Nivel de capacidades de ciberseguridad requeridos para que la Cancillería cumpla sus objetivos estratégicos

Hilda Lucy Pabón Benítez

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2018

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

"General Rafael Reyes Prieto"
Unión, Proyección, Liderazgo

NIVEL DE CAPACIDADES DE CIBERSEGURIDAD REQUERIDOS PARA QUE LA CANCILLERÍA CUMPLA SUS OBJETIVOS ESTRATÉGICOS

ALUMNO: HILDA LUCY PABÓN BENÍTEZ

DIRECTOR: MANUEL HUMBERTO SANTANDER

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2018

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

_____

Firma del jurado

Resumen: El Ministerio de Relaciones Exteriores (en adelante Cancillería), es una entidad que maneja información sensible para el Estado Colombiano, en trámites tales como Pasaportes, Visas, Apostilla, Convenios, tratados con otros países y Organismos Internacionales, con la particularidad de contar con Misiones en 160 países, con diferentes leyes y regulaciones en el manejo de la Ciberseguridad y alto riesgo en el tratamiento de esta información. De igual forma, es responsable en la contribución de estrategias de seguridad y defensa, dada la naturaleza de su misión, es responsable de la ejecución del quinto objetivo del plan nacional de seguridad digital, correspondiente a generar los mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

Así mismo, dadas las limitantes presupuestales que están atravesando actualmente las entidades del Estado, incluida la Cancillería, lo cual afecta la planeación y ejecución de los planes de acción y de acuerdo al nuevo lineamiento del Documento CONPES 3854, para el cumplimiento del mismo es de suma importancia aplicar los conocimientos y las bases de investigación en formulación de nuevos proyectos, diseñando e implementando, un esquema de Ciberdefensa, soportado en un modelo de madurez y de capacidades, que esté enfocado en la implementación y administración de políticas de Ciberseguridad, asociadas con la información de tecnologías, operaciones, activos y el entorno en que ellas operan, permitiendo a la entidad priorizar las acciones e inversiones en procura de fortalecer las capacidades de Ciberseguridad organizacional.

Abstract: The Ministry of Foreign Affairs - Cancillería, is an entity that handles sensitive information for the Colombian State, in procedures such as Passports, Visas, Apostille, Agreements, treaties with other countries and International Organizations, with the particularity of having Missions in 160 countries, with Different laws and regulations in the handling of

cybersecurity and high risk in the treatment of this information, as well as being involved in contributing to security and defense strategies given the nature of its mission, is responsible for the implementation of the fifth objective of the national plan Of digital security, corresponding to generating permanent mechanisms to foster cooperation, collaboration and assistance in digital security, at national and international level, with a strategic approach.

Likewise, given the budgetary constraints currently being faced by state entities, including the Ministry of Foreign Affairs, which affects the planning and execution of the action plans and according to the new guidelines of CONPES Document 3854, it is of relevant importance -for the compliance thereof- to apply the knowledge and research bases in the formulation of new projects, designing and implementing a Cyberdefense scheme supported by a maturity and capacity model focused on the implementation and administration of cybersecurity policies associated with information on technologies, operations, assets and the environment in which they operate, thus allowing the entity to prioritize actions and investments in order to strengthen organizational cybersecurity capabilities.

Palabras Claves: Ciberseguridad, Ciberdefensa, Conflicto Cibernético, Conciencia Situacional, Entorno Digital, Gestión de Riesgos, Derechos Fundamentales, Infraestructuras Críticas, Incidente, Amenaza, Vulnerabilidad, Capacidad, Modelo de Madurez, C2M2, NIST, MINTIC, Stakeholder, SCADA, MSPI.

Agradecimientos

Primero que todo agradecer a Dios por su iluminación y sabiduría, por guiar mis pasos y cuidar siempre de mí. A mi bella madre, por apoyarme siempre en todos mis retos, que no serían posibles sin todo su amor y apoyo, a mis amados hijos por creer siempre en mí y motivarme en el cumplimiento de mis sueños, a mi adorado papito gotica quién me ha enseñado con su amor y ejemplo, el valor y fortaleza para cumplir las metas propuestas, siempre que se hagan las cosas con amor, compromiso, responsabilidad y honestidad se lograrán los objetivos propuestos.

Igualmente quiero agradecer a Mintic y a la Esdegue por todo el compromiso y apoyo en la formación excelente que nos han impartido en esta maestría y a la Directora de Gestión de Información y Tecnología de cancillería, mi estimada y apreciada Martha Lucia Jimenez, por creer siempre en mí y apoyarme en el cumplimiento de esta maestría.

