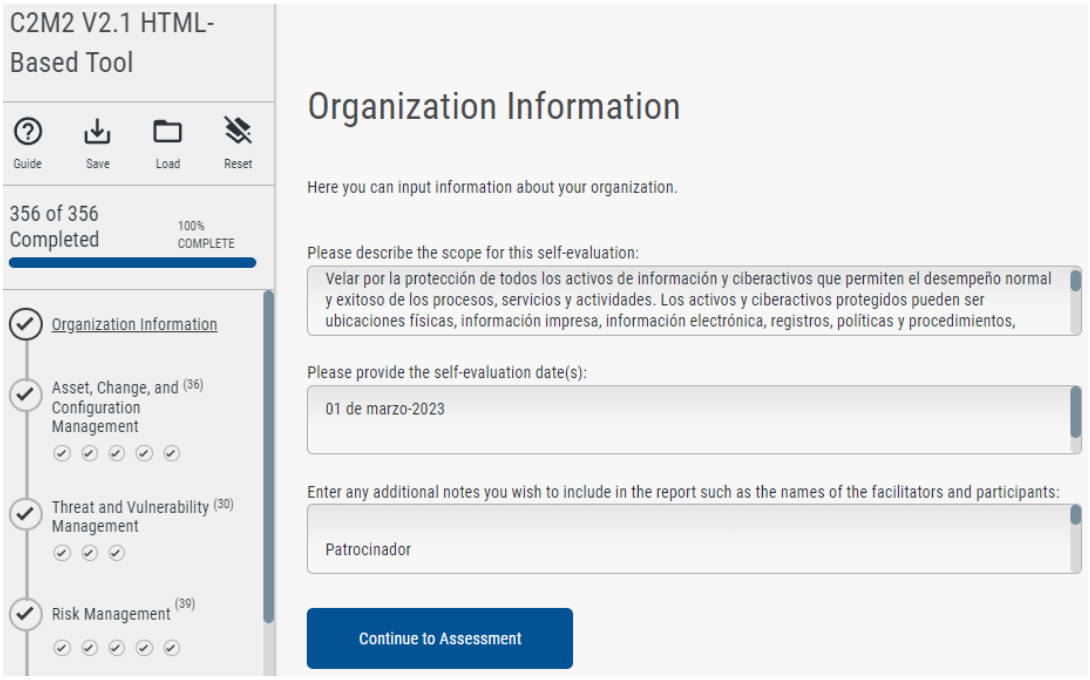
Figura 14. Acceso a la herramienta HTML para realizar la autoevaluación C2M2



Fuente: Propia

Cómo se puede observar en la Figura 15, inicialmente se registra la información de la empresa, cómo el alcance, la fecha de la autoevaluación y notas adicionales, pero sin revelar la identidad de la misma, garantizando la confidencialidad de las respuestas y los resultados. El progreso puede guardase mediante la opción “Save”, generando un archivo JSON que puede descargarse en una estación de trabajo, luego mediante la opción “Load” se carga el archivo JSON y se continua la autoevaluación en el punto guardado.

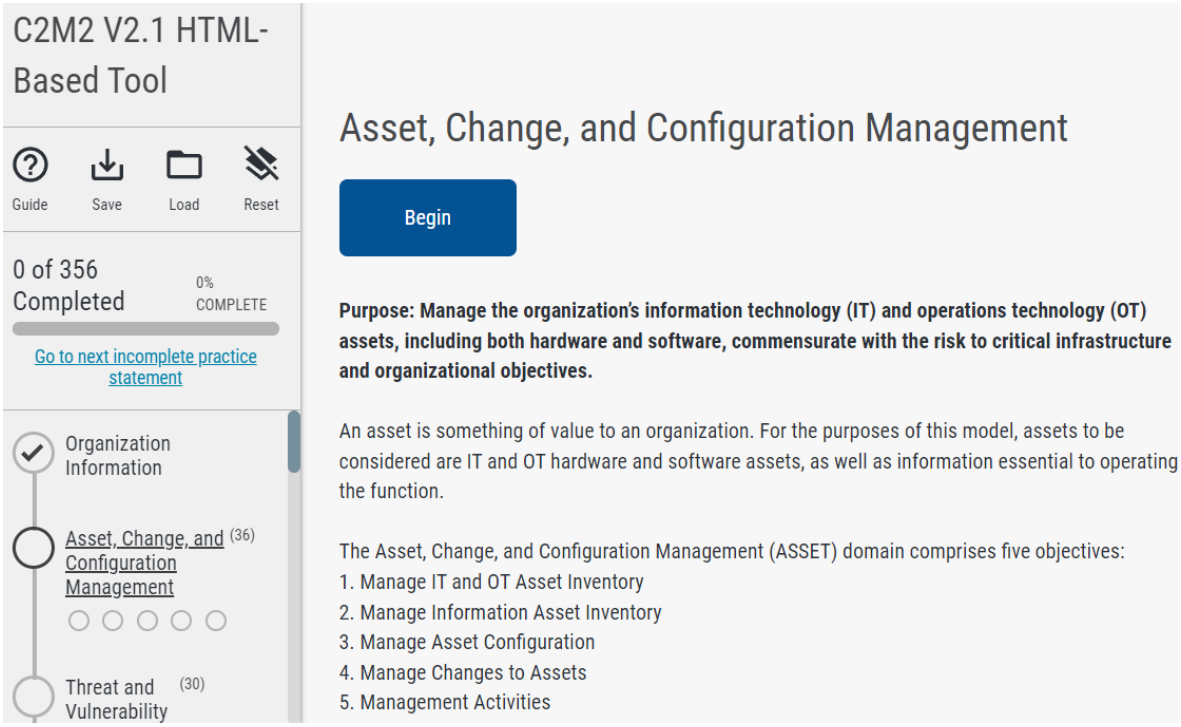
Figura 15. Información de la empresa registrada en C2M2



Fuente: Propia

Para cada dominio, es importante revisar la descripción del dominio, los nombres de los objetivos y las prácticas, y comprender la intención de cada práctica, utilizando el glosario en el modelo o el texto de ayuda según sea necesario, cómo se puede observar en la Figura 16. La herramienta está en idioma inglés, si lo considera necesario puede utilizar extensiones del navegador web para traducirla.

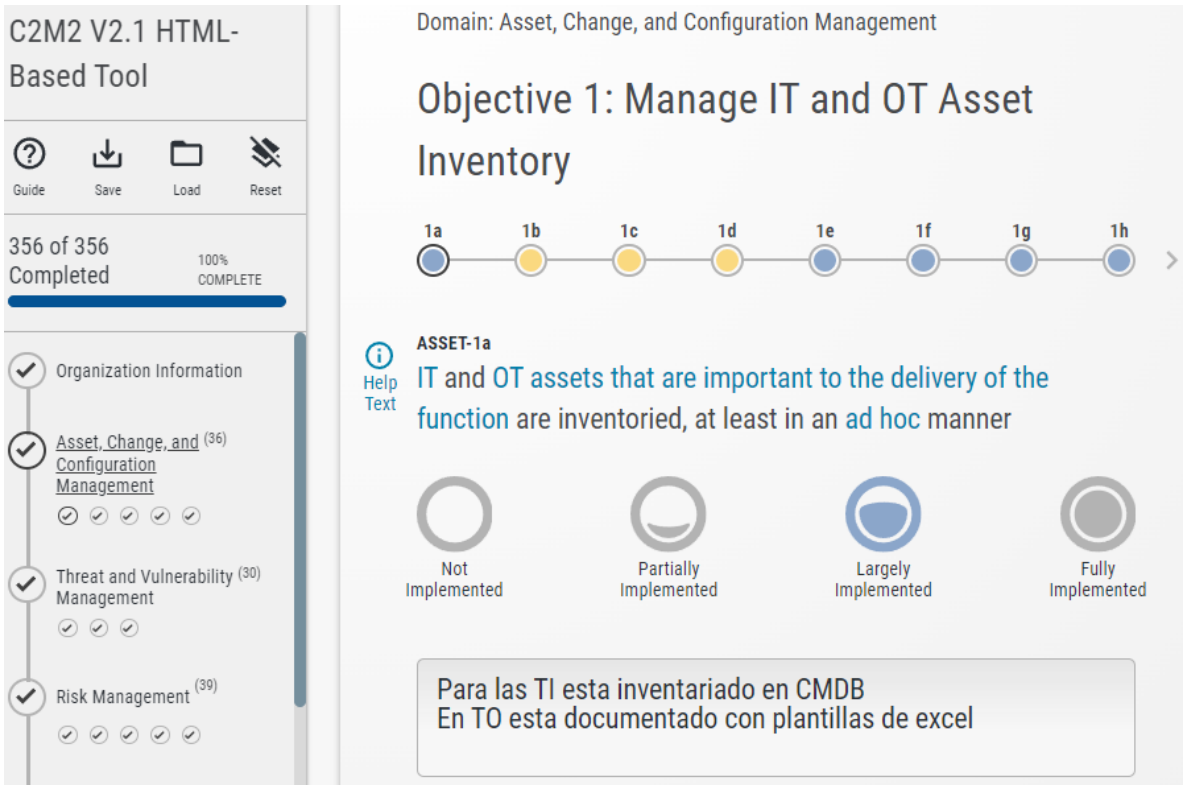
Figura 16. Información del dominio a evaluar en C2M2



Fuente: Propia

Si no se han implementado todas las actividades de una práctica, es esencial reflejar que la implementación es incompleta en la respuesta. Muchos grupos encuentran útil visualizar las prácticas mientras las consideran y ver respuestas previas proyectadas. El facilitador o un escribano registra las respuestas en la herramienta de autoevaluación C2M2, y las prácticas y respuestas son visibles para todos. Cualquier punto importante discutido, como el razonamiento detrás de una respuesta, se anota en el campo "Notas" de la herramienta de evaluación, cómo se ilustra en la Figura 17.

Figura 17. Registro de respuestas en C2M2



Fuente: Propia

En ocasiones, el facilitador debe recordar a los participantes que se centren en la intención de una pregunta en lugar de quedarse atascados en su redacción específica. Cuando no se puede lograr un consenso, agregar el tema a una lista de "estacionamiento" y revisarlo más tarde puede ser útil. El glosario del modelo y el texto de ayuda de C2M2 están disponibles para ayudar a los participantes a alcanzar un entendimiento y deben estar al alcance de los participantes durante el taller, en la herramienta HTML cada practica evaluada tiene un texto de ayuda, cómo se puede ver en la Figura 18.

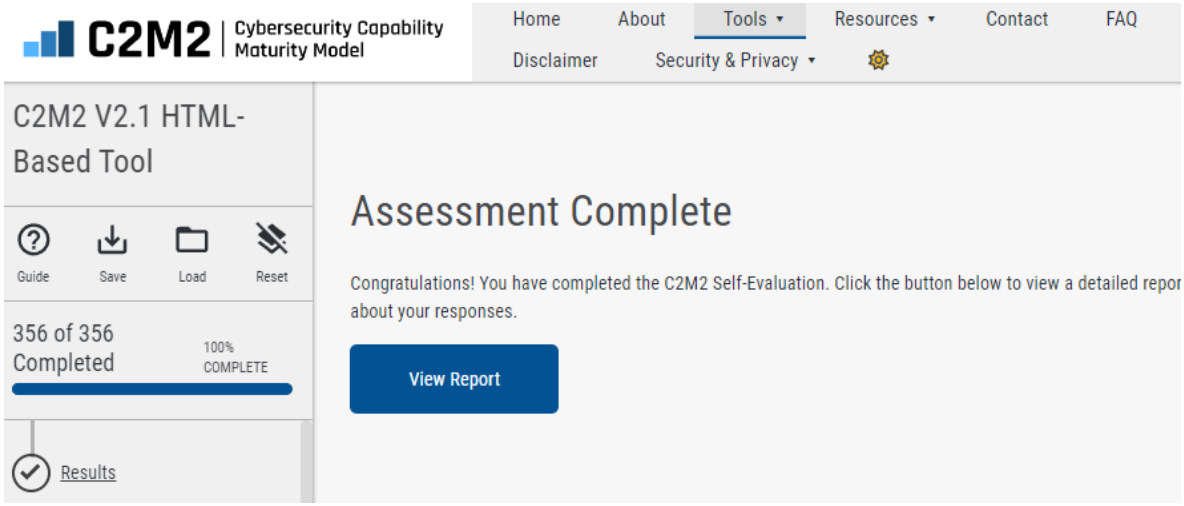
Figura 18. Texto de ayuda en la herramienta HTML para C2M2

Fuente: Propia

c) Generar resultados de autoevaluación

Cómo se puede observar en la Figura 19, una vez se finalizó el registro de las 356 respuestas en la herramienta de autoevaluación C2M2, la opción “Result” ya está habilitada y el informe es generado presionando el botón “View Report”. El informe puede ser consultado en el Anexo 1, Self-Evaluation Report.

Figura 19. Generar resultados de la autoevaluación C2M2



Fuente: Propia

d) Presentar los resultados de la autoevaluación

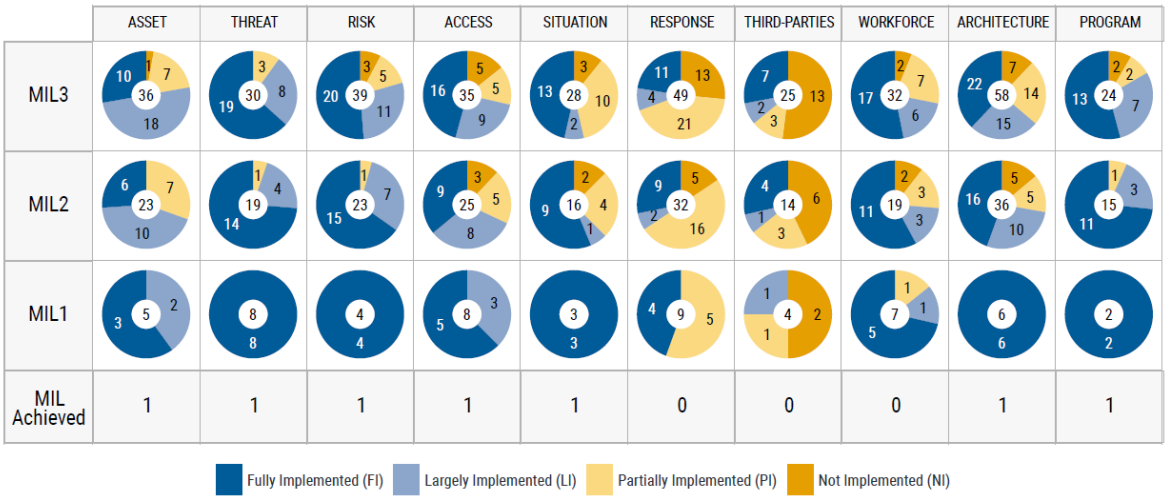
Al concluir la autoevaluación, se aconsejó emplear el Informe de autoevaluación C2M2 para llevar a cabo una revisión. En este punto, el facilitador consideró el tiempo restante y la fatiga de los participantes, ya que, por lo general, se encontraban agotados al final del día. A pesar de la falta de energía para una revisión exhaustiva, los participantes valoraron una discusión y presentación de resultados el mismo día para obtener resultados concretos.

El Informe de autoevaluación presentó los resultados en varios niveles de detalle y empleó diversos elementos visuales. A continuación, se describen los resultados más relevantes y la orientación sobre cómo interpretarlos.

- Interpretación de los gráficos de anillos.

La Figura 20 presenta un resumen gráfico de los resultados generales en forma de una matriz de 3x10 que conecta cada dominio con indicadores de nivele de madurez (MIL) que avanzan de manera progresiva.

Figura 20. Resumen de las Respuestas Ingresadas por MIL y Dominio



Fuente: Propia

Las secciones en azul representan el número de prácticas calificadas como "Totalmente implementadas (FI)" en azul oscuro o "Implementadas en gran medida (LI)" en azul claro. Las secciones en amarillo indican el recuento de prácticas calificadas como "Parcialmente implementadas (PI)" en amarillo claro o "No implementadas (NI)" en amarillo oscuro. Por ejemplo, el gráfico de anillos MIL3 del dominio ACCESO en la Figura 20 muestra que hay 35 prácticas en el dominio ACCESO; 5 prácticas se califican como NI, 5 prácticas son PI, 9 prácticas son LI y 16 prácticas son FI.

El número en el centro de cada gráfico de anillos representa el recuento acumulado de prácticas para cada MIL. Al observar el gráfico de anillos MIL1 en el dominio ACCESO, se evidencia que hay 8 prácticas en el dominio ACCESO en MIL1, junto con 17 prácticas adicionales en MIL2 (= 25 - 8), y 10 prácticas adicionales en MIL3 (= 25 - 35).

Para alcanzar un nivel de madurez (MIL) en un dominio, es necesario que todas las prácticas en ese MIL y en todos los MIL anteriores reciban calificaciones de "Totalmente implementada" o "Implementada en gran medida". No se alcanza un MIL si alguna práctica en ese MIL o en un MIL anterior ha sido calificada como "Parcialmente implementada" o "No implementada". Por ejemplo, para alcanzar MIL3, todas las respuestas en MIL3, MIL2 y MIL1 deben ser "Implementada en gran medida" o "Totalmente implementada".

Conforme a los resultados de la autoevaluación C2M2 en la empresa del sector eléctrico en Colombia, una breve revisión del resumen de dominios en la Figura 20 revela que en MIL1, existen tres dominios, “RESPUESTA”, “TERCERAS PARTES” y "FUERZA LABORAL", en los cuales algunas prácticas han sido calificadas como

"Parcialmente Implementadas" y “No Implementadas”. En consecuencia, no se ha alcanzado el nivel MIL1 en “RESPUESTA”, “TERCERAS PARTES” y "FUERZA LABORAL", y los dominios se encuentran en el nivel MIL0.

El facilitador aclaró que alcanzar el nivel MIL más alto en todos los dominios podría no ser la opción óptima para la empresa. Se señaló que algunas prácticas podrían no haber sido pertinentes para su implementación, dependiendo de las operaciones, el riesgo y las consideraciones comerciales específicas de la empresa. El modelo C2M2 motiva a las empresas a establecer sus propios objetivos para la implementación de las prácticas C2M2, ya sea antes o después de haber realizado una autoevaluación.

El resumen de los dominios puede destacar áreas que podrían beneficiarse de inversiones en ciberseguridad al señalar las diferencias entre los niveles de implementación y los objetivos empresariales[51].

- Interpretación del resumen de implementación de prácticas de gestión.

El objetivo final de cada dominio C2M2 incluye prácticas que se concentran en la gestión de actividades de ciberseguridad. Estas prácticas evalúan el grado en que las actividades de ciberseguridad están integradas o incorporadas en las operaciones de la empresa. Cuanto más profundamente arraigada esté una actividad, mayor será la probabilidad de que la empresa la mantenga a lo largo del tiempo, incluso en momentos de crisis, y que los resultados sean consistentes, repetibles y de alta calidad.

La Figura 21 ofrece una descripción general de alto nivel de la implementación de las prácticas relacionadas a las actividades de gestión desde dos perspectivas: 1) la implementación de todas las actividades de gestión dentro de cada dominio y 2) la implementación de cada práctica de las actividades de gestión en los diez dominios C2M2.

[51] US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

Figura 21. Implementación de actividades de gestión en todos los dominios

	ASSET	THREAT	RISK	ACCESS	SITUATION	RESPONSE	THIRD-PARTIES	WORKFORCE	ARCHITECTURE	PROGRAM
Documented procedures are established, followed, and maintained for activities in the domain	LI	LI	FI	LI	FI	PI	FI	FI	LI	FI
Adequate resources (people, funding, and tools) are provided to support activities in the domain	LI	PI	FI	PI	FI	PI	FI	LI	FI	LI
Up-to-date policies or other organizational directives define requirements for activities in the domain	FI	FI	FI	FI	PI	PI	NI	FI	PI	LI
Responsibility, accountability, and authority for the performance of activities in the domain are assigned to personnel	LI	PI	LI	LI	PI	PI	LI	LI	LI	LI
Personnel performing activities in the domain have the skills and knowledge needed to perform their assigned responsibilities	FI	LI	FI	FI	FI	PI	FI	FI	FI	FI
The effectiveness of activities in the domain is evaluated and tracked	FI	LI	FI	FI	PI	NI	FI	FI	PI	LI

Fuente: Propia

- Interpretación de los resultados detallados de la autoevaluación para cada dominio.

Para cada dominio, el resumen detallado de los resultados de la autoevaluación incluye[52]:

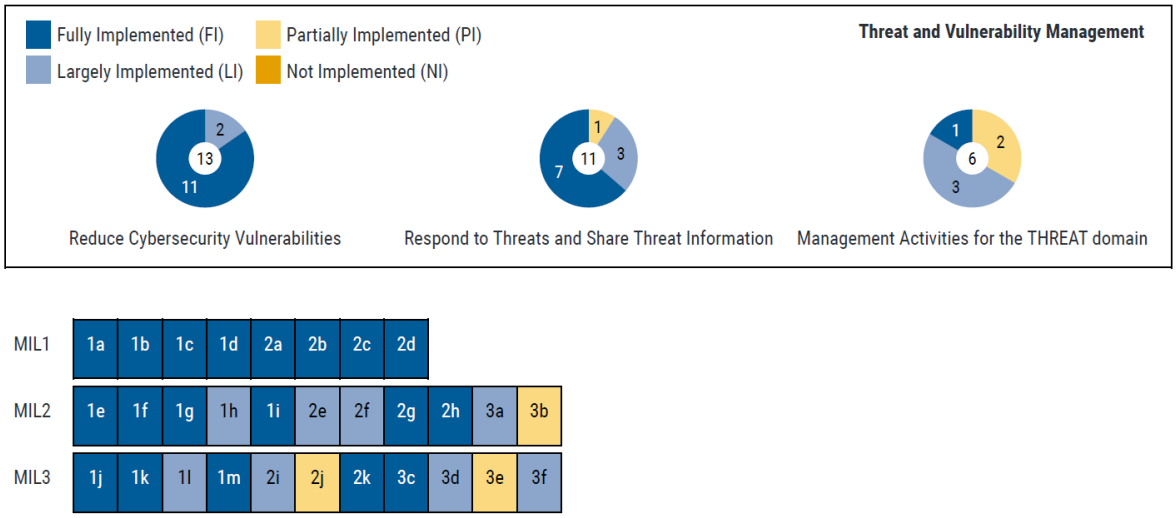
- Gráficos de anillos que representan la implementación de prácticas para cada objetivo dentro del dominio.

[52] US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

- Un cuadro horizontal que detalla la implementación de prácticas para cada MIL dentro del dominio.
- Implementación para cada práctica dentro del dominio.

La Figura 22 proporciona los resultados presentados para el dominio AMENAZA en la empresa del sector eléctrico.

Figura 22. Resultados detallados de autoevaluación para el dominio AMENAZA



Fuente: Propia

- Otros resultados del informe

Las secciones adicionales del informe incluyen un resumen de las notas capturadas para cada práctica y una lista de prácticas parcialmente implementadas y no implementadas. Si bien el facilitador debe estar preparado para revisar brevemente estas secciones del informe durante el taller, son particularmente útiles para apoyar el análisis posterior al trabajo y la planificación de acciones.

e) Cerrar el taller.