Contenido

1. Introducción

En Colombia se ha incrementado el uso de tecnologías de la información elevando su nivel de exposición a amenazas cibernéticas, con el riesgo de acceso indebido a información sensible y afectación en la prestación de servicios. Por lo anterior el Estado colombiano junto con la mesa de expertos nacionales e internacionales frente a las debilidades presentadas en el documento CONPES 3701 del Departamento Nacional de Planeación-DNP (2011) genera el nuevo documento CONPES 3854 de 2016 "Política nacional de seguridad digital".

De acuerdo con el documento CONPES 3854 (2016), el Estado colombiano cambia de enfoque al incluir la gestión de riesgos como uno de los elementos más importantes para abordar la seguridad digital, involucrando activamente a todas las partes interesadas y fortaleciendo las capacidades de las mismas. Es así que todas las entidades del Estado están llamadas a adoptar esquemas que les permitan gestionar los riesgos, igualmente es importante educar y fomentar una cultura en los ciudadanos que los haga conscientes de que el manejo del riesgo es responsabilidad de todos.

En la Política Nacional de Seguridad Digital, cuyo objetivo general es 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, se identifican cinco estratégicas, y la cancillería es responsable del numeral 5.1 en la quinta estrategia, donde se relaciona que debe cumplir con el correspondiente a: "Generar mecanismos para impulsar la cooperación, colaboración y asistencia a nivel internacional, en materia de seguridad digital". Bajo esta estrategia, se busca la adhesión de Colombia a convenios internacionales en torno a la seguridad digital, tales como la Convención de Budapest; la presencia activa de las instancias nacionales de seguridad digital en organismos, redes de intercambio y eventos internacionales; e

impulsar los trámites de firma de acuerdos de cooperación, colaboración o asistencia a nivel internacional (Departamento Nacional de Planeación, 2016).

Así mismo, de acuerdo con los objetivos estratégicos de la Cancillería que se relacionan en la siguiente tabla, es importante contar con un programa de ciberseguridad que permita identificar mecanismos para abordar los temas de ciberdelincuencia que puedan afectar el cumplimiento de los mismos.

Tabla 1
Objetivos Estratégicos de la Cancillería.

OBJETIVO	ESTRATEGIA
Diversificar la agenda de política exterior hacia sectores ejes del desarrollo nacional, fortaleciendo las relaciones bilaterales y velando por el cumplimiento de los compromisos adquiridos.	• Fortalecer las relaciones bilaterales con los socios tradicionales y no tradicionales. • Promover a Colombia como un país contemporáneo, innovador, diverso, inclusivo y comprometido con la búsqueda de la convivencia pacífica desde el Plan de Promoción de Colombia en el Exterior.
Promover y consolidar la presencia y posicionamiento de Colombia en instancias globales, multilaterales, regionales y subregionales para la defensa y promoción de los intereses nacionales.	• Promover, defender y mejorar el posicionamiento de los intereses nacionales en escenarios multilaterales, regionales y subregionales. • Establecer alianzas internacionales en relación con las políticas globales de drogas, y a la formulación de políticas que incorporen nuevos enfoques. • Difundir en los escenarios internacionales los esfuerzos que desarrolla el Estado colombiano para garantizar la protección y el respeto de los Derechos Humanos, y privilegiar el intercambio de buenas prácticas en la promoción y protección de los mismos.
Fortalecer la política migratoria, la gestión consular y el servicio al ciudadano.	• Desarrollar proyectos e iniciativas para fortalecer el Programa Colombia Nos Une. • Desarrollar iniciativas para la optimización de la asistencia a los colombianos en situación de riesgos y/o vulnerabilidad. • Fortalecer la gestión consular • Desarrollar herramientas que permitan garantizar el mejoramiento continuo del servicio al ciudadano. • Fortalecer las capacidades institucionales para enfrentar y atender de manera adecuada el crecimiento de los flujos migratorios.
Impulsar el desarrollo social y económico de las regiones de frontera, su integración con los países vecinos y velar por la soberanía territorial.	• Desarrollar un plan alineado con la estrategia de cierre de brechas y convergencia regional. • Fortalecer la operación de pasos de frontera. Construir e implementar mecanismos binacionales que permiten la ejecución de programas y proyectos transfronterizos.