El facilitador, en colaboración con el organizador y el patrocinador, debatió las actividades de seguimiento con los participantes antes de concluir el taller. Además, el facilitador u organizador informó a los participantes sobre lo que podían recibir después del taller, como una copia del informe o un resumen de los resultados. Se permitió a todos los participantes compartir comentarios u observaciones finales, y se brindó al patrocinador la oportunidad de hacer comentarios finales.

6.4.3 Seguimiento

En esta tercera fase del taller, se describe el seguimiento de las acciones que mitigaran las brechas identificadas mediante la autoevaluación del modelo C2M2 en la empresa del sector electico en Colombia.

a) Realizar análisis adicionales

Antes de presentar los resultados al patrocinador, el organizador, junto con el facilitador y otros participantes relevantes, deseó llevar a cabo un análisis detallado de los resultados de la autoevaluación. A continuación, se definen aspectos de los resultados que requerirán un análisis más detallado y la atención del patrocinador[53]:

- Identificar fortalezas y posibles objetivos de mejora. En particular, se examinó lo siguiente:
  - MIL con muy pocas prácticas no implementadas.
  - Dominios u objetivos con muy pocas prácticas no implementadas.
  - Objetivos que no se han implementado en absoluto.
  - Prácticas en actividades de gestión que no están implementadas o que están implementadas en muy pocos dominios.
  - Resultados de implementación contradictorios.
  - Observaciones que son contrarias a los objetivos declarados o implícitos de la empresa.

- Realizar comparaciones de resultados que puedan proporcionar información para respaldar los planes de acción:
  - Resultados de diferentes dependencias (Funciones) para identificar puntos en común y excepciones.
  - Resultados a lo largo del tiempo.
  - Resultados para puntajes objetivo.

- Examinar los resultados de los dominios centrados en la empresa (RIESGO, ARQUITECTURA y PROGRAMA) para obtener información a nivel empresarial. Por ejemplo, la gestión del riesgo cibernético puede ser un subconjunto de actividades de riesgo empresarial, y los resultados del dominio RIESGO pueden identificar fortalezas o debilidades en las actividades a nivel empresarial.

b) Revisar los resultados con el patrocinador

[53] US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

El organizador y el facilitador expusieron los hallazgos, análisis y recomendaciones al patrocinador, lideres de la empresa y otros participantes clave. Resultó más efectivo extraer secciones relevantes del informe y presentarlas en lugar de revisar el informe completo.

c) Planificar acciones de seguimiento

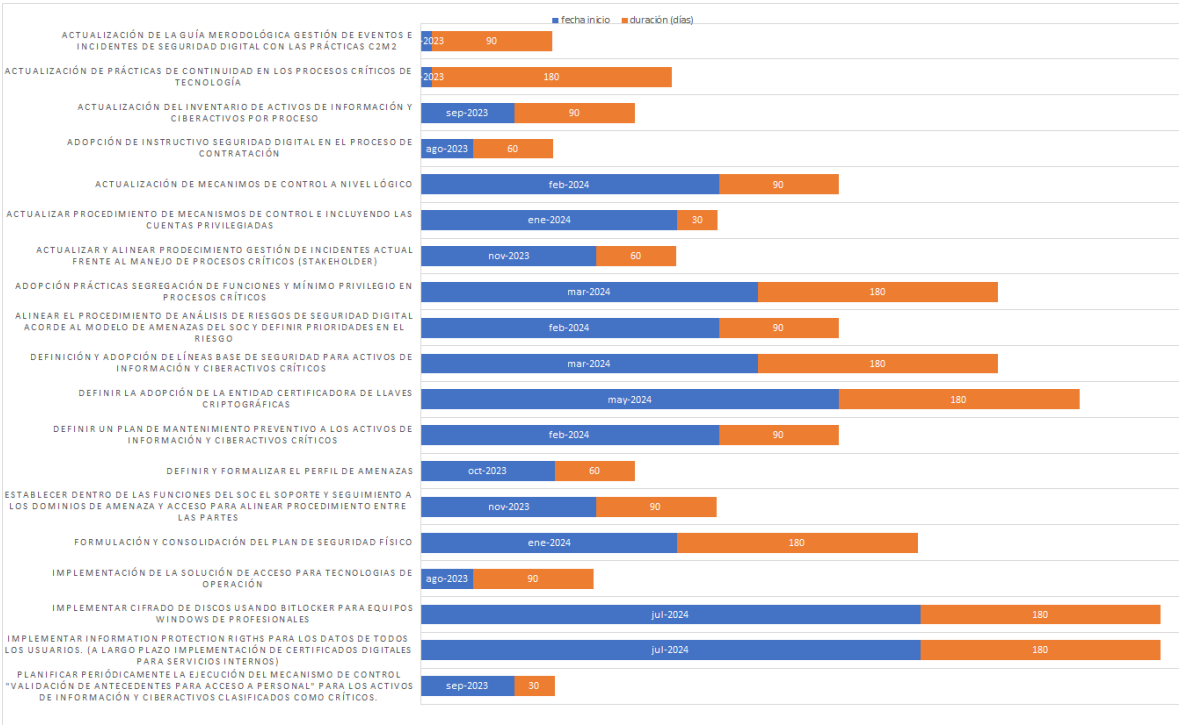
La empresa del sector eléctrico en Colombia puede aprovechar los resultados de su autoevaluación para identificar brechas y planificar acciones e inversiones destinadas a mejorar sus capacidades de ciberseguridad. En el numeral 6.3.3, llamado "Adoptando el modelo C2M2", describe un proceso iterativo que implica establecer un perfil objetivo, identificar brechas entre el perfil actual y el objetivo, implementar mejoras y llevar a cabo evaluaciones posteriores.

La identificación de mejoras comenzó con un análisis de las diferencias entre la situación actual de la empresa y el estado deseado. Resultó útil revisar las notas tomadas durante el taller de autoevaluación para respaldar dicho análisis y la planificación de acciones, ya que estas notas a menudo contenían detalles y sugerencias proporcionadas por los participantes del taller que orientaron las acciones de seguimiento.

Una vez que se completó el análisis de las deficiencias, el organizador pudo priorizar las posibles acciones para abordarlas. La priorización se basó en diversos factores, como los objetivos organizacionales, el presupuesto, el análisis costo-beneficio, los riesgos asociados, la importancia de la empresa como infraestructura crítica, los requisitos de cumplimiento y la disponibilidad de recursos humanos y herramientas necesarios para implementar las prácticas requeridas.

En la Figura 23, se logra observar el plan desarrollado para abordar las deficiencias seleccionadas. Este plan abarcará acciones a corto y largo plazo. La planificación debe seguir los procesos estándar de presupuesto y planificación empresarial. Por lo general, un líder clave dentro de la empresa, como el patrocinador o el organizador, asumirá la responsabilidad de ejecutar el plan, supervisar el progreso, eliminar obstáculos y realizar correcciones necesarias a medida que avanzaba la implementación.

Figura 23. Cronograma del plan de implementación



Fuente: Propia

7 CONCLUSIONES

En una empresa del sector eléctrico en Colombia se logró realizar la medición del proceso de seguridad digital mediante la aplicación del Modelo de Madurez de la Capacidad Cibernética (C2M2), iniciando con la recopilación de la documentación registrada en su Sistema de Gestión Integral (SGI). Está documentación facilitó la ejecución del taller de autoevaluación C2M2 y entre la información más relevante se identificó la guía de cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI), el proceso documentado de Seguridad Digital y la estructura administrativa.

Posteriormente al realizar la revisión de la documentación recopilada, se identificaron los controles de seguridad existentes, definidos en la Declaración de Aplicabilidad (SOA) y soportados por la gestión de riesgos. Teniendo en cuenta esta información y mediante la revisión bibliográfica, se estableció la arquitectura del modelo C2M2 que aplicaría a la empresa del sector eléctrico en Colombia.

Se evaluó la capacidad cibernética en la empresa del sector eléctrico en Colombia, utilizando la herramienta HTML del modelo C2M2, disponible de manera gratuita en la pagina web del Programa C2M2. Durante la preparación del taller de autoevaluación C2M2 se identificaron los roles considerando la estructura admirativa actual y recopilando el material de apoyo mas reciente del modelo C2M2, logrando así registrar exitosamente las opciones de respuesta; “No implementada”, “Implementada parcialmente”, “Implementada en gran medida” y “Totalmente Implementada” en las 356 practicas propuestas en el modelo C2M2.

Una vez finalizado el análisis de las brechas de seguridad, fueron priorizadas las iniciativas o proyectos en un plan de tratamiento. Esta priorización se sustentó en una serie de factores que incluyeron los objetivos estratégicos de la empresa, las restricciones presupuestales, análisis costo-beneficio, los riesgos potenciales asociados, la consideración de la empresa como infraestructura crítica, las obligaciones de cumplimiento normativo y la disponibilidad de los recursos humanos y herramientas necesarias para la ejecución de las prácticas requeridas.

8 RECOMENDACIONES

El modelo C2M2 se revela como una herramienta versátil que puede reforzar las capacidades de ciberseguridad de las empresas del sector eléctrico en Colombia al facilitar la evaluación y comparación efectiva y consistente de las capacidades de ciberseguridad. Además, fomenta la colaboración y el intercambio de mejores prácticas y referencias pertinentes entre empresas del sector eléctrico, lo que contribuye a mejorar sus capacidades de ciberseguridad. Asimismo, el C2M2 ayuda a las organizaciones a priorizar sus acciones e inversiones destinadas a fortalecer sus capacidades de ciberseguridad, proporcionando una hoja de ruta clara para el desarrollo de estrategias de ciberseguridad efectivas.

Considerando lo anteriormente mencionado, se recomienda utilizar la opción “Self-Evaluation Results Comparison” disponible en la pagina web del Programa C2M2, esta herramienta permite comparar los resultados de múltiples autoevaluaciones. Esto puede incluir autoevaluaciones de diferentes funciones o autoevaluaciones realizadas en la misma función en diferentes períodos de tiempo. Todas las autoevaluaciones deben ser de la misma versión de C2M2.

El C2M2 se ha diseñado para orientar tanto el desarrollo de nuevos programas de ciberseguridad como su aplicación en metodologías de autoevaluación para medir y perfeccionar programas de ciberseguridad ya existentes. Por lo tanto, se recomienda su utilización para evaluar el cumplimiento del acuerdo de ciberseguridad del Consejo Nacional de Operación (CNO), conforme a los lineamientos del Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética del Sector Electricidad Colombiano.

El enfoque del C2M2 es descriptivo, en lugar de prescriptivo, y su contenido se presenta a un nivel de abstracción que permite su aplicación en empresas de distintos tipos, estructuras, tamaños y sectores. El uso generalizado del modelo por parte de un sector puede contribuir al benchmarking de las capacidades de ciberseguridad en dicho sector. Estas características hacen del C2M2 una herramienta escalable y adaptable para implementar el Marco de Ciberseguridad del NIST (NIST CSF).

9 BIBLIOGRAFÍA

ÁLVAREZ, M. G.; PÉREZ, G. P. Seguridad informática para empresas y particulares. España: McGraw-Hill, 2004. 20p – 41p.

ANGULO, Susana. Empresas fallan en sus sistemas de seguridad informática. {En línea}. {27 de febrero de 2017}. Disponible en: https://www.enter.co/especiales/empresas-del-futuro/segun-estudio-empresas-fallan-en-sus-sistemas-de-seguridad-informatica/.

CANDELARIO SAMPER, J.; RODRÍGUEZ BOLAÑO, M. Seguridad informática en el siglo XXI: Una perspectiva jurídica tecnológica enfocada hacia las organizaciones Nacionales y Mundiales. En: Revista Especializada en Ingeniería, Universidad Nacional Abierta y a Distancia. {En línea}. {18 de abril de 2014}. Disponible en: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1441/1760.

CCIT. Tendencias Cibercrimen Colombia 2021 – 2022: Nuevas amenazas al comercio electrónico. {En línea}. {2021}. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf.

CHICANO, T. E. Gestión de incidentes de seguridad informática. España: IC Editorial, 2015. 9p – 17p, 151p – 187p.

CHICANO, T. E. Gestión de servicios en el sistema informático. España: IC Editorial, 2015. 22p – 27p.

CONGRESO DE LA REPÚBLICA. Ley 527 de 1999: Diario Oficial 43673. {En línea}. {21 de agosto de 1999}. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276.

CONGRESO DE LA REPÚBLICA. Ley 600 de 2000: Diario Oficial 52130. {En línea}. {18 de agosto de 2022}. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0600_2000_pr006.html.

CONSEJO NACIONAL DE OPERACIÓN (CNO). Acuerdo 1347 de 2020. {En línea}. {16 de septiembre de 2020}. Disponible en: https://www.cno.org.co/content/acuerdo-1347-por-el-cual-se-aprueba-la-actualizacion-de-la-guia-de-ciberseguridad.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Lineamientos de política para ciberseguridad y ciberdefensa: CONPES 3701 de 2011. {En línea}. {14 de julio de 2011}. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3701.pdf.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Política nacional de confianza y seguridad digital: CONPES 3995 de 2020. {En línea}. {1 de julio de 2020}. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Política Nacional de Seguridad Digital: CONPES 3854 de 2016. {En línea}. {11 de abril de 2016}. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

ESCRIVÁ GASCÓ, G. Seguridad informática. España: Macmillan Iberia, 2013. 8p.

FERNÁNDEZ, S. C. M.; PIATTINI, V. M. Modelo para el gobierno de las TIC basado en las normas ISO. España: AENOR, 2012. 83p – 88p.

FISCALÍA GENERAL DE LA NACIÓN. Resolución 0-2369 de 2016: Diario Oficial 49933. {En línea}. {13 de Julio de 2016}. Disponible en: https://normograma.info/crc/docs/pdf/resolucion_fiscalia_2369_2016.pdf.

GÓMEZ VIEITES, Á. Seguridad informática: básico. España: Ecoe Ediciones, 2010. 15p – 55p.

GÓMEZ, F. L.; FERNÁNDEZ, R. P. P. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el esquema nacional de seguridad. España: AENOR, 2018. 57p – 132p.

GONZALEZ, J. Estudio del estado actual de la seguridad informática en las organizaciones de Colombia. Buga, 2020. Proyecto de grado (especialización en seguridad informática). Universidad Nacional Abierta y a Distancia. Escuela de ciencias básicas, tecnología e ingeniería.

GRUPO ATICO34. Control de acceso: Definición, objetivos y tipos. {En línea}. {Consultado el 19 de febrero de 2022}. Disponible en: https://protecciondatos-lopd.com/empresas/control-de-acceso/#Tipos_de_controles_de_acceso.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. NTC-ISO/IEC 27001:2013 Tecnología de la información, Técnicas de seguridad, Sistemas de gestión de la seguridad de la información, Requisitos. Bogotá. INCONTEC, 2013.

LONG, J. Penetration Tester's Open Source Toolkit. United States: Syngress, 2006. 5p – 50p.

LÓPEZ, M. Y. Los virus informáticos: Una amenaza para la sociedad. Cuba: Editorial Universitaria, 2009. 1p – 31p.

LORENZO GONZÁLEZ, D. Herramienta para auditorías de seguridad en entornos industriales y SCADA. Logroño, 2020. Trabajo de investigación (Máster universitario en seguridad informática). Universidad Internacional de la Rioja. ESIT.

MINISTERIO DE TRABAJO. Resolución 0312 de 2019: Diario Oficial 50872. {En línea}. {19 de febrero de 2019}. Disponible en: https://id.presidencia.gov.co/Documents/190219_Resolucion0312EstandaresMinimosSeguridadSalud.pdf.

MINTIC. Seguridad y privacidad de la información: Guía para la gestión y clasificación de incidentes de seguridad de la información. Ministerio de Tecnologías de la Información y las Comunicaciones, 2009. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.

NAKED SECURITY. Seguridad activa y seguridad pasiva en equipos informáticos. {En línea}. {14 de septiembre de 2012}. Disponible en: https://news.sophos.com/es-es/2012/09/14/seguridad-activa-y-seguridad-pasiva-en-equipos-informaticos/.

NIST. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. Estados Unidos: Instituto Nacional de Estándares y Tecnología, 2018. 1p – 44p.

NIST. Security and privacy controls for federal information systems and organizations. United States: NIST Special Publication 800-53, 2013.

OEA; AWS. Marco de Ciberseguridad NIST: Un abordaje integral de la Ciberseguridad. {En línea}. {28 de agosto de 2019}. Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf.

PALELLA, S.; MARTINS, F. Metodología de la Investigación Cuantitativa. Caracas: FEDUPEL, 2006.

PAREDES, F. C. I. Hacking. Argentina: El Cid Editor, 2009. 4p – 29p.

PRESIDENCIA DE LA REPÚBLICA. Decreto 103 de 2015: Diario Oficial 49400. {En línea}. {20 de enero de 2015}. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60556.

PRESIDENCIA DE LA REPÚBLICA. Decreto 1078 de 2015: Diario Oficial 49523. {En línea}. {26 de mayo de 2015}. Disponible en: https://normograma.mintic.gov.co/mintic/docs/decreto_1078_2015.htm.

PRESIDENCIA DE LA REPÚBLICA. Decreto 1413 de 2017: Diario Oficial 50336. {En línea}. {25 de agosto de 2017}. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83253.

PRESIDENCIA DE LA REPÚBLICA. Decreto 1704 de 2012: Diario Oficial 48523. {En línea}. {15 de agosto de 2012}. Disponible en: https://normograma.mintic.gov.co/mintic/docs/decreto_1704_2012.htm.

PRESIDENCIA DE LA REPÚBLICA. Decreto 2364 de 2012: Diario Oficial 48622. {En línea}. {22 de noviembre de 2012}. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=50583.

PRESIDENCIA DE LA REPÚBLICA. Decreto 2573 de 2014: Diario Oficial 49363. {En línea}. {12 de diciembre de 2014}. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=60596.

PRESIDENCIA DE LA REPÚBLICA. Decreto 415 de 2016: Diario Oficial No. 49808. {En línea}. {07 de marzo de 2016}. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=65564.

QUINTERO, J. Introducción a los Sistemas de Control de Acceso. Bogotá, Colombia: Universidad Nacional Abierta y a Distancia, 2020.

SEGU-INFO. Detección de intrusiones en tiempo real. {En línea}. {20 de mayo de 2022}. Disponible en: http://www.segu-info.com.ar/proteccion/deteccion.htm.

STOUFFER, K.; PILLITTERI, V.; LIGHTMAN, S.; ABRAMS, A.; HAHN, A. Guide to Industrial Control Systems (ICS) Security. United States: NIST Special Publication 800-82, 2015.

UNIVERSIDAD INTERNACIONAL DE VALENCIA. Tres tipos de seguridad informática que debes conocer. {En línea}. {10 de octubre de 2016}. Disponible en: https://www.universidadviu.com/es/actualidad/nuestros-expertos/tres-tipos-de-seguridad-informatica-que-debes-conocer.

US DEPARTMENT OF ENERGY. Cybersecurity Capability Maturity Model (C2M2) Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

US DEPARTMENT OF ENERGY. Cybersecurity Capability Maturity Model (C2M2): Additional Resources. {En línea}. {10 de junio de 2022}. Disponible en: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

US DEPARTMENT OF ENERGY. Self-Evaluation Guide: Companion Document to C2M2 Version 2.1. United States: Office of Cybersecurity, Energy Security, and Emergency Response, 2022.

ANEXOS

Anexo 1. Self-Evaluation Report

A continuación, se presenta el informe de autoevaluación llevado a cabo en una empresa perteneciente al sector eléctrico en Colombia.

C2M2 | Cybersecurity Capability Maturity Model

Self-Evaluation Report

C2M2 Version 2.1

SENSITIVE | DO NOT DISCLOSE

U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Table of Contents

Notification

This report is provided “as is” for informational purposes only. The Department of Energy (DOE) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including, but not limited to, direct, indirect, special, or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether or not based upon warranty, contract, tort, or otherwise, whether or not injury was sustained from, or arose out of the results of, or reliance upon the report.

DOE does not endorse any commercial product or service, including the subject of the analysis in this report. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by the agencies.

The display of the DOE official seal or other visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia, or other visual identities of the Department. The DOE seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DOE or the United States Government. Use of the DOE seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DOE policies governing usage of its seal.

1. Introduction

The Cybersecurity Capability Maturity Model (C2M2) can help organizations of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience. This report presents the results of a C2M2 self-evaluation. The results included in this report may be used to measure and improve an existing cybersecurity program. It also may serve as an input for other activities, such as informing cybersecurity risk managers about the controls in place to mitigate cybersecurity risks within an organization.

The results presented in this report are based on participant responses describing the degree to which C2M2 practices are implemented. This report may include sensitive information and should be protected accordingly.

The scope defined for this self-evaluation includes the following:

SCOPE:

Velar por la protección de todos los activos de información y ciberactivos que permiten el desempeño normal y exitoso de los procesos, servicios y actividades. Los activos y ciberactivos protegidos pueden ser ubicaciones físicas, información impresa, información electrónica, registros, políticas y procedimientos, software y licencias, hardware físico de las tecnologías de la información y de la operación.

Se excluye del alcance los siguientes activos de información y/ o ciberactivos: Red de seguridad electrónica y todos los componentes de infraestructura que lo soportan. (dispositivos de la red de video vigilancia para el control de acceso a edificios (cámaras de video vigilancia, dispositivos de almacenamiento de video, etc.).Servicios Cloud, Office 365.

SELF-EVALUATION DATE(S):
Dominio Asset 01 de marzo-2023

ADDITIONAL NOTES:

Introduction

Patrocinador

Jover Alonso Cabrales Pineda

Organizador

Ariadna Valentina Vivas Caceres

Facilitador

Raúl Alejandro Trigos Angarita

Expertos (SMEs)

José Eduardo Patiño Santafé, Rubén Darío Tarazona Pérez

Scribe

Ariadna Valentina Vivas Caceres

This report was generated by the C2M2 HTML-Based Tool Version 2.1 on Tuesday, March 21, 2023 at 15:33:50.

2. Model Architecture

The model is organized into 10 domains. Each domain is a logical grouping of cybersecurity practices. The practices within a domain are grouped by objective—target achievements that support the domain. Within each objective, the practices are ordered by maturity indicator levels (MILs).

The following sections include additional information about the domains and the MILs.

2.1 Domains, Objectives, and Practices

The C2M2 includes 356 cybersecurity practices, which are grouped into 10 domains. These practices represent the activities an organization can perform to establish and mature capability in the domain. For example, the Asset, Change, and Configuration Management domain is a group of practices that an organization can perform to establish and mature asset management, change management, and configuration management capabilities.

The practices within each domain are organized into objectives, which represent achievements that support the domain. For example, the Asset, Change, and Configuration Management domain comprises five objectives:

1. Manage IT and OT Asset Inventory
2. Manage Information Asset Inventory
3. Manage IT and OT Asset Configurations
4. Manage Changes to IT and OT Assets
5. Management Activities for the ASSET domain

Each of the objectives in a domain comprises a set of practices, which are ordered by MIL. Figure 1 summarizes the elements of each domain.

Model Architecture

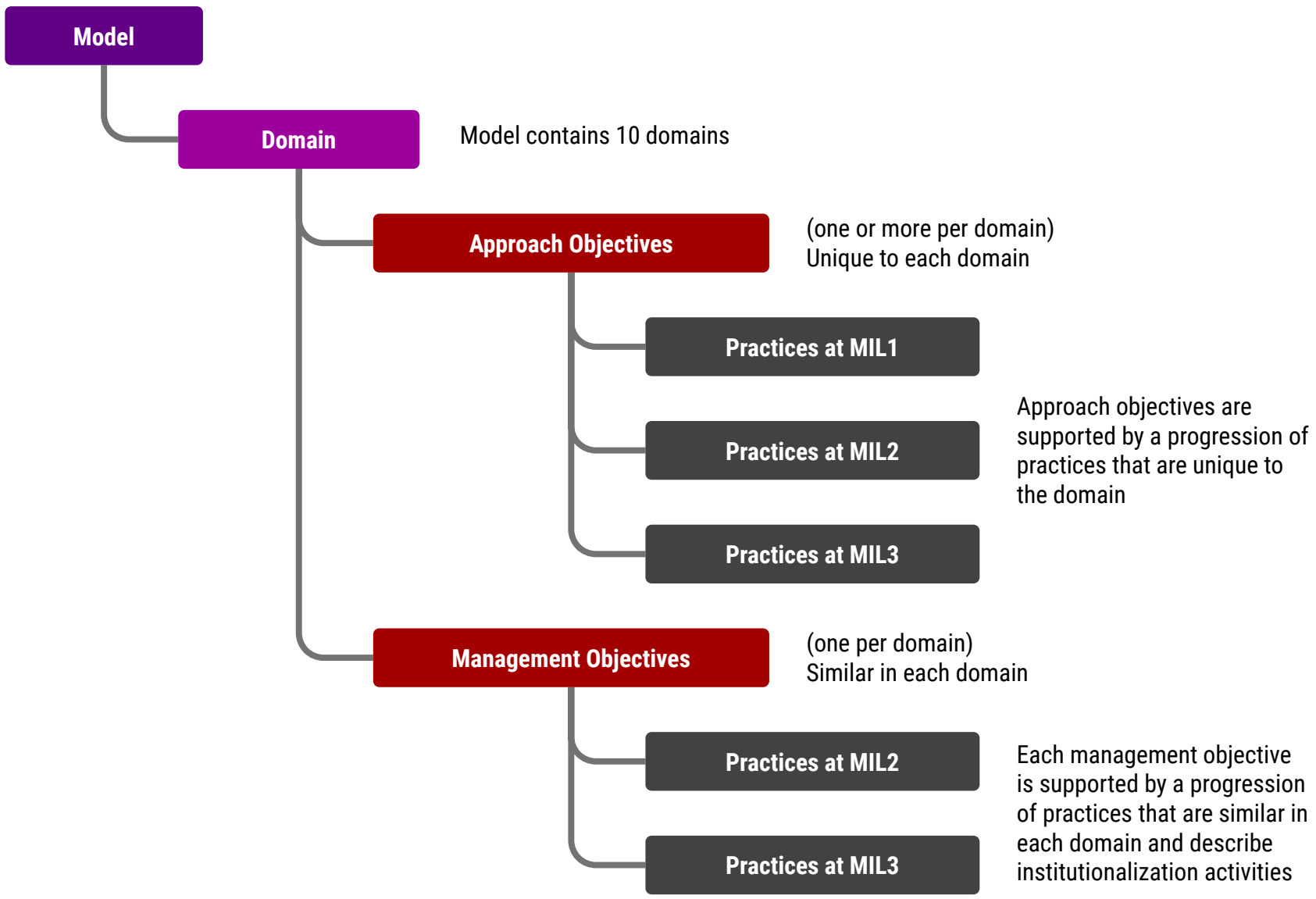


Figure 1: Model and Domain Elements

For each domain, this report provides a purpose statement, which is a high-level summary of the intent of the domain. Further guidance for each of the domains, such as introductory discussions and example scenarios is provided in the C2M2 V2.1 model document.

The purpose statement for each of the 10 domains follows in the order in which the domains appear in the model and in this report. Next to each of the domain names, a short name is provided that is used throughout the model.

Domain: Asset, Change, and Configuration Management (ASSET)

Manage the organization's IT and OT assets, including both hardware and software, and information assets commensurate with the risk to critical infrastructure and organizational objectives.

Domain: Threat and Vulnerability Management (THREAT)

Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (such as critical, IT, and operational) and organizational objectives.

Domain: Risk Management (RISK)

Establish, operate, and maintain an enterprise cyber risk management program to identify, analyze, and respond to cyber risk the organization is subject to, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

Domain: Identity and Access Management (ACCESS)

Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.

Domain: Situational Awareness (SITUATION)

Establish and maintain activities and technologies to collect, monitor, analyze, alarm, report, and use operational, security, and threat information, including status and summary information from the other model domains, to establish situational awareness for both the organization's operational state and cybersecurity state.

Domain: Event and Incident Response, Continuity of Operations (RESPONSE)

Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents and to sustain operations during cybersecurity incidents, commensurate with the risk to critical infrastructure and organizational objectives.

Domain: Third-Party Risk Management (THIRD-PARTIES)

Establish and maintain controls to manage the cyber risks arising from suppliers and other third parties,

commensurate with the risk to critical infrastructure and organizational objectives.

Domain: Workforce Management (WORKFORCE)

Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

Domain: Cybersecurity Architecture (ARCHITECTURE)

Establish and maintain the structure and behavior of the organization's cybersecurity architecture, including controls, processes, technologies, and other elements, commensurate with the risk to critical infrastructure and organizational objectives.

Domain: Cybersecurity Program Management (PROGRAM)

Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with both the organization's strategic objectives and the risk to critical infrastructure.

For a more in-depth description of the C2M2 domains, refer to the C2M2 V2.1 model document available here: https://energy.gov/C2M2 .

2.2 Maturity Indicator Levels

The model defines four maturity indicator levels (MILs), MIL0 through MIL3, which apply independently to each domain in the model. The MILs define a dual progression of maturity: an approach progression and a management progression.

Four aspects of the MILs are important for understanding and applying the model:

- The maturity indicator levels apply independently to each domain. As a result, an organization using the model may be operating at different MIL ratings in different domains. For example, an organization could be operating at MIL1 in one domain, MIL2 in another domain, and MIL3 in a third domain.
- The MILs—MIL0 through MIL3—are cumulative within each domain. To earn a MIL in a given domain, an organization must perform all of the practices in that level and its predecessor level. For example, an organization must perform all of the domain practices in MIL1 and MIL2 to achieve MIL2 in the domain. Similarly, the organization must perform all practices in MIL1, MIL2, and MIL3 to achieve MIL3.
- Establishing a target MIL for each domain is an effective strategy for using the model to guide cybersecurity program improvement. Organizations should become familiar with the practices in the model prior to determining target MILs. Then, they can focus gap analysis activities and improvement efforts on achieving those target levels.
- Practice performance and MIL achievement need to align with business objectives and the organization's cybersecurity program strategy. Striving to achieve the highest MIL in all domains may not be optimal. Companies should evaluate the costs of achieving a specific MIL versus its potential benefits. However, the model was designed so that all companies, regardless of size, should be able to achieve MIL1 across all domains.

For a more in- depth description of the C2M2 MILs and the concept of dual progression, refer to the C2M2 V2.1 model document available here: https://energy.gov/C2M2 .

2.3 Maturity Indicator Level Scoring

MIL achievement scores are derived from responses entered into the C2M2 Self- Evaluation Tool. Responses are chosen from a four- point scale: Fully Implemented (FI), Largely Implemented (LI), Partially Implemented (PI), and Not Implemented (NI). A MIL is achieved when all practices in that MIL and all preceding MILs receive responses of Fully Implemented or Largely Implemented. A MIL is not achieved if any practices in that MIL or a preceding MIL have received a response of Partially Implemented or Not Implemented.

In other words, achieving a MIL in a domain requires the following:

1. Responses of Fully Implemented or Largely Implemented for all practices in that MIL
2. Responses of Fully Implemented or Largely Implemented for all practices in all preceding MILs in that domain

For example, to achieve MIL1 in a domain with four MIL1 practices, all four MIL1 practices have responses of Fully Implemented or Largely Implemented. To achieve MIL2 in that same domain, all MIL1 and MIL2 practices must have responses of Fully Implemented or Largely Implemented.

Descriptions for self-evaluation response options are shown in the following table.

Response	Implementation Description
Fully Implemented (FI)	Complete
Largely Implemented (LI)	Complete, but with a recognized opportunity for improvement
Partially Implemented (PI)	Incomplete; there are multiple opportunities for improvement
Not Implemented (NI)	Absent; the practice is not performed by the organization

Table 1: Description of Self-Evaluation Response Options

3. Summary of Self-Evaluation Results

3.1 MIL Achievement by Domain

Figure 2 shows the MIL achieved for each C2M2 domain.

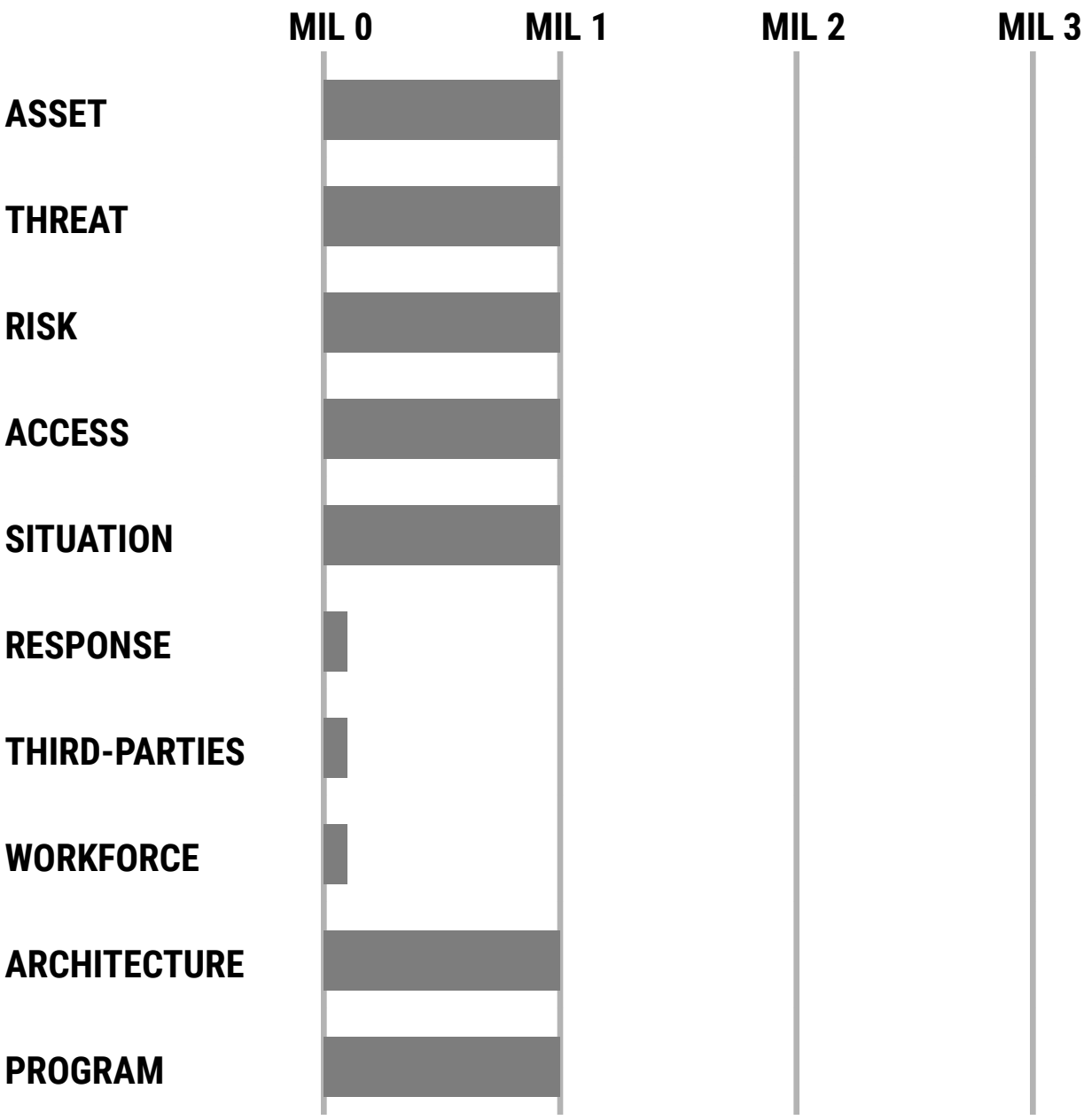


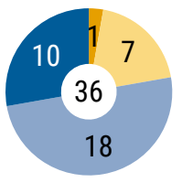
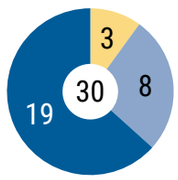
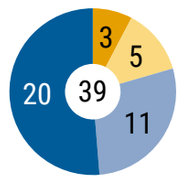
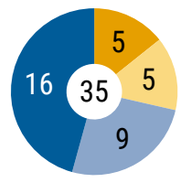
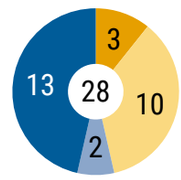
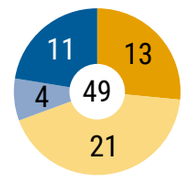
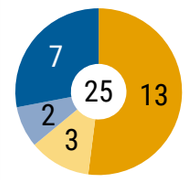
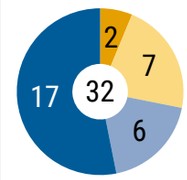
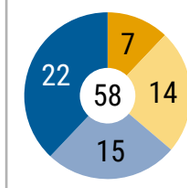
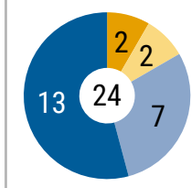
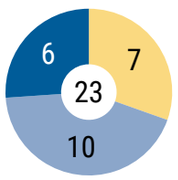
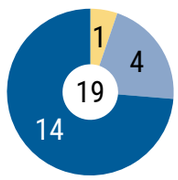
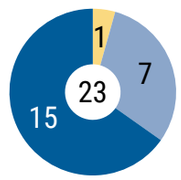
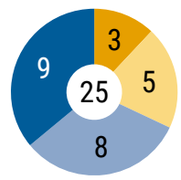
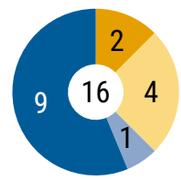
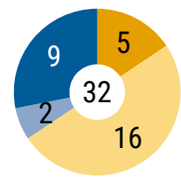
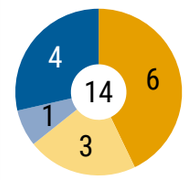
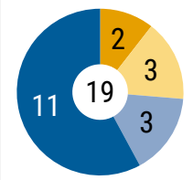
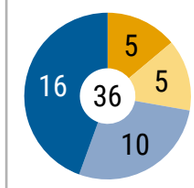
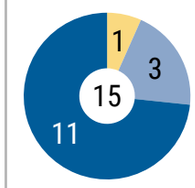
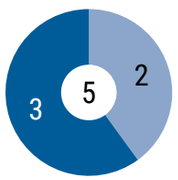
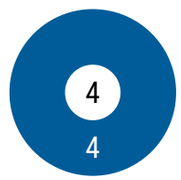
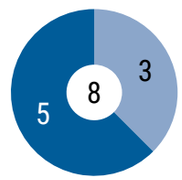
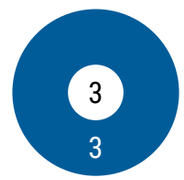
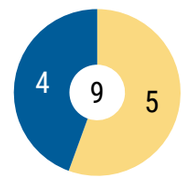
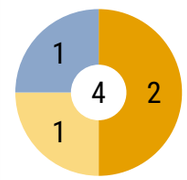
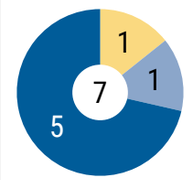
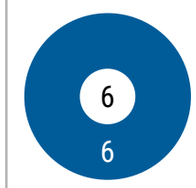
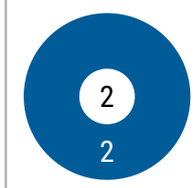
Figure 2: MIL Achieved by Domain

3.2 Practice Implementation by Domain

Figure 3 shows summarized implementation level responses for each C2M2 practice, grouped by domain. The MIL achieved for each domain is listed at the bottom of the figure. A MIL is achieved when all practices in that MIL and all preceding MILs receive responses of Fully Implemented or Largely Implemented. A high-level understanding of the organization's self-evaluation results can be gained from this figure and may be useful when evaluating areas for future improvement.

The number in the center of each donut chart represents the cumulative number of practices in that MIL for that domain. Refer to Section 4.2 of the C2M2 V2.1 model document for a description of how MIL achievement is determined.

Summary of Self-Evaluation Results

	ASSET	THREAT	RISK	ACCESS	SITUATION	RESPONSE	THIRD-PARTIES	WORKFORCE	ARCHITECTURE	PROGRAM
MIL3										
MIL2										
MIL1										
MIL Achieved	1	1	1	1	1	0	0	0	1	1

Fully Implemented (FI) Largely Implemented (LI) Partially Implemented (PI) Not Implemented (NI)

Figure 3: Summary of Responses Input by MIL and Domain

3.3 Implementation of Management Activities across Domains

The final objective of each C2M2 domain includes practices focused on cybersecurity management activities. These practices focus on the extent to which cybersecurity practices are institutionalized, or ingrained, in the organization's operations. The more deeply ingrained an activity, the more likely it is that the organization will continue to perform the activity over time; the activity will be retained under times of stress; and the outcomes of the activity will be consistent, repeatable, and of high quality. Table 2 provides a high-level overview of implementation of the Management Activities practices from two perspectives: 1) implementation of all Management Activities within each domain and 2) implementation of each Management Activities practice across the ten C2M2 domains.

Summary of Self-Evaluation Results

	ASSET	THREAT	RISK	ACCESS	SITUATION	RESPONSE	THIRD-PARTIES	WORKFORCE	ARCHITECTURE	PROGRAM
Documented procedures are established, followed, and maintained for activities in the domain	LI	LI	FI	LI	FI	PI	FI	FI	LI	FI
Adequate resources (people, funding, and tools) are provided to support activities in the domain	LI	PI	FI	PI	FI	PI	FI	LI	FI	LI
Up-to-date policies or other organizational directives define requirements for activities in the domain	FI	FI	FI	FI	PI	PI	NI	FI	PI	LI
Responsibility, accountability, and authority for the performance of activities in the domain are assigned to personnel	LI	PI	LI	LI	PI	PI	LI	LI	LI	LI
Personnel performing activities in the domain have the skills and knowledge needed to perform their assigned responsibilities	FI	LI	FI	FI	FI	PI	FI	FI	FI	FI
The effectiveness of activities in the domain is evaluated and tracked	FI	LI	FI	FI	PI	NI	FI	FI	PI	LI

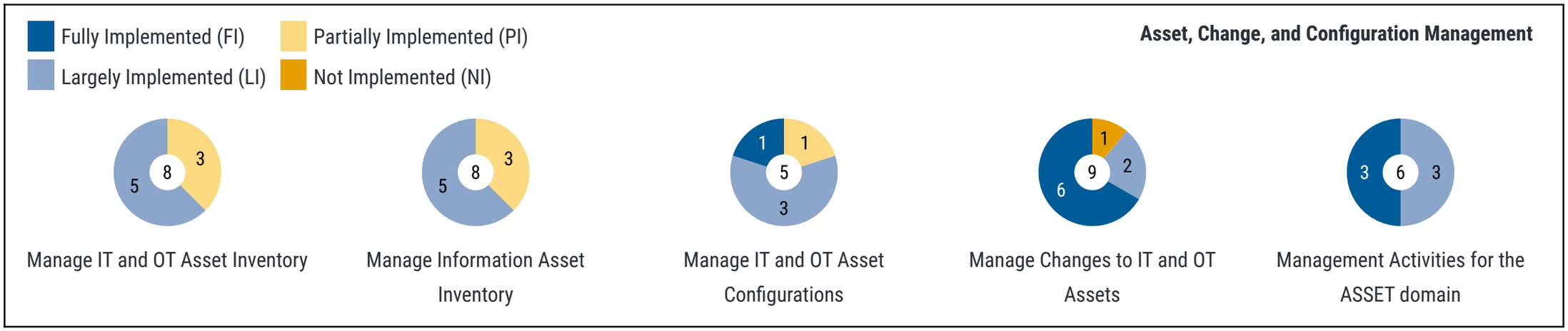
Table 2: Management Activities

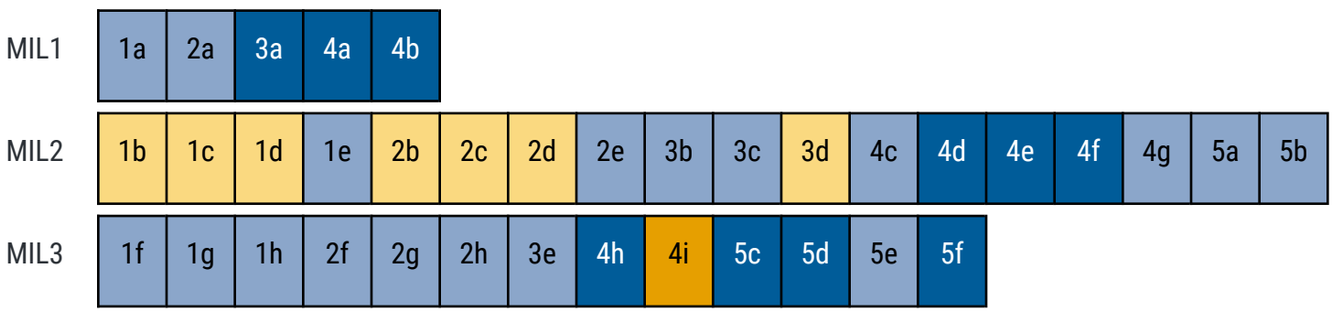
4. Detailed Self-Evaluation Results

This section provides the level of implementation (i.e., Fully Implemented, Largely Implemented, Partially Implemented, and Not Implemented) input to the self-evaluation tool for each C2M2 practice by domain, objective, and MIL. See Section 2.3 Maturity Indicator Level Scoring for a detailed explanation of the scoring process and Section 5 Using the Model for further detail regarding self-evaluation results.

4.1 Domain: Asset, Change, and Configuration Management (ASSET)

Manage the organization's IT and OT assets, including both hardware and software, and information assets commensurate with the risk to critical infrastructure and organizational objectives.





Objective 1: Manage IT and OT Asset Inventory

	ID	Practice Statement	Response
MIL1	ASSET-1a	IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner	LI
MIL2	ASSET-1b	The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective	PI
MIL2	ASSET-1c	Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function	PI
MIL2	ASSET-1d	Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	PI
MIL2	ASSET-1e	The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, asset owner, operating system and firmware versions)	LI
MIL3	ASSET-1f	The IT and OT asset inventory is complete (the inventory includes all assets within the function)	LI
MIL3	ASSET-1g	The IT and OT asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes	LI
MIL3	ASSET-1h	Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life	LI

Objective 2: Manage Information Asset Inventory

	ID	Practice Statement	Response
MIL1	ASSET-2a	Information assets that are important to the delivery of the function (for example, SCADA set points and customer information) are inventoried, at least in an ad hoc manner	LI
MIL2	ASSET-2b	The information asset inventory includes information assets within the function that may be leveraged to achieve a threat objective	PI
MIL2	ASSET-2c	Inventoried information assets are categorized based on defined criteria that includes importance to the delivery of the function	PI
MIL2	ASSET-2d	Categorization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	PI
MIL2	ASSET-2e	The information asset inventory includes attributes that support cybersecurity activities (for example, asset category, backup locations and frequencies, storage locations, asset owner, cybersecurity requirements)	LI
MIL3	ASSET-2f	The information asset inventory is complete (the inventory includes all assets within the function)	LI
MIL3	ASSET-2g	The information asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes	LI
MIL3	ASSET-2h	Information assets are sanitized or destroyed at end of life using techniques appropriate to their cybersecurity requirements	LI

Objective 3: Manage IT and OT Asset Configurations

	ID	Practice Statement	Response
MIL1	ASSET-3a	Configuration baselines are established, at least in an ad hoc manner	FI
MIL2	ASSET-3b	Configuration baselines are used to configure assets at deployment and restoration	LI
MIL2	ASSET-3c	Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARCHITECTURE-1f)	LI
MIL2	ASSET-3d	Configuration baselines are reviewed and updated periodically and according to defined triggers, such as system changes and changes to the cybersecurity architecture	PI
MIL3	ASSET-3e	Asset configurations are monitored for consistency with baselines throughout the assets' lifecycles	LI

Objective 4: Manage Changes to IT and OT Assets

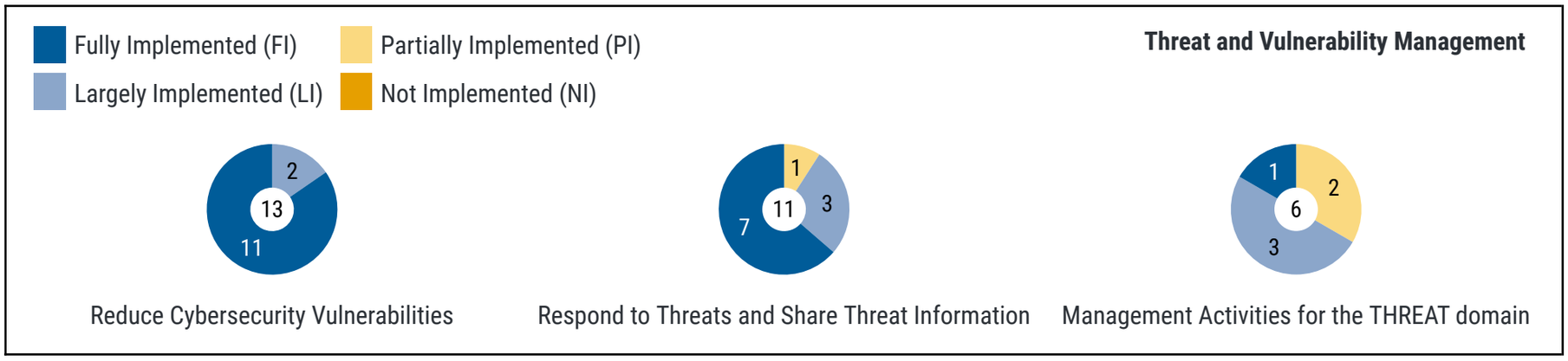
	ID	Practice Statement	Response
MIL1	ASSET-4a	Changes to assets are evaluated and approved before being implemented, at least in an ad hoc manner	FI
MIL1	ASSET-4b	Changes to assets are documented, at least in an ad hoc manner	FI
MIL2	ASSET-4c	Documentation requirements for asset changes are established and maintained	LI
MIL2	ASSET-4d	Changes to higher priority assets are tested prior to being deployed	FI
MIL2	ASSET-4e	Changes and updates are implemented in a secure manner	FI
MIL2	ASSET-4f	The capability to reverse changes is established and maintained for assets that are important to the delivery of the function	FI
MIL2	ASSET-4g	Change management practices address the full lifecycle of assets (for example, acquisition, deployment, operation, and retirement)	LI
MIL3	ASSET-4h	Changes to higher priority assets are tested for cybersecurity impact prior to being deployed	FI
MIL3	ASSET-4i	Change logs include information about modifications that impact the cybersecurity requirements of assets	NI

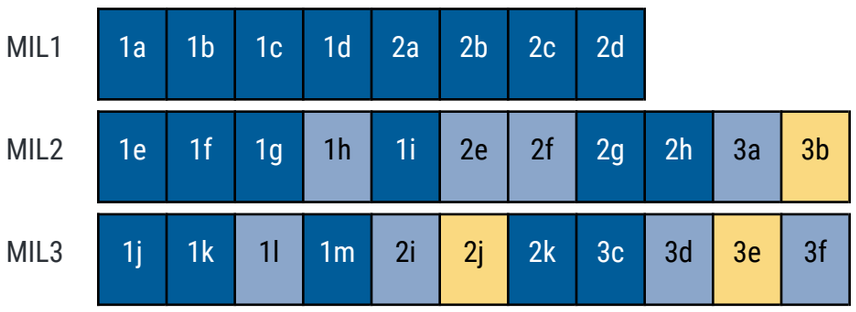
Objective 5: Management Activities for the ASSET domain

	ID	Practice Statement	Response
MIL2	ASSET-5a	Documented procedures are established, followed, and maintained for activities in the ASSET domain	LI
MIL2	ASSET-5b	Adequate resources (people, funding, and tools) are provided to support activities in the ASSET domain	LI
MIL3	ASSET-5c	Up-to-date policies or other organizational directives define requirements for activities in the ASSET domain	FI
MIL3	ASSET-5d	Responsibility, accountability, and authority for the performance of activities in the ASSET domain are assigned to personnel	FI
MIL3	ASSET-5e	Personnel performing activities in the ASSET domain have the skills and knowledge needed to perform their assigned responsibilities	LI
MIL3	ASSET-5f	The effectiveness of activities in the ASSET domain is evaluated and tracked	FI

4.2 Domain: Threat and Vulnerability Management (THREAT)

Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (such as critical, IT, and operational) and organizational objectives.





Objective 1: Reduce Cybersecurity Vulnerabilities

	ID	Practice Statement	Response
MIL1	THREAT-1a	Information sources to support cybersecurity vulnerability discovery are identified, at least in an ad hoc manner	FI
MIL1	THREAT-1b	Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner	FI
MIL1	THREAT-1c	Cybersecurity vulnerability assessments are performed, at least in an ad hoc manner	FI
MIL1	THREAT-1d	Cybersecurity vulnerabilities that are relevant to the delivery of the function are mitigated, at least in an ad hoc manner	FI
MIL2	THREAT-1e	Cybersecurity vulnerability information sources that collectively address higher priority assets are monitored	FI
MIL2	THREAT-1f	Cybersecurity vulnerability assessments are performed periodically and according to defined triggers, such as system changes and external events	FI
MIL2	THREAT-1g	Identified cybersecurity vulnerabilities are analyzed and prioritized, and are addressed accordingly	FI
MIL2	THREAT-1h	Operational impact to the function is evaluated prior to deploying patches or other mitigations	LI
MIL2	THREAT-1i	Information on discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders	FI

	ID	Practice Statement	Response
MIL3	THREAT-1j	Cybersecurity vulnerability information sources that collectively address all IT and OT assets within the function are monitored	FI
MIL3	THREAT-1k	Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of the function	FI
MIL3	THREAT-1l	Vulnerability monitoring activities include review to confirm that actions taken in response to cybersecurity vulnerabilities were effective	LI
MIL3	THREAT-1m	Mechanisms are established and maintained to receive and respond to reports from the public or external parties of potential vulnerabilities related to the organization's IT and OT assets, such as public-facing websites or mobile applications	FI

Objective 2: Respond to Threats and Share Threat Information

	ID	Practice Statement	Response
MIL1	THREAT-2a	Internal and external information sources to support threat management activities are identified, at least in an ad hoc manner	FI
MIL1	THREAT-2b	Information about cybersecurity threats is gathered and interpreted for the function, at least in an ad hoc manner	FI
MIL1	THREAT-2c	Threat objectives for the function are identified, at least in an ad hoc manner	FI
MIL1	THREAT-2d	Threats that are relevant to the delivery of the function are addressed, at least in an ad hoc manner	FI
MIL2	THREAT-2e	A threat profile for the function is established that includes threat objectives and additional threat characteristics (for example, threat actor types, motives, capabilities, and targets)	LI
MIL2	THREAT-2f	Threat information sources that collectively address all components of the threat profile are prioritized and monitored	LI
MIL2	THREAT-2g	Identified threats are analyzed and prioritized and are addressed accordingly	FI
MIL2	THREAT-2h	Threat information is exchanged with stakeholders (for example, executives, operations staff, government, connected organizations, vendors, sector organizations, regulators, Information Sharing and Analysis Centers [ISACs])	FI

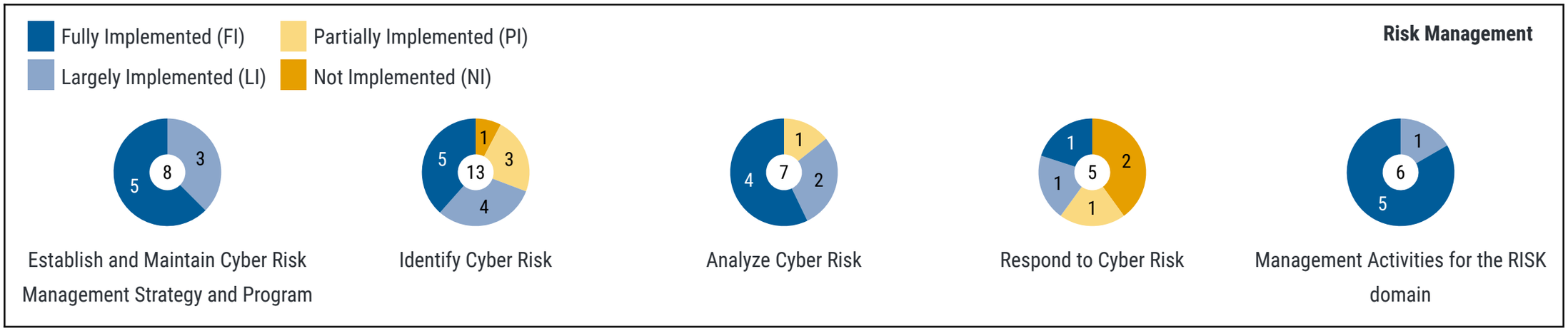
	ID	Practice Statement	Response
MIL3	THREAT-2i	The threat profile for the function is updated periodically and according to defined triggers, such as system changes and external events	LI
MIL3	THREAT-2j	Threat monitoring and response activities leverage and trigger predefined states of operation (SITUATION-3g)	PI
MIL3	THREAT-2k	Secure, near-real-time methods are used for receiving and sharing threat information to enable rapid analysis and action	FI

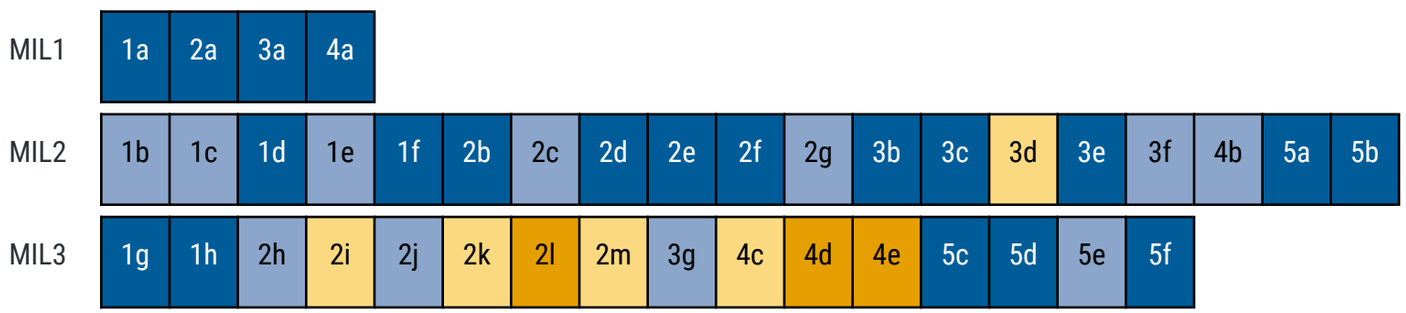
Objective 3: Management Activities for the THREAT domain

	ID	Practice Statement	Response
MIL2	THREAT-3a	Documented procedures are established, followed, and maintained for activities in the THREAT domain	LI
MIL2	THREAT-3b	Adequate resources (people, funding, and tools) are provided to support activities in the THREAT domain	PI
MIL3	THREAT-3c	Up-to-date policies or other organizational directives define requirements for activities in the THREAT domain	FI
MIL3	THREAT-3d	Responsibility, accountability, and authority for the performance of activities in the THREAT domain are assigned to personnel	LI
MIL3	THREAT-3e	Personnel performing activities in the THREAT domain have the skills and knowledge needed to perform their assigned responsibilities	PI
MIL3	THREAT-3f	The effectiveness of activities in the THREAT domain is evaluated and tracked	LI

4.3 Domain: Risk Management (RISK)

Establish, operate, and maintain an enterprise cyber risk management program to identify, analyze, and respond to cyber risk the organization is subject to, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.





Objective 1: Establish and Maintain Cyber Risk Management Strategy and Program

	ID	Practice Statement	Response
MIL1	RISK-1a	The organization has a strategy for cyber risk management, which may be developed and managed in an ad hoc manner	FI
MIL2	RISK-1b	A strategy for cyber risk management is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture	LI
MIL2	RISK-1c	The cyber risk management program is established and maintained to perform cyber risk management activities according to the cyber risk management strategy	LI
MIL2	RISK-1d	Information from RISK domain activities is communicated to relevant stakeholders	FI
MIL2	RISK-1e	Governance for the cyber risk management program is established and maintained	LI
MIL2	RISK-1f	Senior management sponsorship for the cyber risk management program is visible and active	FI
MIL3	RISK-1g	The cyber risk management program aligns with the organization's mission and objectives	FI
MIL3	RISK-1h	The cyber risk management program is coordinated with the organization's enterprise-wide risk management program	FI

Objective 2: Identify Cyber Risk

	ID	Practice Statement	Response
MIL1	RISK-2a	Cyber risks are identified, at least in an ad hoc manner	FI
MIL2	RISK-2b	A defined method is used to identify cyber risks	FI
MIL2	RISK-2c	Stakeholders from appropriate operations and business areas participate in the identification of cyber risks	LI
MIL2	RISK-2d	Identified cyber risks are consolidated into categories (for example, data breaches, insider mistakes, ransomware, OT control takeover) to facilitate management at the category level	FI
MIL2	RISK-2e	Cyber risk categories and cyber risks are documented in a risk register or other artifact	FI
MIL2	RISK-2f	Cyber risk categories and cyber risks are assigned to risk owners	FI
MIL2	RISK-2g	Cyber risk identification activities are performed periodically and according to defined triggers, such as system changes and external events	LI
MIL3	RISK-2h	Cyber risk identification activities leverage asset inventory and prioritization information from the ASSET domain, such as IT and OT asset end of support, single points of failure, information asset risk of disclosure, tampering, or destruction	LI

	ID	Practice Statement	Response
MIL3	RISK-2i	Vulnerability management information from THREAT domain activities is used to update cyber risks and identify new risks (such as risks arising from vulnerabilities that pose an ongoing risk to the organization or newly identified vulnerabilities)	PI
MIL3	RISK-2j	Threat management information from THREAT domain activities is used to update cyber risks and identify new risks	LI
MIL3	RISK-2k	Information from THIRD-PARTIES domain activities is used to update cyber risks and identify new risks	PI
MIL3	RISK-2l	Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks	NI
MIL3	RISK-2m	Cyber risk identification considers risks that may arise from or affect critical infrastructure or other interdependent organizations	PI

Objective 3: Analyze Cyber Risk

	ID	Practice Statement	Response
MIL1	RISK-3a	Cyber risks are prioritized based on estimated impact, at least in an ad hoc manner	FI
MIL2	RISK-3b	Defined criteria are used to prioritize cyber risks (for example, impact to the organization, impact to the community, likelihood, susceptibility, risk tolerance)	FI
MIL2	RISK-3c	A defined method is used to estimate impact for higher priority cyber risks (for example, comparison to actual events, risk quantification)	FI
MIL2	RISK-3d	Defined methods are used to analyze higher-priority cyber risks (for example, analyzing the prevalence of types of attacks to estimate likelihood, using the results of controls assessments to estimate susceptibility)	PI
MIL2	RISK-3e	Organizational stakeholders from appropriate operations and business functions participate in the analysis of higher-priority cyber risks	FI
MIL2	RISK-3f	Cyber risks are removed from the risk register or other artifact used to document and manage identified risks when they no longer require tracking or response	LI
MIL3	RISK-3g	Cyber risk analyses are updated periodically and according to defined triggers, such as system changes, external events, and information from other model domains	LI

Objective 4: Respond to Cyber Risk

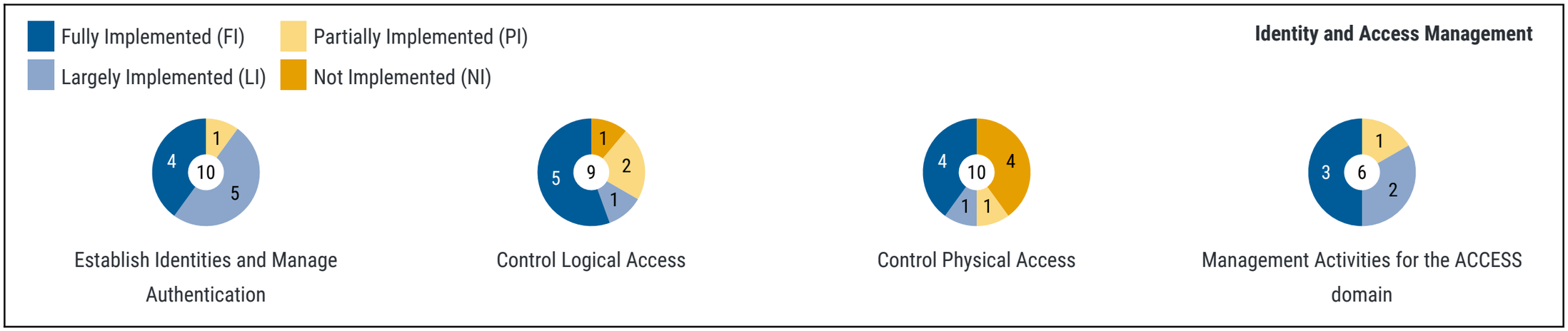
	ID	Practice Statement	Response
MIL1	RISK-4a	Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risks, at least in an ad hoc manner	FI
MIL2	RISK-4b	A defined method is used to select and implement risk responses based on analysis and prioritization	LI
MIL3	RISK-4c	Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to mitigate identified cyber risks	PI
MIL3	RISK-4d	Results from cyber risk impact analyses and cybersecurity control evaluations are reviewed together by enterprise leadership to determine whether cyber risks are sufficiently mitigated and risk tolerances are not exceeded	NI
MIL3	RISK-4e	Risk responses (such as mitigate, accept, avoid, or transfer) are reviewed periodically by leadership to determine whether they are still appropriate	NI

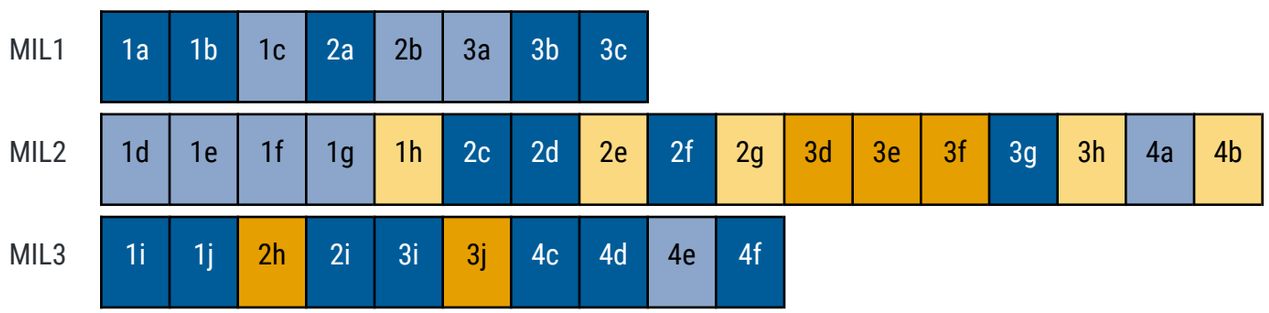
Objective 5: Management Activities for the RISK domain

	ID	Practice Statement	Response
MIL2	RISK-5a	Documented procedures are established, followed, and maintained for activities in the RISK domain	FI
MIL2	RISK-5b	Adequate resources (people, funding, and tools) are provided to support activities in the RISK domain	FI
MIL3	RISK-5c	Up-to-date policies or other organizational directives define requirements for activities in the RISK domain	FI
MIL3	RISK-5d	Responsibility, accountability, and authority for the performance of activities in the RISK domain are assigned to personnel	FI
MIL3	RISK-5e	Personnel performing activities in the RISK domain have the skills and knowledge needed to perform their assigned responsibilities	LI
MIL3	RISK-5f	The effectiveness of activities in the RISK domain is evaluated and tracked	FI

4.4 Domain: Identity and Access Management (ACCESS)

Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.





Objective 1: Establish Identities and Manage Authentication

	ID	Practice Statement	Response
MIL1	ACCESS-1a	Identities are provisioned, at least in an ad hoc manner, for personnel and other entities such as services and devices that require access to assets (note that this does not preclude shared identities)	FI
MIL1	ACCESS-1b	Credentials (such as passwords, smartcards, certificates, and keys) are issued for personnel and other entities that require access to assets, at least in an ad hoc manner	FI
MIL1	ACCESS-1c	Identities are deprovisioned, at least in an ad hoc manner, when no longer required	LI
MIL2	ACCESS-1d	Password strength and reuse restrictions are defined and enforced	LI
MIL2	ACCESS-1e	Identity repositories are reviewed and updated periodically and according to defined triggers, such as system changes and changes to organizational structure	LI
MIL2	ACCESS-1f	Identities are deprovisioned within organization-defined time thresholds when no longer required	LI
MIL2	ACCESS-1g	The use of privileged credentials is limited to processes for which they are required	LI
MIL2	ACCESS-1h	Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access)	PI
MIL3	ACCESS-1i	Multifactor authentication is required for all access, where feasible	FI

	ID	Practice Statement	Response
MIL3	ACCESS-1j	Identities are disabled after a defined period of inactivity, where feasible	FI

Objective 2: Control Logical Access

	ID	Practice Statement	Response
MIL1	ACCESS-2a	Logical access controls are implemented, at least in an ad hoc manner	FI
MIL1	ACCESS-2b	Logical access privileges are revoked when no longer needed, at least in an ad hoc manner	LI
MIL2	ACCESS-2c	Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters)	FI
MIL2	ACCESS-2d	Logical access requirements incorporate the principle of least privilege	FI
MIL2	ACCESS-2e	Logical access requirements incorporate the principle of separation of duties	PI
MIL2	ACCESS-2f	Logical access requests are reviewed and approved by the asset owner	FI
MIL2	ACCESS-2g	Logical access privileges that pose a higher risk to the function receive additional scrutiny and monitoring	PI
MIL3	ACCESS-2h	Logical access privileges are reviewed and updated to ensure conformance with access requirements periodically and according to defined triggers, such as changes to organizational structure, and after any temporary elevation of privileges	NI

	ID	Practice Statement	Response
MIL3	ACCESS-2i	Anomalous logical access attempts are monitored as indicators of cybersecurity events	FI

Objective 3: Control Physical Access

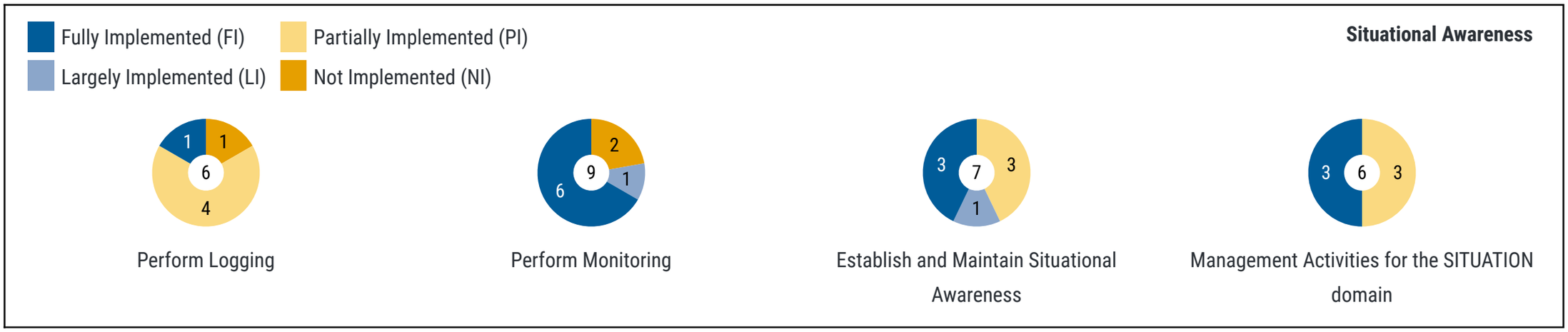
	ID	Practice Statement	Response
MIL1	ACCESS-3a	Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner	LI
MIL1	ACCESS-3b	Physical access privileges are revoked when no longer needed, at least in an ad hoc manner	FI
MIL1	ACCESS-3c	Physical access logs are maintained, at least in an ad hoc manner	FI
MIL2	ACCESS-3d	Physical access requirements are established and maintained (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access)	NI
MIL2	ACCESS-3e	Physical access requirements incorporate the principle of least privilege	NI
MIL2	ACCESS-3f	Physical access requirements incorporate the principle of separation of duties	NI
MIL2	ACCESS-3g	Physical access requests are reviewed and approved by the asset owner	FI
MIL2	ACCESS-3h	Physical access privileges that pose higher risk to the function receive additional scrutiny and monitoring	PI
MIL3	ACCESS-3i	Physical access privileges are reviewed and updated	FI
MIL3	ACCESS-3j	Physical access is monitored to identify potential cybersecurity events	NI

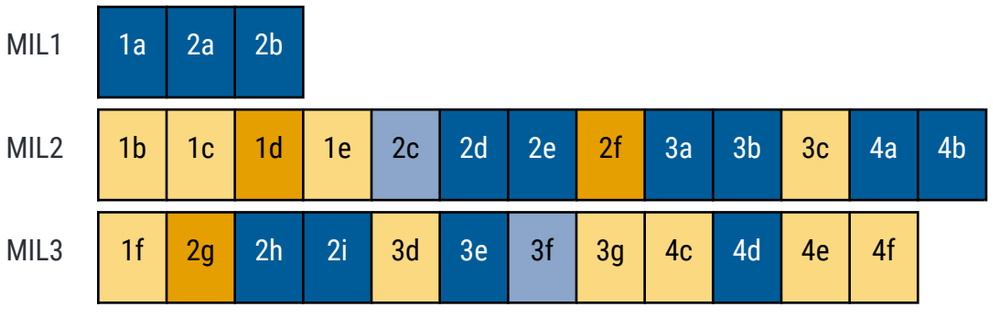
Objective 4: Management Activities for the ACCESS domain

	ID	Practice Statement	Response
MIL2	ACCESS-4a	Documented procedures are established, followed, and maintained for activities in the ACCESS domain	LI
MIL2	ACCESS-4b	Adequate resources (people, funding, and tools) are provided to support activities in the ACCESS domain	PI
MIL3	ACCESS-4c	Up-to-date policies or other organizational directives define requirements for activities in the ACCESS domain	FI
MIL3	ACCESS-4d	Responsibility, accountability, and authority for the performance of activities in the ACCESS domain are assigned to personnel	FI
MIL3	ACCESS-4e	Personnel performing activities in the ACCESS domain have the skills and knowledge needed to perform their assigned responsibilities	LI
MIL3	ACCESS-4f	The effectiveness of activities in the ACCESS domain is evaluated and tracked	FI

4.5 Domain: Situational Awareness (SITUATION)

Establish and maintain activities and technologies to collect, monitor, analyze, alarm, report, and use operational, security, and threat information, including status and summary information from the other model domains, to establish situational awareness for both the organization's operational state and cybersecurity state.





Objective 1: Perform Logging

	ID	Practice Statement	Response
MIL1	SITUATION-1a	Logging is occurring for assets that are important to the delivery of the function, at least in an ad hoc manner	FI
MIL2	SITUATION-1b	Logging is occurring for assets within the function that may be leveraged to achieve a threat objective, wherever feasible	PI
MIL2	SITUATION-1c	Logging requirements are established and maintained for IT and OT assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective	PI
MIL2	SITUATION-1d	Logging requirements are established and maintained for network and host monitoring infrastructure (for example, web gateways, endpoint detection and response software, intrusion detection and prevention systems)	NI
MIL2	SITUATION-1e	Log data are being aggregated within the function	PI
MIL3	SITUATION-1f	More rigorous logging is performed for higher priority assets	PI

Objective 2: Perform Monitoring

	ID	Practice Statement	Response
MIL1	SITUATION-2a	Periodic reviews of log data or other cybersecurity monitoring activities are performed, at least in an ad hoc manner	FI
MIL1	SITUATION-2b	Data and alerts from network and host monitoring infrastructure assets are periodically reviewed, at least in an ad hoc manner	FI
MIL2	SITUATION-2c	Monitoring and analysis requirements are established and maintained for the function and address timely review of event data	LI
MIL2	SITUATION-2d	Indicators of anomalous activity are established and maintained based on system logs, data flows, network baselines, cybersecurity events, and architecture and are monitored across the IT and OT environments	FI
MIL2	SITUATION-2e	Alarms and alerts are configured and maintained to support the identification of cybersecurity events	FI
MIL2	SITUATION-2f	Monitoring activities are aligned with the threat profile (THREAT-2e)	NI
MIL3	SITUATION-2g	More rigorous monitoring is performed for higher priority assets	NI
MIL3	SITUATION-2h	Risk analysis information (RISK-3d) is used to identify indicators of anomalous activity	FI

	ID	Practice Statement	Response
MIL3	SITUATION-2i	Indicators of anomalous activity are evaluated and updated periodically and according to defined triggers, such as system changes and external events	FI

Objective 3: Establish and Maintain Situational Awareness

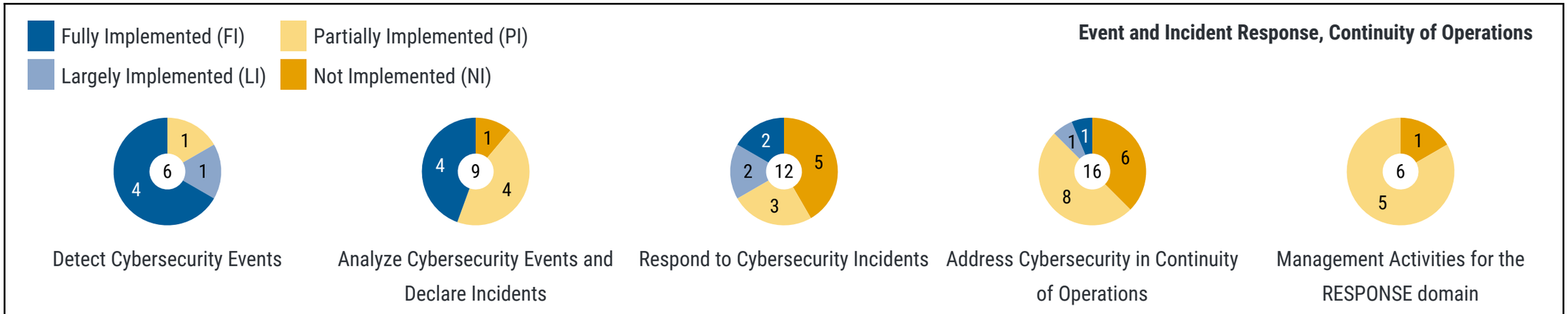
	ID	Practice Statement	Response
MIL2	SITUATION-3a	Methods of communicating the current state of cybersecurity for the function are established and maintained	FI
MIL2	SITUATION-3b	Monitoring data are aggregated to provide an understanding of the operational state of the function	FI
MIL2	SITUATION-3c	Relevant information from across the organization is available to enhance situational awareness	PI
MIL3	SITUATION-3d	Situational awareness reporting requirements have been defined and address the timely dissemination of cybersecurity information to organization-defined stakeholders	PI
MIL3	SITUATION-3e	Relevant information from outside the organization is collected and made available across the organization to enhance situational awareness	FI
MIL3	SITUATION-3f	A capability is established and maintained to aggregate, correlate, and analyze the outputs of cybersecurity monitoring activities and provide a near-real-time understanding of the cybersecurity state of the function	LI
MIL3	SITUATION-3g	Predefined states of operation are documented and can be implemented based on the cybersecurity state of the function or when triggered by activities in other domains	PI

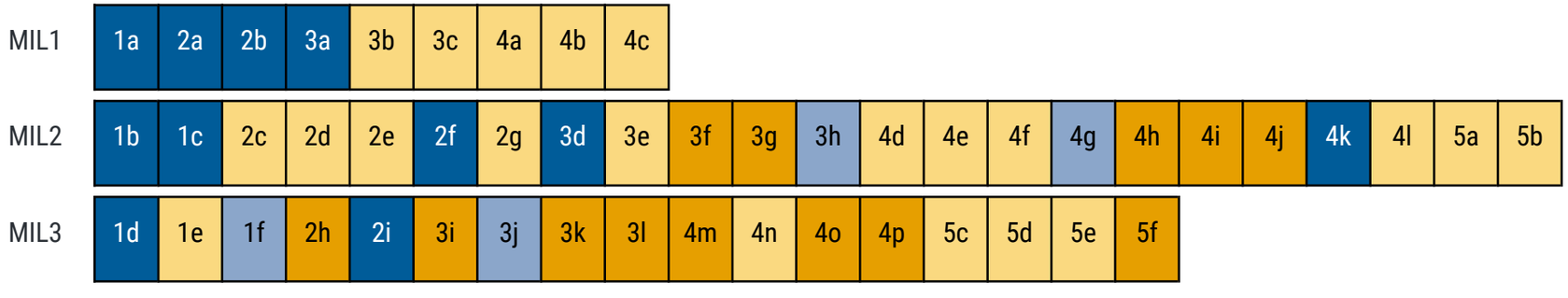
Objective 4: Management Activities for the SITUATION domain

	ID	Practice Statement	Response
MIL2	SITUATION-4a	Documented procedures are established, followed, and maintained for activities in the SITUATION domain	FI
MIL2	SITUATION-4b	Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	FI
MIL3	SITUATION-4c	Up-to-date policies or other organizational directives define requirements for activities in the SITUATION domain	PI
MIL3	SITUATION-4d	Responsibility, accountability, and authority for the performance of activities in the SITUATION domain are assigned to personnel	FI
MIL3	SITUATION-4e	Personnel performing activities in the SITUATION domain have the skills and knowledge needed to perform their assigned responsibilities	PI
MIL3	SITUATION-4f	The effectiveness of activities in the SITUATION domain is evaluated and tracked	PI

4.6 Domain: Event and Incident Response, Continuity of Operations (RESPONSE)

Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents and to sustain operations during cybersecurity incidents, commensurate with the risk to critical infrastructure and organizational objectives.





Objective 1: Detect Cybersecurity Events

	ID	Practice Statement	Response
MIL1	RESPONSE-1a	Detected cybersecurity events are reported to a specified person or role and documented, at least in an ad hoc manner	FI
MIL2	RESPONSE-1b	Criteria are established for cybersecurity event detection (for example, what constitutes a cybersecurity event, where to look for cybersecurity events)	FI
MIL2	RESPONSE-1c	Cybersecurity events are documented based on the established criteria	FI
MIL3	RESPONSE-1d	Event information is correlated to support incident analysis by identifying patterns, trends, and other common features	FI
MIL3	RESPONSE-1e	Cybersecurity event detection activities are adjusted based on identified risks and the organization's threat profile (THREAT-2e)	PI
MIL3	RESPONSE-1f	Situational awareness for the function is monitored to support the identification of cybersecurity events	LI

Objective 2: Analyze Cybersecurity Events and Declare Incidents

	ID	Practice Statement	Response
MIL1	RESPONSE-2a	Criteria for declaring cybersecurity incidents are established, at least in an ad hoc manner	FI
MIL1	RESPONSE-2b	Cybersecurity events are analyzed to support the declaration of cybersecurity incidents, at least in an ad hoc manner	FI
MIL2	RESPONSE-2c	Cybersecurity incident declaration criteria are formally established based on potential impact to the function	PI
MIL2	RESPONSE-2d	Cybersecurity events are declared to be incidents based on established criteria	PI
MIL2	RESPONSE-2e	Cybersecurity incident declaration criteria are updated periodically and according to defined triggers, such as organizational changes, lessons learned from plan execution, or newly identified threats	PI
MIL2	RESPONSE-2f	There is a repository where cybersecurity events and incidents are documented and tracked to closure	FI
MIL2	RESPONSE-2g	Internal and external stakeholders (for example, executives, attorneys, government agencies, connected organizations, vendors, sector organizations, regulators) are identified and notified of incidents based on situational awareness reporting requirements (SITUATION-3d)	PI
MIL3	RESPONSE-2h	Criteria for cybersecurity incident declaration are aligned with cyber risk prioritization criteria (RISK-3b)	NI

	ID	Practice Statement	Response
MIL3	RESPONSE-2i	Cybersecurity incidents are correlated to identify patterns, trends, and other common features across multiple incidents	FI

Objective 3: Respond to Cybersecurity Incidents

	ID	Practice Statement	Response
MIL1	RESPONSE-3a	Cybersecurity incident response personnel are identified and roles are assigned, at least in an ad hoc manner	FI
MIL1	RESPONSE-3b	Responses to cybersecurity incidents are executed, at least in an ad hoc manner, to limit impact to the function and restore normal operations	PI
MIL1	RESPONSE-3c	Reporting of incidents is performed (for example, internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner	PI
MIL2	RESPONSE-3d	Cybersecurity incident response plans that address all phases of the incident life cycle are established and maintained	FI
MIL2	RESPONSE-3e	Cybersecurity incident response is executed according to defined plans and procedures	PI
MIL2	RESPONSE-3f	Cybersecurity incident response plans include a communications plan for internal and external stakeholders	NI
MIL2	RESPONSE-3g	Cybersecurity incident response plan exercises are conducted periodically and according to defined triggers, such as system changes and external events	NI
MIL2	RESPONSE-3h	Cybersecurity incident lessons-learned activities are performed and corrective actions are taken, including updates to the incident response plan	LI

	ID	Practice Statement	Response
MIL3	RESPONSE-3i	Cybersecurity incident root-cause analysis is performed and corrective actions are taken, including updates to the incident response plan	NI
MIL3	RESPONSE-3j	Cybersecurity incident responses are coordinated with vendors, law enforcement, and other external entities as appropriate, including support for evidence collection and preservation	LI
MIL3	RESPONSE-3k	Cybersecurity incident response personnel participate in joint cybersecurity exercises with other organizations	NI
MIL3	RESPONSE-3l	Cybersecurity incident responses leverage and trigger predefined states of operation (SITUATION-3g)	NI

Objective 4: Address Cybersecurity in Continuity of Operations

	ID	Practice Statement	Response
MIL1	RESPONSE-4a	Continuity plans are developed to sustain and restore operation of the function if a cybersecurity event or incident occurs, at least in an ad hoc manner	PI
MIL1	RESPONSE-4b	Data backups are available and tested, at least in an ad hoc manner	PI
MIL1	RESPONSE-4c	IT and OT assets requiring spares are identified, at least in an ad hoc manner	PI
MIL2	RESPONSE-4d	Continuity plans address potential impacts from cybersecurity incidents	PI
MIL2	RESPONSE-4e	The assets and activities necessary to sustain minimum operations of the function are identified and documented in continuity plans	PI
MIL2	RESPONSE-4f	Continuity plans address IT, OT, and information assets that are important to the delivery of the function, including the availability of backup data and replacement, redundant, and spare IT and OT assets	PI
MIL2	RESPONSE-4g	Recovery time objectives (RTOs) and recovery point objectives (RPOs) for assets that are important to the delivery of the function are incorporated into continuity plans	LI

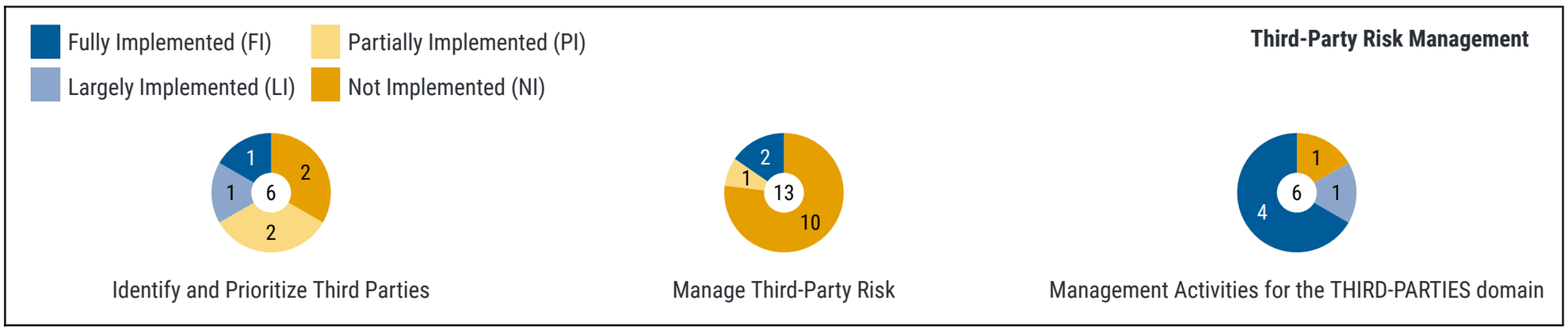
	ID	Practice Statement	Response
MIL2	RESPONSE-4h	Cybersecurity incident criteria that trigger the execution of continuity plans are established and communicated to incident response and continuity management personnel	NI
MIL2	RESPONSE-4i	Continuity plans are tested through evaluations and exercises periodically and according to defined triggers, such as system changes and external events	NI
MIL2	RESPONSE-4j	Cybersecurity controls protecting backup data are equivalent to or more rigorous than controls protecting source data	NI
MIL2	RESPONSE-4k	Data backups are logically or physically separated from source data	FI
MIL2	RESPONSE-4l	Spares for selected IT and OT assets are available	PI
MIL3	RESPONSE-4m	Continuity plans are aligned with identified risks and the organization's threat profile (THREAT-2e) to ensure coverage of identified risk categories and threats	NI
MIL3	RESPONSE-4n	Continuity plan exercises address higher priority risks	PI
MIL3	RESPONSE-4o	The results of continuity plan testing or activation are compared to recovery objectives, and plans are improved accordingly	NI
MIL3	RESPONSE-4p	Continuity plans are periodically reviewed and updated	NI

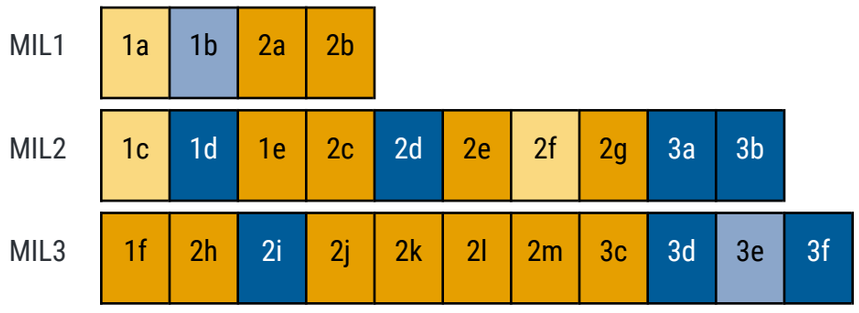
Objective 5: Management Activities for the RESPONSE domain

	ID	Practice Statement	Response
MIL2	RESPONSE-5a	Documented procedures are established, followed, and maintained for activities in the RESPONSE domain	PI
MIL2	RESPONSE-5b	Adequate resources (people, funding, and tools) are provided to support activities in the RESPONSE domain	PI
MIL3	RESPONSE-5c	Up-to-date policies or other organizational directives define requirements for activities in the RESPONSE domain	PI
MIL3	RESPONSE-5d	Responsibility, accountability, and authority for the performance of activities in the RESPONSE domain are assigned to personnel	PI
MIL3	RESPONSE-5e	Personnel performing activities in the RESPONSE domain have the skills and knowledge needed to perform their assigned responsibilities	PI
MIL3	RESPONSE-5f	The effectiveness of activities in the RESPONSE domain is evaluated and tracked	NI

4.7 Domain: Third-Party Risk Management (THIRD-PARTIES)

Establish and maintain controls to manage the cyber risks arising from suppliers and other third parties, commensurate with the risk to critical infrastructure and organizational objectives.





Objective 1: Identify and Prioritize Third Parties

	ID	Practice Statement	Response
MIL1	THIRD-PARTIES-1a	Important IT and OT third-party dependencies are identified (that is, internal and external parties on which the delivery of the function depends, including operating partners), at least in an ad hoc manner	PI
MIL1	THIRD-PARTIES-1b	Third parties that have access to, control of, or custody of any IT, OT, or information assets that are important to the delivery of the function are identified, at least in an ad hoc manner	LI
MIL2	THIRD-PARTIES-1c	A defined method is followed to identify risks arising from suppliers and other third parties	PI
MIL2	THIRD-PARTIES-1d	Third parties are prioritized according to established criteria (for example, importance to the delivery of the function, impact of a compromise or disruption, ability to negotiate cybersecurity requirements within contracts)	FI
MIL2	THIRD-PARTIES-1e	Escalated prioritization is assigned to suppliers and other third parties whose compromise or disruption could cause significant consequences (for example, single-source suppliers, suppliers with privileged access)	NI
MIL3	THIRD-PARTIES-1f	Prioritization of suppliers and other third parties is updated periodically and according to defined triggers, such as system changes and external events	NI

Objective 2: Manage Third-Party Risk

	ID	Practice Statement	Response
MIL1	THIRD-PARTIES-2a	The selection of suppliers and other third parties includes consideration of their cybersecurity qualifications, at least in an ad hoc manner	NI
MIL1	THIRD-PARTIES-2b	The selection of products and services includes consideration of their cybersecurity capabilities, at least in an ad hoc manner	NI
MIL2	THIRD-PARTIES-2c	A defined method is followed to identify cybersecurity requirements and implement associated controls that protect against the risks arising from suppliers and other third parties	NI
MIL2	THIRD-PARTIES-2d	A defined method is followed to evaluate and select suppliers and other third parties	FI
MIL2	THIRD-PARTIES-2e	More rigorous cybersecurity controls are implemented for higher priority suppliers and other third parties	NI
MIL2	THIRD-PARTIES-2f	Cybersecurity requirements (for example, vulnerability notification, incident-related SLA requirements) are formalized in agreements with suppliers and other third parties	PI
MIL2	THIRD-PARTIES-2g	Suppliers and other third parties periodically attest to their ability to meet cybersecurity requirements	NI

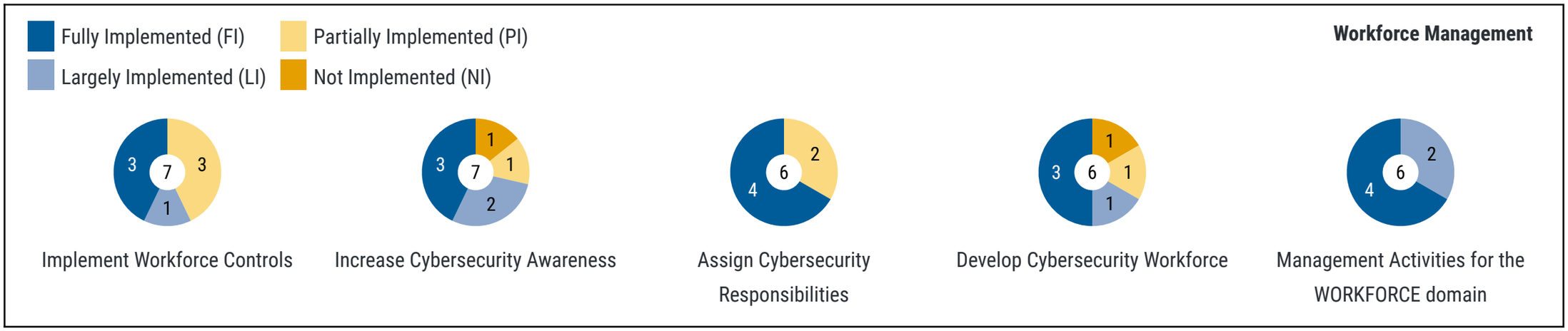
	ID	Practice Statement	Response
MIL3	THIRD-PARTIES-2h	Cybersecurity requirements for suppliers and other third parties include secure software and secure product development requirements where appropriate	NI
MIL3	THIRD-PARTIES-2i	Selection criteria for products include consideration of end-of-life and end-of-support timelines	FI
MIL3	THIRD-PARTIES-2j	Selection criteria include consideration of safeguards against counterfeit or compromised software, hardware, and services	NI
MIL3	THIRD-PARTIES-2k	Selection criteria for higher priority assets include evaluation of bills of material for key asset elements, such as hardware and software	NI
MIL3	THIRD-PARTIES-2l	Selection criteria for higher priority assets include evaluation of any associated third-party hosting environments and source data	NI
MIL3	THIRD-PARTIES-2m	Acceptance testing of procured assets includes consideration of cybersecurity requirements	NI

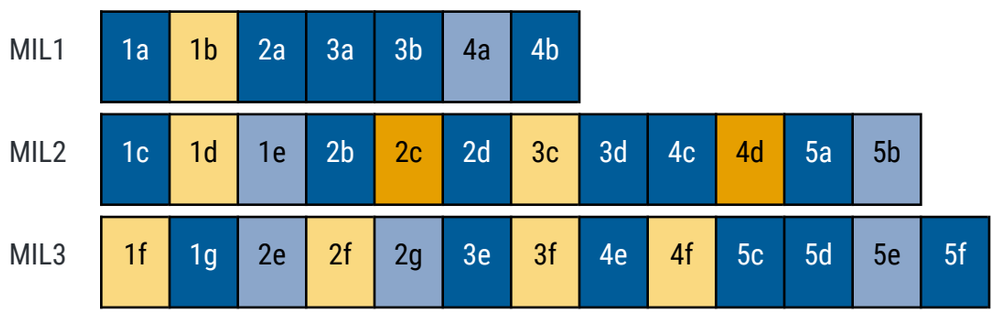
Objective 3: Management Activities for the THIRD-PARTIES domain

	ID	Practice Statement	Response
MIL2	THIRD-PARTIES-3a	Documented procedures are established, followed, and maintained for activities in the THIRD-PARTIES domain	FI
MIL2	THIRD-PARTIES-3b	Adequate resources (people, funding, and tools) are provided to support activities in the THIRD-PARTIES domain	FI
MIL3	THIRD-PARTIES-3c	Up-to-date policies or other organizational directives define requirements for activities in the THIRD-PARTIES domain	NI
MIL3	THIRD-PARTIES-3d	Responsibility, accountability, and authority for the performance of activities in the THIRD-PARTIES domain are assigned to personnel	FI
MIL3	THIRD-PARTIES-3e	Personnel performing activities in the THIRD-PARTIES domain have the skills and knowledge needed to perform their assigned responsibilities	LI
MIL3	THIRD-PARTIES-3f	The effectiveness of activities in the THIRD-PARTIES domain is evaluated and tracked	FI

4.8 Domain: Workforce Management (WORKFORCE)

Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.





Objective 1: Implement Workforce Controls

	ID	Practice Statement	Response
MIL1	WORKFORCE-1a	Personnel vetting (for example, background checks, drug tests) is performed upon hire, at least in an ad hoc manner	FI
MIL1	WORKFORCE-1b	Personnel separation procedures address cybersecurity, at least in an ad hoc manner	PI
MIL2	WORKFORCE-1c	Personnel vetting is performed at hire and periodically for positions that have access to assets that are important to the delivery of the function	FI
MIL2	WORKFORCE-1d	Personnel separation and transfer procedures address cybersecurity, including supplementary vetting as appropriate	PI
MIL2	WORKFORCE-1e	Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets	LI
MIL3	WORKFORCE-1f	Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk	PI
MIL3	WORKFORCE-1g	A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures	FI

Objective 2: Increase Cybersecurity Awareness

	ID	Practice Statement	Response
MIL1	WORKFORCE-2a	Cybersecurity awareness activities occur, at least in an ad hoc manner	FI
MIL2	WORKFORCE-2b	Cybersecurity awareness objectives are established and maintained	FI
MIL2	WORKFORCE-2c	Cybersecurity awareness objectives are aligned with the defined threat profile (THREAT-2e)	NI
MIL2	WORKFORCE-2d	Cybersecurity awareness activities are conducted periodically	FI
MIL3	WORKFORCE-2e	Cybersecurity awareness activities are tailored to job role	LI
MIL3	WORKFORCE-2f	Cybersecurity awareness activities address predefined states of operation (SITUATION-3g)	PI
MIL3	WORKFORCE-2g	The effectiveness of cybersecurity awareness activities is evaluated periodically and according to defined triggers, such as system changes and external events, and improvements are made as appropriate	LI

Objective 3: Assign Cybersecurity Responsibilities

	ID	Practice Statement	Response
MIL1	WORKFORCE-3a	Cybersecurity responsibilities for the function are identified, at least in an ad hoc manner	FI
MIL1	WORKFORCE-3b	Cybersecurity responsibilities are assigned to specific people, at least in an ad hoc manner	FI
MIL2	WORKFORCE-3c	Cybersecurity responsibilities are assigned to specific roles, including external service providers	PI
MIL2	WORKFORCE-3d	Cybersecurity responsibilities are documented	FI
MIL3	WORKFORCE-3e	Cybersecurity responsibilities and job requirements are reviewed and updated periodically and according to defined triggers, such as system changes and changes to organizational structure	FI
MIL3	WORKFORCE-3f	Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage, including succession planning	PI

Objective 4: Develop Cybersecurity Workforce

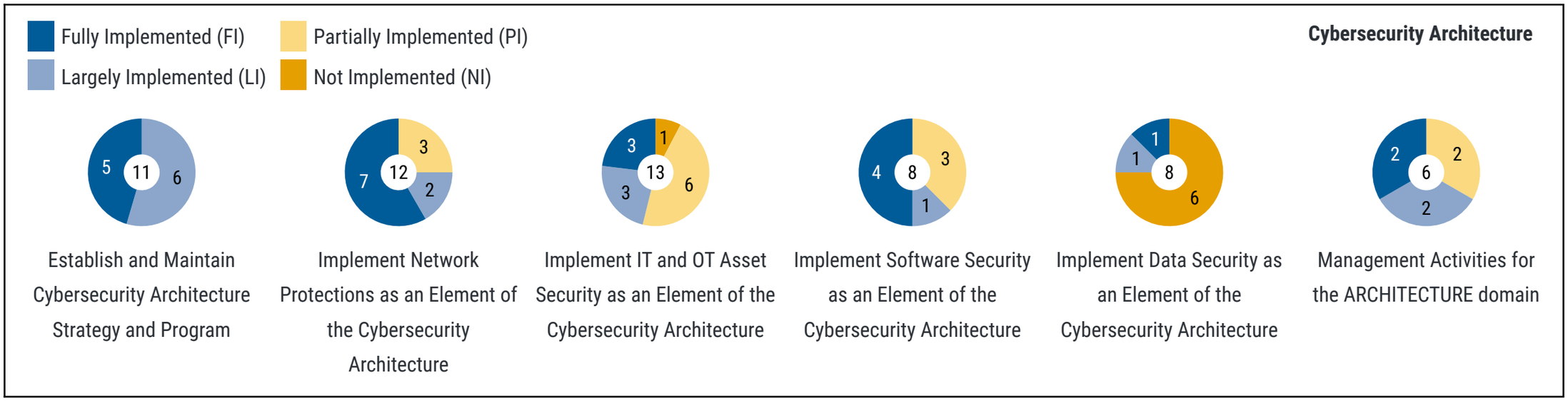
	ID	Practice Statement	Response
MIL1	WORKFORCE-4a	Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities, at least in an ad hoc manner	LI
MIL1	WORKFORCE-4b	Cybersecurity knowledge, skill, and ability requirements and gaps are identified for both current and future operational needs, at least in an ad hoc manner	FI
MIL2	WORKFORCE-4c	Identified cybersecurity knowledge, skill, and ability gaps are addressed through training, recruiting, and retention efforts	FI
MIL2	WORKFORCE-4d	Cybersecurity training is provided as a prerequisite to granting access to assets that are important to the delivery of the function	NI
MIL3	WORKFORCE-4e	The effectiveness of training programs is evaluated periodically, and improvements are made as appropriate	FI
MIL3	WORKFORCE-4f	Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities	PI

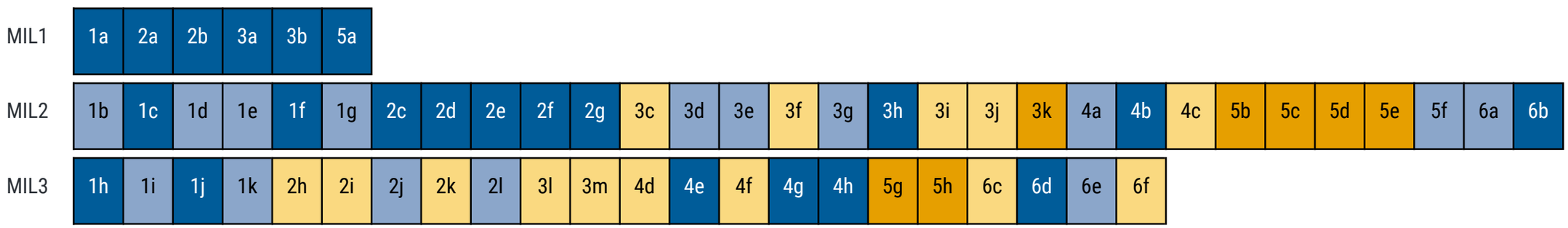
Objective 5: Management Activities for the WORKFORCE domain

	ID	Practice Statement	Response
MIL2	WORKFORCE-5a	Documented procedures are established, followed, and maintained for activities in the WORKFORCE domain	FI
MIL2	WORKFORCE-5b	Adequate resources (people, funding, and tools) are provided to support activities in the WORKFORCE domain	LI
MIL3	WORKFORCE-5c	Up-to-date policies or other organizational directives define requirements for activities in the WORKFORCE domain	FI
MIL3	WORKFORCE-5d	Responsibility, accountability, and authority for the performance of activities in the WORKFORCE domain are assigned to personnel	FI
MIL3	WORKFORCE-5e	Personnel performing activities in the WORKFORCE domain have the skills and knowledge needed to perform their assigned responsibilities	LI
MIL3	WORKFORCE-5f	The effectiveness of activities in the WORKFORCE domain is evaluated and tracked	FI

4.9 Domain: Cybersecurity Architecture (ARCHITECTURE)

Establish and maintain the structure and behavior of the organization's cybersecurity architecture, including controls, processes, technologies, and other elements, commensurate with the risk to critical infrastructure and organizational objectives.





Objective 1: Establish and Maintain Cybersecurity Architecture Strategy and Program

	ID	Practice Statement	Response
MIL1	ARCHITECTURE-1a	The organization has a strategy for cybersecurity architecture, which may be developed and managed in an ad hoc manner	FI
MIL2	ARCHITECTURE-1b	A strategy for cybersecurity architecture is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture	LI
MIL2	ARCHITECTURE-1c	A documented cybersecurity architecture is established and maintained that includes IT and OT systems and networks and aligns with system and asset categorization and prioritization	FI
MIL2	ARCHITECTURE-1d	Governance for cybersecurity architecture (such as an architecture review process) is established and maintained that includes provisions for periodic architectural reviews and an exceptions process	LI
MIL2	ARCHITECTURE-1e	Senior management sponsorship for the cybersecurity architecture program is visible and active	LI
MIL2	ARCHITECTURE-1f	The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets	FI
MIL2	ARCHITECTURE-1g	Cybersecurity controls are selected and implemented to meet cybersecurity requirements	LI

	ID	Practice Statement	Response
MIL3	ARCHITECTURE-1h	The cybersecurity architecture strategy and program are aligned with the organization's enterprise architecture strategy and program	FI
MIL3	ARCHITECTURE-1i	Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events	LI
MIL3	ARCHITECTURE-1j	The cybersecurity architecture is guided by the organization's risk analysis information (RISK-3d) and threat profile (THREAT-2e)	FI
MIL3	ARCHITECTURE-1k	The cybersecurity architecture addresses predefined states of operation (SITUATION-3g)	LI

Objective 2: Implement Network Protections as an Element of the Cybersecurity Architecture

	ID	Practice Statement	Response
MIL1	ARCHITECTURE-2a	Network protections are implemented, at least in an ad hoc manner	FI
MIL1	ARCHITECTURE-2b	The organization's IT systems are separated from OT systems through segmentation, either through physical means or logical means, at least in an ad hoc manner	FI
MIL2	ARCHITECTURE-2c	Network protections are defined and enforced for selected asset types according to asset risk and priority (for example, internal assets, perimeter assets, assets connected to the organization's Wi-Fi, cloud assets, remote access, and externally owned devices)	FI
MIL2	ARCHITECTURE-2d	Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements	FI
MIL2	ARCHITECTURE-2e	Network protections incorporate the principles of least privilege and least functionality	FI
MIL2	ARCHITECTURE-2f	Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, allowlisting, intrusion detection and prevention systems [IDPS])	FI

	ID	Practice Statement	Response
MIL2	ARCHITECTURE-2g	Web traffic and email are monitored, analyzed, and controlled (for example, malicious link blocking, suspicious download blocking, email authentication techniques, IP address blocking)	FI
MIL3	ARCHITECTURE-2h	All assets are segmented into distinct security zones based on cybersecurity requirements	PI
MIL3	ARCHITECTURE-2i	Separate networks are implemented, where warranted, that logically or physically segment assets into security zones with independent authentication	PI
MIL3	ARCHITECTURE-2j	OT systems are operationally independent from IT systems so that OT operations can be sustained during an outage of IT systems	LI
MIL3	ARCHITECTURE-2k	Device connections to the network are controlled to ensure that only authorized devices can connect (for example, network access control [NAC])	PI
MIL3	ARCHITECTURE-2l	The cybersecurity architecture enables the isolation of compromised assets	LI

Objective 3: Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture

	ID	Practice Statement	Response
MIL1	ARCHITECTURE-3a	Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner	FI
MIL1	ARCHITECTURE-3b	Endpoint protections (such as secure configuration, security applications, and host monitoring) are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner	FI
MIL2	ARCHITECTURE-3c	The principle of least privilege (for example, limiting administrative access for users and service accounts) is enforced	PI
MIL2	ARCHITECTURE-3d	The principle of least functionality (for example, limiting services, limiting applications, limiting ports, limiting connected devices) is enforced	LI
MIL2	ARCHITECTURE-3e	Secure configurations are established and maintained as part of the asset deployment process where feasible	LI
MIL2	ARCHITECTURE-3f	Security applications are required as an element of device configuration where feasible (for example, endpoint detection and response, host-based firewalls)	PI

	ID	Practice Statement	Response
MIL2	ARCHITECTURE-3g	The use of removeable media is controlled (for example, limiting the use of USB devices, managing external hard drives)	LI
MIL2	ARCHITECTURE-3h	Cybersecurity controls are implemented for all assets within the function either at the asset level or as compensating controls where asset-level controls are not feasible	FI
MIL2	ARCHITECTURE-3i	Maintenance and capacity management activities are performed for all assets within the function	PI
MIL2	ARCHITECTURE-3j	The physical operating environment is controlled to protect the operation of assets within the function	PI
MIL2	ARCHITECTURE-3k	More rigorous cybersecurity controls are implemented for higher priority assets	NI
MIL3	ARCHITECTURE-3l	Configuration of and changes to firmware are controlled throughout the asset lifecycle	PI
MIL3	ARCHITECTURE-3m	Controls (such as allowlists, blocklists, and configuration settings) are implemented to prevent the execution of unauthorized code	PI

Objective 4: Implement Software Security as an Element of the Cybersecurity Architecture

	ID	Practice Statement	Response
MIL2	ARCHITECTURE-4a	Software developed in-house for deployment on higher priority assets is developed using secure software development practices	LI
MIL2	ARCHITECTURE-4b	The selection of procured software for deployment on higher priority assets includes consideration of the vendor's secure software development practices	FI
MIL2	ARCHITECTURE-4c	Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house	PI
MIL3	ARCHITECTURE-4d	All software developed in-house is developed using secure software development practices	PI
MIL3	ARCHITECTURE-4e	The selection of all procured software includes consideration of the vendor's secure software development practices	FI
MIL3	ARCHITECTURE-4f	The architecture review process evaluates the security of new and revised applications prior to deployment	PI
MIL3	ARCHITECTURE-4g	The authenticity of all software and firmware is validated prior to deployment	FI

	ID	Practice Statement	Response
MIL3	ARCHITECTURE-4h	Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications periodically and according to defined triggers, such as system changes and external events	FI

Objective 5: Implement Data Security as an Element of the Cybersecurity Architecture

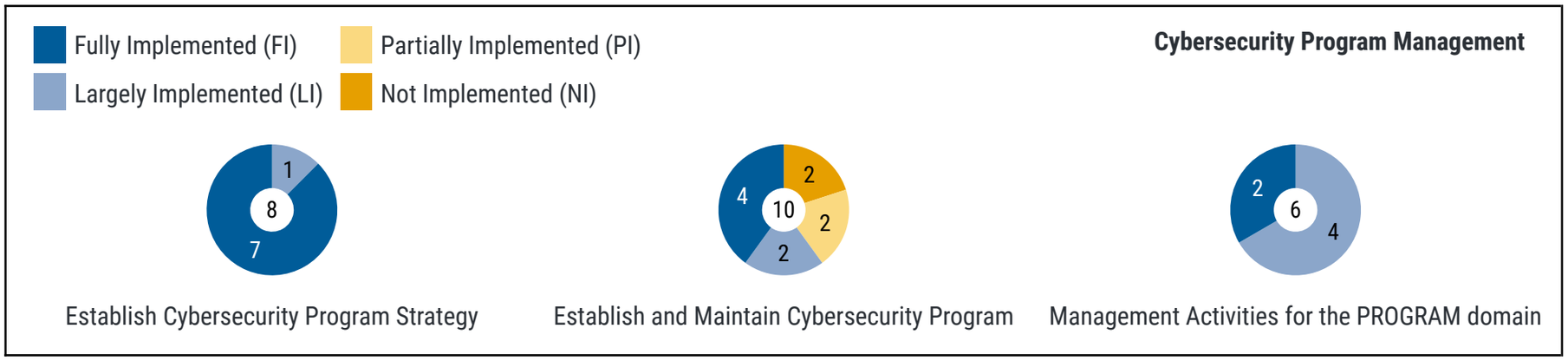
	ID	Practice Statement	Response
MIL1	ARCHITECTURE-5a	Sensitive data is protected at rest, at least in an ad hoc manner	FI
MIL2	ARCHITECTURE-5b	All data at rest is protected for selected data categories	NI
MIL2	ARCHITECTURE-5c	All data in transit is protected for selected data categories	NI
MIL2	ARCHITECTURE-5d	Cryptographic controls are implemented for data at rest and data in transit for selected data categories	NI
MIL2	ARCHITECTURE-5e	Key management infrastructure (that is, key generation, key storage, key destruction, key update, and key revocation) is implemented to support cryptographic controls	NI
MIL2	ARCHITECTURE-5f	Controls to restrict the exfiltration of data (for example, data loss prevention tools) are implemented	LI
MIL3	ARCHITECTURE-5g	The cybersecurity architecture includes protections (such as full disk encryption) for data that is stored on assets that may be lost or stolen	NI
MIL3	ARCHITECTURE-5h	The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and data	NI

Objective 6: Management Activities for the ARCHITECTURE domain

	ID	Practice Statement	Response
MIL2	ARCHITECTURE-6a	Documented procedures are established, followed, and maintained for activities in the ARCHITECTURE domain	LI
MIL2	ARCHITECTURE-6b	Adequate resources (people, funding, and tools) are provided to support activities in the ARCHITECTURE domain	FI
MIL3	ARCHITECTURE-6c	Up-to-date policies or other organizational directives define requirements for activities in the ARCHITECTURE domain	PI
MIL3	ARCHITECTURE-6d	Responsibility, accountability, and authority for the performance of activities in the ARCHITECTURE domain are assigned to personnel	FI
MIL3	ARCHITECTURE-6e	Personnel performing activities in the ARCHITECTURE domain have the skills and knowledge needed to perform their assigned responsibilities	LI
MIL3	ARCHITECTURE-6f	The effectiveness of activities in the ARCHITECTURE domain is evaluated and tracked	PI

4.10 Domain: Cybersecurity Program Management (PROGRAM)

Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with both the organization's strategic objectives and the risk to critical infrastructure.



Objective 1: Establish Cybersecurity Program Strategy

	ID	Practice Statement	Response
MIL1	PROGRAM-1a	The organization has a cybersecurity program strategy, which may be developed and managed in an ad hoc manner	FI
MIL2	PROGRAM-1b	The cybersecurity program strategy defines goals and objectives for the organization's cybersecurity activities	FI
MIL2	PROGRAM-1c	The cybersecurity program strategy and priorities are documented and aligned with the organization's mission, strategic objectives, and risk to critical infrastructure	FI
MIL2	PROGRAM-1d	The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities	FI
MIL2	PROGRAM-1e	The cybersecurity program strategy defines the structure and organization of the cybersecurity program	FI
MIL2	PROGRAM-1f	The cybersecurity program strategy identifies standards and guidelines intended to be followed by the program	FI
MIL2	PROGRAM-1g	The cybersecurity program strategy identifies any applicable compliance requirements that must be satisfied by the program (for example, NERC CIP, TSA Pipeline Security Guidelines, PCI DSS, ISO, DoD CMMC)	FI

	ID	Practice Statement	Response
MIL3	PROGRAM-1h	The cybersecurity program strategy is updated periodically and according to defined triggers, such as business changes, changes in the operating environment, and changes in the threat profile (THREAT-2e)	LI

Objective 2: Establish and Maintain Cybersecurity Program

	ID	Practice Statement	Response
MIL1	PROGRAM-2a	Senior management with proper authority provides support for the cybersecurity program, at least in an ad hoc manner	FI
MIL2	PROGRAM-2b	The cybersecurity program is established according to the cybersecurity program strategy	FI
MIL2	PROGRAM-2c	Senior management sponsorship for the cybersecurity program is visible and active	LI
MIL2	PROGRAM-2d	Senior management sponsorship is provided for the development, maintenance, and enforcement of cybersecurity policies	LI
MIL2	PROGRAM-2e	Responsibility for the cybersecurity program is assigned to a role with sufficient authority	FI
MIL2	PROGRAM-2f	Stakeholders for cybersecurity program management activities are identified and involved	PI
MIL3	PROGRAM-2g	Cybersecurity program activities are periodically reviewed to ensure that they align with the cybersecurity program strategy	PI
MIL3	PROGRAM-2h	Cybersecurity activities are independently reviewed to ensure conformance with cybersecurity policies and procedures, periodically and according to defined triggers, such as process changes	NI

	ID	Practice Statement	Response
MIL3	PROGRAM-2i	The cybersecurity program addresses and enables the achievement of legal and regulatory compliance, as appropriate	FI
MIL3	PROGRAM-2j	The organization collaborates with external entities to contribute to the development and implementation of cybersecurity standards, guidelines, leading practices, lessons learned, and emerging technologies	NI

Objective 3: Management Activities for the PROGRAM domain

	ID	Practice Statement	Response
MIL2	PROGRAM-3a	Documented procedures are established, followed, and maintained for activities in the PROGRAM domain	FI
MIL2	PROGRAM-3b	Adequate resources (people, funding, and tools) are provided to support activities in the PROGRAM domain	LI
MIL3	PROGRAM-3c	Up-to-date policies or other organizational directives define requirements for activities in the PROGRAM domain	LI
MIL3	PROGRAM-3d	Responsibility, accountability, and authority for the performance of activities in the PROGRAM domain are assigned to personnel	FI
MIL3	PROGRAM-3e	Personnel performing activities in the PROGRAM domain have the skills and knowledge needed to perform their assigned responsibilities	LI
MIL3	PROGRAM-3f	The effectiveness of activities in the PROGRAM domain is evaluated and tracked	LI

5. Using the Self-Evaluation Results

The C2M2 is meant to be used by an organization to evaluate its cybersecurity capabilities consistently, to communicate its capability levels in meaningful terms, and to inform the prioritization of its cybersecurity investments. Figure 4 summarizes a potential approach for using the model. An organization performs a self-evaluation against the model, uses that self-evaluation to identify gaps in capability, prioritizes those gaps and develops plans to address them, and finally implements plans to address the gaps. As plans are implemented, business objectives change, and the risk environment evolves, the process is repeated. This section offers a brief overview of how to use the self-evaluation results in this approach. For a more detailed review of these steps and additional guidance, see the "Using the Model" section of the C2M2 V2.1 model document available here: https://energy.gov/C2M2 .

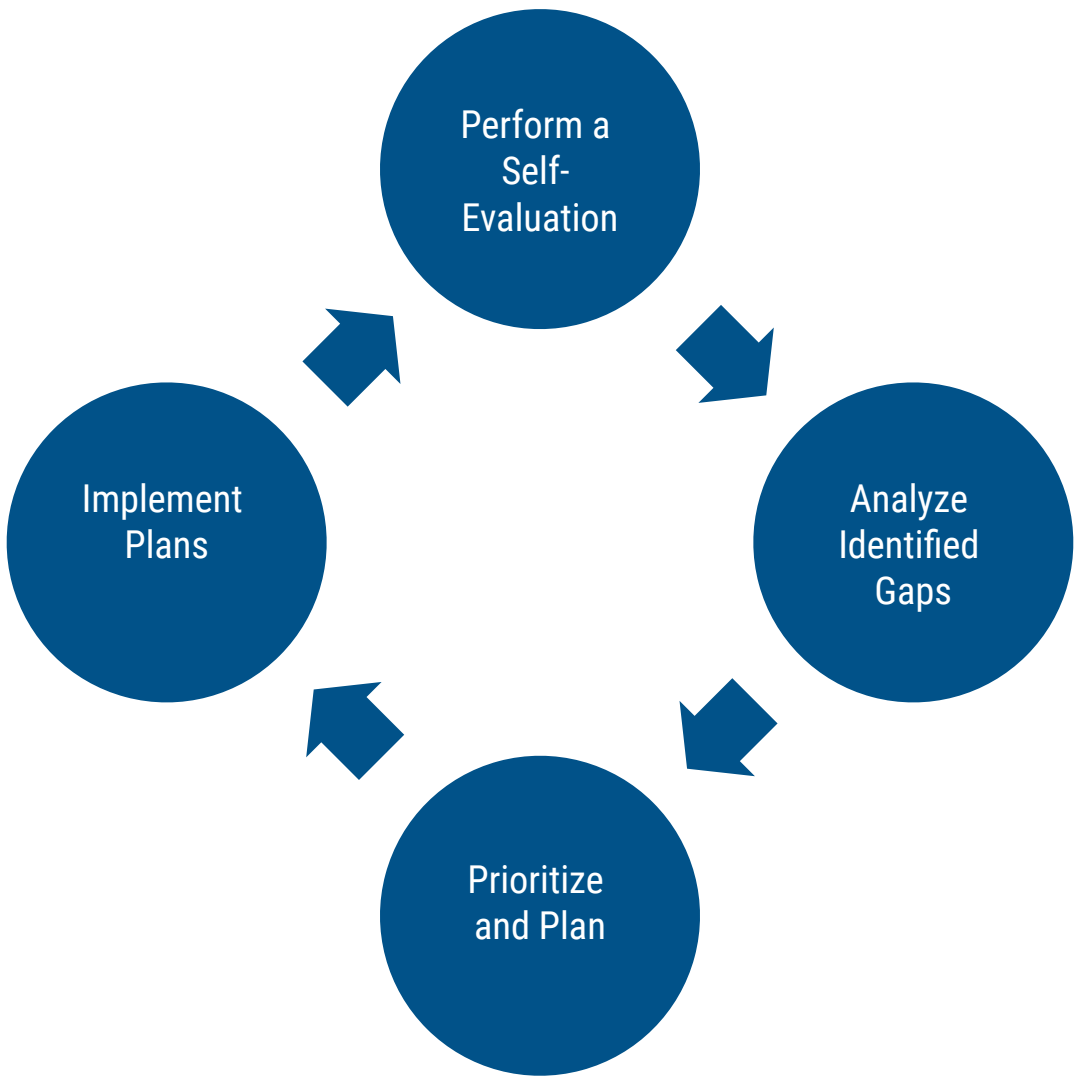


Figure 4: Proposed Approach for Using the Model

This report summarizes the results of the organization's self-evaluation conducted in Step 1, Perform a

Self-Evaluation.

It provides a point-in-time view of the cybersecurity posture of the in-scope function. Self-evaluation workshop participants should review this report and collectively address, and any discrepancies or questions before the next step.

In Step 2, Analyze Identified Gaps, the organization identifies gaps in the performance of model practices by examining the self-evaluation results against its target profile — the desired profile that represents the organization's target MIL rating for each domain in the model. Organizations using the model for the first time may identify the target profile after performing a self-evaluation, while others often identify a target profile before conducting a self-evaluation. For more information on setting targets, see Appendix D, "Setting Targets" in the C2M2 Self-Evaluation Guide available here: https://energy.gov/C2M2 .

In Step 3, Prioritize and Plan, the organization uses the gap analysis to prioritize the actions needed to fully implement the practices in the target profile. A cost-benefit analysis may help to inform the prioritization of actions needed. The organization should then develop a plan to address the selected gaps and assign ownership of the plan to an individual with sufficient authority to oversee implementation.

Regular reviews by organizational leadership should be conducted to evaluate status, clear obstacles, and identify any necessary course corrections as implementation progresses.

In Step 4, Implement Plans and Periodically Reevaluate, plans developed in the previous step should be implemented to address the identified gaps. Subsequent model self-evaluations are particularly useful in tracking implementation and should be conducted periodically to ensure that desired progress is achieved. Reevaluations should also be considered in response to major changes in business, technology, market, or threat environments to ensure that the current profile matches the organization's desired state.

6. Self-Evaluation Notes

This section lists all practices for which notes were captured during the self-evaluation, regardless of implementation status. Reviewing the notes may provide the rationale for the selection of an implementation response during the completion of the self-evaluation. The tables in this section are ordered by model practice identifier.

Domain: Asset, Change, and Configuration Management (ASSET)

ID	MIL	Practice	Response	Self-Evaluation Notes
ASSET-1a	1	IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner	Largely Implemented (LI)	Para las TI esta inventariado en CMDB En TO esta documentado con plantillas de excel
ASSET-1b	2	The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective	Partially Implemented (PI)	No existe una herramienta tecnologica que centralice todos los activos de información incluyendo los atributos de amenazas. Se encuentra parcialmente implementado para los activos de TO en excel
ASSET-1c	2	Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function	Partially Implemented (PI)	No existe una herramienta tecnologica que centralice todos los activos de tecnologia incluyendo los atributos de priorización.

Self-Evaluation Notes

ID	MIL	Practice	Response	Self-Evaluation Notes
ASSET-1d	2	Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	Partially Implemented (PI)	Se debe incluir la información asociada al nivel de vulnerabilidad de los activos de tecnología que permitan definir un criterio de priorización en su tratamiento.
ASSET-1e	2	The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, asset owner, operating system and firmware versions)	Largely Implemented (LI)	En la CMDB y en las plantillas de excel se identifican los atributos que permiten caracterizar sus propiedades
ASSET-1f	3	The IT and OT asset inventory is complete (the inventory includes all assets within the function)	Largely Implemented (LI)	Dentro del inventario actual se incluyen los activos de macroprocesos de Gestión de tecnología e información,Operación del Sistema de Transmisión y Distribución,Tecnologías de Operación.
ASSET-1g	3	The IT and OT asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes	Largely Implemented (LI)	Existen actividades programadas periodicamente para la actualización de activos de tecnología.
ASSET-1h	3	Data is destroyed or securely removed from IT and OT assets prior to redeployment	Largely Implemented (LI)	Existe un instructivo para el borrado seguro de la información, pendiente por

ID	MIL	Practice	Response	Self-Evaluation Notes
		and at end of life		adoptar en TO.
ASSET-2a	1	Information assets that are important to the delivery of the function (for example, SCADA set points and customer information) are inventoried, at least in an ad hoc manner	Largely Implemented (LI)	En la CMDB se tiene inventariado las bases de datos, pendiente por inventariar otras fuentes de información como : información administrada por un tercero o información ubicada por fuera de las instalaciones.
ASSET-4i	3	Change logs include information about modifications that impact the cybersecurity requirements of assets	Not Implemented (NI)	Incluir en el plan de implementación de cambios un apartado para registrar si las modificaciones afectan los requisitos de ciberseguridad.

Domain: Threat and Vulnerability Management (THREAT)

ID	MIL	Practice	Response	Self-Evaluation Notes
Notes were not entered for the THREAT domain. Added notes will appear in this table.				

Domain: Risk Management (RISK)

ID	MIL	Practice	Response	Self-Evaluation Notes
RISK-1b	2	A strategy for cyber risk management is established and maintained in alignment with the organization's	Largely Implemented (LI)	Pendiente por actualización

ID	MIL	Practice	Response	Self-Evaluation Notes
		cybersecurity program strategy (PROGRAM-1b) and enterprise architecture		
RISK-1c	2	The cyber risk management program is established and maintained to perform cyber risk management activities according to the cyber risk management strategy	Largely Implemented (LI)	Se encuentra en adopción la metodología en los procesos a ser intervenidos
RISK-1h	3	The cyber risk management program is coordinated with the organization's enterprise-wide risk management program	Fully Implemented (FI)	El programa de riesgos ciberneticos esta integrado con el programa de riesgos de la empresa.
RISK-2a	1	Cyber risks are identified, at least in an ad hoc manner	Fully Implemented (FI)	Disponible en el sistema de Gestión integrado
RISK-2b	2	A defined method is used to identify cyber risks	Fully Implemented (FI)	Disponible en el sistema de Gestión integrado
RISK-2i	3	Vulnerability management information from THREAT domain activities is used to update cyber risks and identify new risks (such as risks arising from vulnerabilities that pose an ongoing risk to the	Partially Implemented (PI)	La gestión de vulnerabilidades y la actualización de riesgos no estan sincronizadas.

ID	MIL	Practice	Response	Self-Evaluation Notes
		organization or newly identified vulnerabilities)		
RISK-2j	3	Threat management information from THREAT domain activities is used to update cyber risks and identify new risks	Largely Implemented (LI)	Se debe mejorar la gestión de vulnerabilidades sincronizada con la actualización de los niveles de riesgo
RISK-2k	3	Information from THIRD-PARTIES domain activities is used to update cyber risks and identify new risks	Partially Implemented (PI)	No se encuentra sincronizada la actualización de tercera partes(cti) con la actualización de niveles de riesgo.
RISK-2l	3	Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks	Not Implemented (NI)	No definido por el proceso de gestión de la información
RISK-2m	3	Cyber risk identification considers risks that may arise from or affect critical infrastructure or other interdependent organizations	Partially Implemented (PI)	Pendiente de integrar en el plan de recuperación de desastres, la necesidad de contar con la disponibilidad de otros servicios publicos
RISK-4c	3	Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to	Partially Implemented (PI)	Pendiente por adoptar una evaluación apropiada de los controles de seguridad

ID	MIL	Practice	Response	Self-Evaluation Notes
		mitigate identified cyber risks		
RISK-4d	3	Results from cyber risk impact analyses and cybersecurity control evaluations are reviewed together by enterprise leadership to determine whether cyber risks are sufficiently mitigated and risk tolerances are not exceeded	Not Implemented (NI)	No se ha definido la evaluación y revisión de la efectividad de los controles de seguridad digital con la alta dirección
RISK-5a	2	Documented procedures are established, followed, and maintained for activities in the RISK domain	Fully Implemented (FI)	La gestión documental para los procedimientos de riesgos estan disponibles en el sistema de gestión de calidad
RISK-5b	2	Adequate resources (people, funding, and tools) are provided to support activities in the RISK domain	Fully Implemented (FI)	La alta dirección esta comprometida para provisionar los recursos de este dominio

Domain: Identity and Access Management (ACCESS)

ID	MIL	Practice	Response	Self-Evaluation Notes
ACCESS-1c	1	Identities are deprovisioned, at least in an ad hoc manner, when no longer required	Largely Implemented (LI)	Se tiene implementado para el control de usuarios registrados en el directorio activos, pero para aplicaciones legadas el control es manual.
ACCESS-1d	2	Password strength and reuse	Largely	Pendiente por definir una linea

ID	MIL	Practice	Response	Self-Evaluation Notes
		restrictions are defined and enforced	Implemented (LI)	base del manejo de contraseñas para aplicaciones
ACCESS-1g	2	The use of privileged credentials is limited to processes for which they are required	Largely Implemented (LI)	Pendiente por realizar gestión de cuentas privilegiadas en aplicaciones que no estan sincronizadas con el directorio activo
ACCESS-1h	2	Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access)	Partially Implemented (PI)	No se cuenta con un mecanismo multifactor para la autenticación de cuentas privilegiadas solamente acceso por password
ACCESS-2h	3	Logical access privileges are reviewed and updated to ensure conformance with access requirements periodically and according to defined triggers, such as changes to organizational structure, and after any temporary elevation of privileges	Not Implemented (NI)	Pendiente por crear procedimiento para la gestión de privilegios por cambios de estructuras o permisos asignados
ACCESS-4b	2	Adequate resources (people, funding, and tools) are provided to support activities in the ACCESS domain	Partially Implemented (PI)	El dominio de seguridad fisica presenta debilidades en su alineación con la seguridad digital en lo que requieren las infraestructuras criticas

Domain: Situational Awareness (SITUATION)

ID	MIL	Practice	Response	Self-Evaluation Notes
SITUATION-1b	2	Logging is occurring for assets within the function that may be leveraged to achieve a threat objective, wherever feasible	Partially Implemented (PI)	Se tiene las practicas de registro de logging en los activos de información críticos.
SITUATION-1c	2	Logging requirements are established and maintained for IT and OT assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective	Partially Implemented (PI)	Se tiene las practicas de registro de logging en los activos de información críticos. Pendiente por aplicar en TO.
SITUATION-1e	2	Log data are being aggregated within the function	Partially Implemented (PI)	Se almacenan solo los logs de seguridad en un sistema de gestión de eventos e información de seguridad (SIEM) respaldado por un proveedor.
SITUATION-1f	3	More rigorous logging is performed for higher priority assets	Partially Implemented (PI)	Pendiente por implementar el doble factor de autenticación para acceso a servidores y ciberactivos críticos.
SITUATION-2c	2	Monitoring and analysis requirements are established and maintained for the function and address timely review of event data	Largely Implemented (LI)	Se realiza de manera as hoc.

Self-Evaluation Notes

ID	MIL	Practice	Response	Self-Evaluation Notes
SITUATION-2f	2	Monitoring activities are aligned with the threat profile (THREAT-2e)	Not Implemented (NI)	Los requisitos de monitoreo no se define bajo un perfil de amenazas.
SITUATION-2g	3	More rigorous monitoring is performed for higher priority assets	Not Implemented (NI)	Pendiente por establecer niveles de criticidad en los activos.
SITUATION-3b	2	Monitoring data are aggregated to provide an understanding of the operational state of the function	Fully Implemented (FI)	Este servicio es suministrado por el SOC.
SITUATION-3c	2	Relevant information from across the organization is available to enhance situational awareness	Partially Implemented (PI)	Pendiente por incluir los procesos críticos dentro de la organización.
SITUATION-3d	3	Situational awareness reporting requirements have been defined and address the timely dissemination of cybersecurity information to organization-defined stakeholders	Partially Implemented (PI)	Pendiente mejorar la gestión de comunicación a los interesados.
SITUATION-3f	3	A capability is established and maintained to aggregate, correlate, and analyze the outputs of cybersecurity monitoring activities and provide a near-real-time	Largely Implemented (LI)	Pendiente por abarcar todos los ciberactivos críticos.

ID	MIL	Practice	Response	Self-Evaluation Notes
		understanding of the cybersecurity state of the function		
SITUATION-3g	3	Predefined states of operation are documented and can be implemented based on the cybersecurity state of the function or when triggered by activities in other domains	Partially Implemented (PI)	Pendiente documentar los modelos de análisis del estado de seguridad.

Domain: Event and Incident Response, Continuity of Operations (RESPONSE)

ID	MIL	Practice	Response	Self-Evaluation Notes
RESPONSE-1e	3	Cybersecurity event detection activities are adjusted based on identified risks and the organization's threat profile (THREAT-2e)	Partially Implemented (PI)	Pendiente por definir el perfil de amenazas.
RESPONSE-1f	3	Situational awareness for the function is monitored to support the identification of cybersecurity events	Largely Implemented (LI)	La interelación de los servicios de ciberseguridad y ciberdefenza gestionados por el SOC permite la identificación de eventos de seguridad digital.
RESPONSE-2c	2	Cybersecurity incident declaration criteria are formally established based on potential impact to the	Partially Implemented (PI)	El impacto no esta totalmente definido en la organización.

ID	MIL	Practice	Response	Self-Evaluation Notes
		function		
RESPONSE-2d	2	Cybersecurity events are declared to be incidents based on established criteria	Partially Implemented (PI)	El impacto no esta totalmente definido en la organización.
RESPONSE-2e	2	Cybersecurity incident declaration criteria are updated periodically and according to defined triggers, such as organizational changes, lessons learned from plan execution, or newly identified threats	Partially Implemented (PI)	El impacto no esta totalmente definido en la organización.
RESPONSE-2g	2	Internal and external stakeholders (for example, executives, attorneys, government agencies, connected organizations, vendors, sector organizations, regulators) are identified and notified of incidents based on situational awareness reporting requirements (SITUATION-3d)	Partially Implemented (PI)	La comunicación de los incidentes de seguridad se realiza de manera ad hoc
RESPONSE-3b	1	Responses to cybersecurity incidents are executed, at least in an ad hoc manner, to limit impact to the function and restore normal operations	Partially Implemented (PI)	Pendiente mayor cobertura en escenarios de repuestas a incidentes.

Self-Evaluation Notes

ID	MIL	Practice	Response	Self-Evaluation Notes
RESPONSE-4a	1	Continuity plans are developed to sustain and restore operation of the function if a cybersecurity event or incident occurs, at least in an ad hoc manner	Partially Implemented (PI)	Pendiente por actualizar las practicas de continuidad.
RESPONSE-4c	1	IT and OT assets requiring spares are identified, at least in an ad hoc manner	Partially Implemented (PI)	Pentiente activos de respaldos en TO.
RESPONSE-4d	2	Continuity plans address potential impacts from cybersecurity incidents	Partially Implemented (PI)	Pendiente por actualizar las practicas de continuidad.
RESPONSE-4e	2	The assets and activities necessary to sustain minimum operations of the function are identified and documented in continuity plans	Partially Implemented (PI)	Pendiente por actualizar las practicas de continuidad.
RESPONSE-4f	2	Continuity plans address IT, OT, and information assets that are important to the delivery of the function, including the availability of backup data and replacement, redundant, and spare IT and OT assets	Partially Implemented (PI)	Pendiente por actualizar las practicas de continuidad.
RESPONSE-4l	2	Spares for selected IT and OT assets are available	Partially Implemented	Depende de los tiempos de entrega por parte de los

ID	MIL	Practice	Response	Self-Evaluation Notes
			(PI)	proveedores.
RESPONSE-4n	3	Continuity plan exercises address higher priority risks	Partially Implemented (PI)	Pendiente por actualizar las practicas de continuidad.
RESPONSE-5a	2	Documented procedures are established, followed, and maintained for activities in the RESPONSE domain	Partially Implemented (PI)	Pendiente por actualizar las practicas de continuidad.

Domain: Third-Party Risk Management (THIRD-PARTIES)

ID	MIL	Practice	Response	Self-Evaluation Notes
THIRD-PARTIES-1a	1	Important IT and OT third-party dependencies are identified (that is, internal and external parties on which the delivery of the function depends, including operating partners), at least in an ad hoc manner	Partially Implemented (PI)	Solamente se cuenta con la información de contactos para los servicios tercerizados que tiene la empresa
THIRD-PARTIES-1c	2	A defined method is followed to identify risks arising from suppliers and other third parties	Partially Implemented (PI)	Se tiene una propuesta para la identificación de riesgos en terceras partes y falta la adopción por parte del area responsable
THIRD-PARTIES-2f	2	Cybersecurity requirements (for example, vulnerability	Partially Implemented	Pendiente por incorporar en los acuerdos de niveles de servicio

ID	MIL	Practice	Response	Self-Evaluation Notes
		notification, incident-related SLA requirements) are formalized in agreements with suppliers and other third parties	(PI)	con los proveedores requisitos de seguridad relacionados a la confidencialidad, integridad y no repudio. Debido a que solo se tienen en cuenta SLA relacionadas a la disponibilidad del servicio.

Domain: Workforce Management (WORKFORCE)

ID	MIL	Practice	Response	Self-Evaluation Notes
WORKFORCE-1f	3	Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk	Partially Implemented (PI)	Solamente se implementa para el personal que ingresa a la organización en curso la adopción del control Validación de antecedentes para acceso al personal
WORKFORCE-2f	3	Cybersecurity awareness activities address predefined states of operation (SITUATION-3g)	Partially Implemented (PI)	La sensibilización y formación se define de manera Adhoc y no en un estado de operación
WORKFORCE-3c	2	Cybersecurity responsibilities are assigned to specific roles, including external service providers	Partially Implemented (PI)	En curso la adopción de la guia de seguridad para contrataciones.

Domain: Cybersecurity Architecture (ARCHITECTURE)

ID	MIL	Practice	Response	Self-Evaluation Notes

Self-Evaluation Notes

ID	MIL	Practice	Response	Self-Evaluation Notes
ARCHITECTURE-1b	2	A strategy for cybersecurity architecture is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture	Largely Implemented (LI)	Se debe realizar la actualización del modelo de gestión
ARCHITECTURE-1d	2	Governance for cybersecurity architecture (such as an architecture review process) is established and maintained that includes provisions for periodic architectural reviews and an exceptions process	Largely Implemented (LI)	Se debe realizar la actualización del modelo de gestión
ARCHITECTURE-1i	3	Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events	Largely Implemented (LI)	Se debe realizar la actualización del modelo de gestión

Domain: Cybersecurity Program Management (PROGRAM)

ID	MIL	Practice	Response	Self-Evaluation Notes

Self-Evaluation Notes

ID	MIL	Practice	Response	Self-Evaluation Notes
Notes were not entered for the PROGRAM domain. Added notes will appear in this table.				

7. List of Partially Implemented and Not Implemented Practices

Practices that received a response of Partially Implemented or Not Implemented are consolidated in this section and shown with any notes captured during the self-evaluation. If an organization is targeting a MIL in a specific domain, these tables will highlight the practices the organization must prioritize to achieve the target MIL.

The tables in this section are ordered first by MIL, then further ordered by the implementation response for practices at that MIL, with Partially Implemented practices followed by Not Implemented practices. This highlights the practices that may be the focus of improvement efforts to reach a MIL target in each domain.

Domain: Asset, Change, and Configuration Management (ASSET)

MIL	Response	ID	Practice	Self-Evaluation Notes
2	Partially Implemented (PI)	ASSET-1b	The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective	No existe una herramienta tecnologica que centralice todos los activos de información incluyendo los atributos de amenazas. Se encuentra parcialmente implementado para los activos de TO en excel
		ASSET-1c	Inventoried IT and OT assets are prioritized based on	No existe una herramienta tecnologica que centralice todos

MIL	Response	ID	Practice	Self-Evaluation Notes
			defined criteria that include importance to the delivery of the function	los activos de tecnologia incluyendo los atributos de priorización.
		ASSET-1d	Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	Se debe incluir la información asociada al nivel de vulnerabilidad de los activos de tecnología que permitan definir un criterio de priorización en su tratamiento.
		ASSET-2b	The information asset inventory includes information assets within the function that may be leveraged to achieve a threat objective	
		ASSET-2c	Inventoried information assets are categorized based on defined criteria that includes importance to the delivery of the function	
		ASSET-2d	Categorization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective	
		ASSET-3d	Configuration baselines are reviewed and updated periodically and according to	

MIL	Response	ID	Practice	Self-Evaluation Notes
			defined triggers, such as system changes and changes to the cybersecurity architecture	
3	Not Implemented (NI)	ASSET-4i	Change logs include information about modifications that impact the cybersecurity requirements of assets	Incluir en el plan de implementación de cambios un apartado para registrar si las modificaciones afectan los requisitos de ciberseguridad.

Domain: Threat and Vulnerability Management (THREAT)

MIL	Response	ID	Practice	Self-Evaluation Notes
2	Partially Implemented (PI)	THREAT-3b	Adequate resources (people, funding, and tools) are provided to support activities in the THREAT domain	
3	Partially Implemented (PI)	THREAT-2j	Threat monitoring and response activities leverage and trigger predefined states of operation (SITUATION-3g)	
		THREAT-3e	Personnel performing activities in the THREAT domain have the skills and knowledge needed to perform	

MIL	Response	ID	Practice	Self-Evaluation Notes
			their assigned responsibilities	

Domain: Risk Management (RISK)

MIL	Response	ID	Practice	Self-Evaluation Notes
2	Partially Implemented (PI)	RISK-3d	Defined methods are used to analyze higher-priority cyber risks (for example, analyzing the prevalence of types of attacks to estimate likelihood, using the results of controls assessments to estimate susceptibility)	
3	Partially Implemented (PI)	RISK-2i	Vulnerability management information from THREAT domain activities is used to update cyber risks and identify new risks (such as risks arising from vulnerabilities that pose an ongoing risk to the organization or newly identified vulnerabilities)	La gestión de vulnerabilidades y la actualización de riesgos no estan sincronizadas.
		RISK-2k	Information from THIRD-PARTIES domain activities is used to update cyber risks and identify new risks	No se encuentra sincronizada la actualización de tercera partes(cti) con la actualización de niveles de riesgo.
		RISK-2m	Cyber risk identification	Pendiente de integrar en el plan

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
			considers risks that may arise from or affect critical infrastructure or other interdependent organizations	de recuperación de desastres, la necesidad de contar con la disponibilidad de otros servicios publicos
		RISK-4c	Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to mitigate identified cyber risks	Pendiente por adoptar una evaluación apropiada de los controles de seguridad
	Not Implemented (NI)	RISK-2l	Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks	No definido por el proceso de gestión de la información
		RISK-4d	Results from cyber risk impact analyses and cybersecurity control evaluations are reviewed together by enterprise leadership to determine whether cyber risks are sufficiently mitigated and risk tolerances are not exceeded	No se ha definido la evaluación y revisión de la efectividad de los controles de seguridad digital con la alta dirección
		RISK-4e	Risk responses (such as mitigate, accept, avoid, or transfer) are reviewed	

MIL	Response	ID	Practice	Self-Evaluation Notes
			periodically by leadership to determine whether they are still appropriate	

Domain: Identity and Access Management (ACCESS)

MIL	Response	ID	Practice	Self-Evaluation Notes
2	Partially Implemented (PI)	ACCESS-1h	Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access)	No se cuenta con un mecanismo multifactor para la autenticación de cuentas privilegiadas solamente acceso por password
		ACCESS-2e	Logical access requirements incorporate the principle of separation of duties	
		ACCESS-2g	Logical access privileges that pose a higher risk to the function receive additional scrutiny and monitoring	
		ACCESS-3h	Physical access privileges that pose higher risk to the function receive additional scrutiny and monitoring	
		ACCESS-4b	Adequate resources (people, funding, and tools) are	El dominio de seguridad fisica presenta debilidades en su

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
			provided to support activities in the ACCESS domain	alineación con la seguridad digital en lo que requieren las infraestructuras criticas
	Not Implemented (NI)	ACCESS-3d	Physical access requirements are established and maintained (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access)	
		ACCESS-3e	Physical access requirements incorporate the principle of least privilege	
		ACCESS-3f	Physical access requirements incorporate the principle of separation of duties	
3	Not Implemented (NI)	ACCESS-2h	Logical access privileges are reviewed and updated to ensure conformance with access requirements periodically and according to defined triggers, such as changes to organizational structure, and after any temporary elevation of privileges	Pendiente por crear procedimiento para la gestión de privilegios por cambios de estructuras o permisos asignados
		ACCESS-3j	Physical access is monitored	

MIL	Response	ID	Practice	Self-Evaluation Notes
			to identify potential cybersecurity events	

Domain: Situational Awareness (SITUATION)

MIL	Response	ID	Practice	Self-Evaluation Notes
2	Partially Implemented (PI)	SITUATION-1b	Logging is occurring for assets within the function that may be leveraged to achieve a threat objective, wherever feasible	Se tiene las practicas de registro de logging en los activos de información críticos.
		SITUATION-1c	Logging requirements are established and maintained for IT and OT assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective	Se tiene las practicas de registro de logging en los activos de información críticos. Pendiente por aplicar en TO.
		SITUATION-1e	Log data are being aggregated within the function	Se almacenan solo los logs de seguridad en un sistema de gestión de eventos e información de seguridad (SIEM) respaldado por un proveedor.
		SITUATION-3c	Relevant information from across the organization is available to enhance situational awareness	Pendiente por incluir los procesos críticos dentro de la organización.
	Not	SITUATION-	Logging requirements are	

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
	Implemented (NI)	1d	established and maintained for network and host monitoring infrastructure (for example, web gateways, endpoint detection and response software, intrusion detection and prevention systems)	
		SITUATION-2f	Monitoring activities are aligned with the threat profile (THREAT-2e)	Los requisitos de monitoreo no se define bajo un perfil de amenazas.
3	Partially Implemented (PI)	SITUATION-1f	More rigorous logging is performed for higher priority assets	Pendiente por implementar el doble factor de autenticación para acceso a servidores y ciberactivos críticos.
		SITUATION-3d	Situational awareness reporting requirements have been defined and address the timely dissemination of cybersecurity information to organization-defined stakeholders	Pendiente mejorar la gestión de comunicación a los interesados.
		SITUATION-3g	Predefined states of operation are documented and can be implemented based on the cybersecurity state of the function or when triggered by activities in other domains	Pendiente documentar los modelos de análisis del estado de seguridad.

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
		SITUATION-4c	Up-to-date policies or other organizational directives define requirements for activities in the SITUATION domain	
		SITUATION-4e	Personnel performing activities in the SITUATION domain have the skills and knowledge needed to perform their assigned responsibilities	
		SITUATION-4f	The effectiveness of activities in the SITUATION domain is evaluated and tracked	
	Not Implemented (NI)	SITUATION-2g	More rigorous monitoring is performed for higher priority assets	Pendiente por establecer niveles de criticidad en los activos.

Domain: Event and Incident Response, Continuity of Operations (RESPONSE)

MIL	Response	ID	Practice	Self-Evaluation Notes
1	Partially Implemented (PI)	RESPONSE-3b	Responses to cybersecurity incidents are executed, at least in an ad hoc manner, to limit impact to the function and restore normal operations	Pendiente mayor cobertura en escenarios de repuestas a incidentes.

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
		RESPONSE-3c	Reporting of incidents is performed (for example, internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner	
		RESPONSE-4a	Continuity plans are developed to sustain and restore operation of the function if a cybersecurity event or incident occurs, at least in an ad hoc manner	Pendiente por actualizar las practicas de continuidad.
		RESPONSE-4b	Data backups are available and tested, at least in an ad hoc manner	
		RESPONSE-4c	IT and OT assets requiring spares are identified, at least in an ad hoc manner	Pentiente activos de respaldos en TO.
2	Partially Implemented (PI)	RESPONSE-2c	Cybersecurity incident declaration criteria are formally established based on potential impact to the function	El impacto no esta totalmente definido en la organización.
		RESPONSE-2d	Cybersecurity events are declared to be incidents based on established criteria	El impacto no esta totalmente definido en la organización.
		RESPONSE-2e	Cybersecurity incident declaration criteria are	El impacto no esta totalmente definido en la organización.

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
			updated periodically and according to defined triggers, such as organizational changes, lessons learned from plan execution, or newly identified threats	
		RESPONSE-2g	Internal and external stakeholders (for example, executives, attorneys, government agencies, connected organizations, vendors, sector organizations, regulators) are identified and notified of incidents based on situational awareness reporting requirements (SITUATION-3d)	La comunicación de los incidentes de seguridad se realiza de manera ad hoc
		RESPONSE-3e	Cybersecurity incident response is executed according to defined plans and procedures	
		RESPONSE-4d	Continuity plans address potential impacts from cybersecurity incidents	Pendiente por actualizar las practicas de continuidad.
		RESPONSE-4e	The assets and activities necessary to sustain minimum operations of the function are identified and documented in	Pendiente por actualizar las practicas de continuidad.

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
			continuity plans	
		RESPONSE-4f	Continuity plans address IT, OT, and information assets that are important to the delivery of the function, including the availability of backup data and replacement, redundant, and spare IT and OT assets	Pendiente por actualizar las practicas de continuidad.
		RESPONSE-4l	Spares for selected IT and OT assets are available	Depende de los tiempos de entrega por parte de los proveedores.
		RESPONSE-5a	Documented procedures are established, followed, and maintained for activities in the RESPONSE domain	Pendiente por actualizar las practicas de continuidad.
		RESPONSE-5b	Adequate resources (people, funding, and tools) are provided to support activities in the RESPONSE domain	
	Not Implemented (NI)	RESPONSE-3f	Cybersecurity incident response plans include a communications plan for internal and external stakeholders	
		RESPONSE-3g	Cybersecurity incident response plan exercises are conducted periodically and	

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
			according to defined triggers, such as system changes and external events	
		RESPONSE-4h	Cybersecurity incident criteria that trigger the execution of continuity plans are established and communicated to incident response and continuity management personnel	
		RESPONSE-4i	Continuity plans are tested through evaluations and exercises periodically and according to defined triggers, such as system changes and external events	
		RESPONSE-4j	Cybersecurity controls protecting backup data are equivalent to or more rigorous than controls protecting source data	
3	Partially Implemented (PI)	RESPONSE-1e	Cybersecurity event detection activities are adjusted based on identified risks and the organization’s threat profile (THREAT-2e)	Pendiente por definir el perfil de amenazas.
		RESPONSE-	Continuity plan exercises	Pendiente por actualizar las

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
		4n	address higher priority risks	practicas de continuidad.
		RESPONSE-5c	Up-to-date policies or other organizational directives define requirements for activities in the RESPONSE domain	
		RESPONSE-5d	Responsibility, accountability, and authority for the performance of activities in the RESPONSE domain are assigned to personnel	
		RESPONSE-5e	Personnel performing activities in the RESPONSE domain have the skills and knowledge needed to perform their assigned responsibilities	
	Not Implemented (NI)	RESPONSE-2h	Criteria for cybersecurity incident declaration are aligned with cyber risk prioritization criteria (RISK-3b)	
		RESPONSE-3i	Cybersecurity incident root-cause analysis is performed and corrective actions are taken, including updates to the incident response plan	
		RESPONSE-3k	Cybersecurity incident response personnel participate	

MIL	Response	ID	Practice	Self-Evaluation Notes
			in joint cybersecurity exercises with other organizations	
		RESPONSE-3l	Cybersecurity incident responses leverage and trigger predefined states of operation (SITUATION-3g)	
		RESPONSE-4m	Continuity plans are aligned with identified risks and the organization's threat profile (THREAT-2e) to ensure coverage of identified risk categories and threats	
		RESPONSE-4o	The results of continuity plan testing or activation are compared to recovery objectives, and plans are improved accordingly	
		RESPONSE-4p	Continuity plans are periodically reviewed and updated	
		RESPONSE-5f	The effectiveness of activities in the RESPONSE domain is evaluated and tracked	

Domain: Third-Party Risk Management (THIRD-

PARTIES)

MIL	Response	ID	Practice	Self-Evaluation Notes
1	Partially Implemented (PI)	THIRD-PARTIES-1a	Important IT and OT third-party dependencies are identified (that is, internal and external parties on which the delivery of the function depends, including operating partners), at least in an ad hoc manner	Solamente se cuenta con la información de contactos para los servicios tercerizados que tiene la empresa
	Not Implemented (NI)	THIRD-PARTIES-2a	The selection of suppliers and other third parties includes consideration of their cybersecurity qualifications, at least in an ad hoc manner	
		THIRD-PARTIES-2b	The selection of products and services includes consideration of their cybersecurity capabilities, at least in an ad hoc manner	
2	Partially Implemented (PI)	THIRD-PARTIES-1c	A defined method is followed to identify risks arising from suppliers and other third parties	Se tiene una propuesta para la identificación de riesgos en terceras partes y falta la adopción por parte del area responsable
		THIRD-PARTIES-2f	Cybersecurity requirements (for example, vulnerability notification, incident-related SLA requirements) are	Pendiente por incorporar en los acuerdos de niveles de servicio con los proveedores requisitos de seguridad relacionados a la

MIL	Response	ID	Practice	Self-Evaluation Notes
			formalized in agreements with suppliers and other third parties	confidencialidad, integridad y no repudio. Debido a que solo se tienen en cuenta SLA relacionadas a la disponibilidad del servicio.
	Not Implemented (NI)	THIRD-PARTIES-1e	Escalated prioritization is assigned to suppliers and other third parties whose compromise or disruption could cause significant consequences (for example, single-source suppliers, suppliers with privileged access)	
		THIRD-PARTIES-2c	A defined method is followed to identify cybersecurity requirements and implement associated controls that protect against the risks arising from suppliers and other third parties	
		THIRD-PARTIES-2e	More rigorous cybersecurity controls are implemented for higher priority suppliers and other third parties	
		THIRD-PARTIES-2g	Suppliers and other third parties periodically attest to their ability to meet	

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
			cybersecurity requirements	
3	Not Implemented (NI)	THIRD-PARTIES-1f	Prioritization of suppliers and other third parties is updated periodically and according to defined triggers, such as system changes and external events	
		THIRD-PARTIES-2h	Cybersecurity requirements for suppliers and other third parties include secure software and secure product development requirements where appropriate	
		THIRD-PARTIES-2j	Selection criteria include consideration of safeguards against counterfeit or compromised software, hardware, and services	
		THIRD-PARTIES-2k	Selection criteria for higher priority assets include evaluation of bills of material for key asset elements, such as hardware and software	
		THIRD-PARTIES-2l	Selection criteria for higher priority assets include evaluation of any associated third-party hosting	

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
			environments and source data	
		THIRD-PARTIES-2m	Acceptance testing of procured assets includes consideration of cybersecurity requirements	
		THIRD-PARTIES-3c	Up-to-date policies or other organizational directives define requirements for activities in the THIRD-PARTIES domain	

Domain: Workforce Management (WORKFORCE)

MIL	Response	ID	Practice	Self-Evaluation Notes
1	Partially Implemented (PI)	WORKFORCE-1b	Personnel separation procedures address cybersecurity, at least in an ad hoc manner	
2	Partially Implemented (PI)	WORKFORCE-1d	Personnel separation and transfer procedures address cybersecurity, including supplementary vetting as appropriate	
		WORKFORCE-3c	Cybersecurity responsibilities are assigned to specific roles, including external service providers	En curso la adopción de la guia de seguridad para contrataciones.

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
	Not Implemented (NI)	WORKFORCE-2c	Cybersecurity awareness objectives are aligned with the defined threat profile (THREAT-2e)	
		WORKFORCE-4d	Cybersecurity training is provided as a prerequisite to granting access to assets that are important to the delivery of the function	
3	Partially Implemented (PI)	WORKFORCE-1f	Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk	Solamente se implementa para el personal que ingresa a la organización en curso la adopción del control Validación de antecedentes para acceso al personal
		WORKFORCE-2f	Cybersecurity awareness activities address predefined states of operation (SITUATION-3g)	La sensibilización y formación se define de manera Adhoc y no en un estado de operación
		WORKFORCE-3f	Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage, including succession planning	
		WORKFORCE-4f	Training programs include continuing education and professional development	

MIL	Response	ID	Practice	Self-Evaluation Notes
			opportunities for personnel with significant cybersecurity responsibilities	

Domain: Cybersecurity Architecture (ARCHITECTURE)

MIL	Response	ID	Practice	Self-Evaluation Notes
2	Partially Implemented (PI)	ARCHITECTURE-3c	The principle of least privilege (for example, limiting administrative access for users and service accounts) is enforced	
		ARCHITECTURE-3f	Security applications are required as an element of device configuration where feasible (for example, endpoint detection and response, host-based firewalls)	
		ARCHITECTURE-3i	Maintenance and capacity management activities are performed for all assets within the function	
		ARCHITECTURE-3j	The physical operating environment is controlled to protect the operation of assets within the function	
		ARCHITECT	Secure software configurations	

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
		URE-4c	are required as part of the software deployment process for both procured software and software developed in-house	
	Not Implemented (NI)	ARCHITECT URE-3k	More rigorous cybersecurity controls are implemented for higher priority assets	
		ARCHITECT URE-5b	All data at rest is protected for selected data categories	
		ARCHITECT URE-5c	All data in transit is protected for selected data categories	
		ARCHITECT URE-5d	Cryptographic controls are implemented for data at rest and data in transit for selected data categories	
		ARCHITECT URE-5e	Key management infrastructure (that is, key generation, key storage, key destruction, key update, and key revocation) is implemented to support cryptographic controls	
3	Partially Implemented (PI)	ARCHITECT URE-2h	All assets are segmented into distinct security zones based on cybersecurity requirements	
		ARCHITECTU RE-2i	Separate networks are implemented, where	

MIL	Response	ID	Practice	Self-Evaluation Notes
			warranted, that logically or physically segment assets into security zones with independent authentication	
		ARCHITECTURE-2k	Device connections to the network are controlled to ensure that only authorized devices can connect (for example, network access control [NAC])	
		ARCHITECTURE-3l	Configuration of and changes to firmware are controlled throughout the asset lifecycle	
		ARCHITECTURE-3m	Controls (such as allowlists, blocklists, and configuration settings) are implemented to prevent the execution of unauthorized code	
		ARCHITECTURE-4d	All software developed in-house is developed using secure software development practices	
		ARCHITECTURE-4f	The architecture review process evaluates the security of new and revised applications prior to deployment	

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
		ARCHITECTURE-6c	Up-to-date policies or other organizational directives define requirements for activities in the ARCHITECTURE domain	
		ARCHITECTURE-6f	The effectiveness of activities in the ARCHITECTURE domain is evaluated and tracked	
	Not Implemented (NI)	ARCHITECTURE-5g	The cybersecurity architecture includes protections (such as full disk encryption) for data that is stored on assets that may be lost or stolen	
		ARCHITECTURE-5h	The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and data	

Domain: Cybersecurity Program Management (PROGRAM)

MIL	Response	ID	Practice	Self-Evaluation Notes
2	Partially Implemented (PI)	PROGRAM-2f	Stakeholders for cybersecurity program management activities are identified and involved	

List of Partially Implemented and Not Implemented Practices

MIL	Response	ID	Practice	Self-Evaluation Notes
3	Partially Implemented (PI)	PROGRAM-2 g	Cybersecurity program activities are periodically reviewed to ensure that they align with the cybersecurity program strategy	
	Not Implemented (NI)	PROGRAM-2 h	Cybersecurity activities are independently reviewed to ensure conformance with cybersecurity policies and procedures, periodically and according to defined triggers, such as process changes	
		PROGRAM-2 j	The organization collaborates with external entities to contribute to the development and implementation of cybersecurity standards, guidelines, leading practices, lessons learned, and emerging technologies	