	• Promover la defensa de los intereses nacionales frente a sus posibles amenazas que deriven en la vulneración de su integridad territorial o de su soberanía.
Fortalecer institucionalmente la cancillería y su Fondo Rotatorio.	• Mejorar la infraestructura física de las sedes. • Adquirir sedes y dar apertura a nuevas representaciones diplomáticas. • Implementar y mantener un modelo de gestión de las Tecnologías de la Información y la Comunicación innovador y eficaz. • Implementar mecanismos de lucha contra la corrupción, transparencia y promoción del control ciudadano.
Consolidar y orientar la oferta y la demanda de cooperación internacional en función de los objetivos de política exterior que sirvan a los intereses fundamentales del país.	• Promover y afianzar las relaciones bilaterales y fortalecer las estrategias regionales de cooperación Sur – Sur. • Posicionar a Colombia como oferente de buenas prácticas a través de la cooperación Sur–Sur.
Implementar y fortalecer herramientas y modelos que permitan mejorar la eficacia, eficiencia y efectividad del Sistema Integral de Gestión.	• Fortalecer la implementación del Sistema Integral de Gestión. • Implementar y mantener el Sistema de Seguridad y Salud en el Trabajo y el Sistema de Gestión Ambiental.
Desarrollar y fortalecer las habilidades, aptitudes y conocimientos del Talento Humano.	• Desarrollar procesos de selección, vinculación y formación integral del Talento Humano. • Promover el ingreso, la formación integral y los procesos de ascenso de los funcionarios de la Carrera Diplomática y Consular incentivando la excelencia académica. • Fortalecer la cultura organizacional y el clima laboral.

Nota. Recuperado de Planeación Estratégica Ministerio de Relaciones Exteriores y su Fondo Rotatorio, Cancillería, (2017). Recuperado de: http://www.cancilleria.gov.co/ministerio/mision_vision_objetivos_normas_principios_lineamientos#8.

Por lo anteriormente expuesto, es relevante para la Cancillería estar preparada para afrontar estos nuevos retos y compromisos establecidos frente a la política nacional de seguridad digital y el cumplimiento de sus objetivos estratégicos, es así como se entrará a revisar el contexto interno de la Cancillería en lo concerniente a:

¿Está preparada la Cancillería para identificar posibles peligros en la entidad, frente a su infraestructura y manejo de información sensible, evitarlos y saber cómo reaccionar ante alguna eventualidad, fortaleciendo a la entidad y las Misiones en el exterior en procesos y habilidades en Ciberseguridad y Ciberdefensa?, para lo cual se plantea la siguiente hipótesis, en la cual se fundamenta el desarrollo de este trabajo:

Hipótesis: A mayor nivel de capacidades de Ciberseguridad de la cancillería, se fortalecerá el cumplimiento de sus objetivos estratégicos, la imagen institucional y los vínculos con los colombianos en el exterior, en el cumplimiento de su función a nivel nacional e internacional, generando una excelente relación costo-beneficio.

Se identifica la importancia de contar con un programa de Ciberseguridad y Ciberdefensa, en el cual se contemplen las capacidades en ciberseguridad actuales de la entidad y el plan de acción que le permita alcanzar el estado deseado, en cumplimiento de su misión correspondiente a: Promover los intereses nacionales mediante el fortalecimiento y diversificación geográfica y temática de la política exterior, priorizando la cooperación internacional y el desarrollo de las fronteras y fomentando los vínculos con los colombianos en el exterior.

2. Estado del Arte

2.1 Modelos de Capacidad de Ciberseguridad.

El reciente informe del 2016, del Observatorio de la Ciberseguridad en América Latina y el Caribe, es el resultado de una gestión de colaboración entre el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), (Observatorio de la ciberseguridad en América Latina y el Caribe, 2016), así mismo, se presenta una imagen completa y actualizada del estado de la seguridad cibernética de los países de América Latina y el Caribe. A través de este documento la profesora Sadie Creese del Centro Global de Capacidad sobre Ciberseguridad Cibernética de la Universidad de Oxford, referencia que la manera en que los Estados-Nación y las regiones abordan la capacidad de seguridad cibernética es esencial para contar con una seguridad cibernética eficaz, eficiente y sostenible. Es imperativo que como comunidad internacional aboguemos por tener un enfoque integral y holístico para la construcción

de capacidad de seguridad cibernética para fomentar una economía digital segura y competitiva, y para obtener los beneficios que la participación en el ciberespacio puede aportarles a las sociedades y las personas en todas partes.

Es así que, con la ayuda de 200 expertos internacionales del gobierno, la academia, la industria y la comunidad técnica, se desarrolló un modelo para entender la madurez de las capacidades de seguridad cibernética. El Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM, por sus siglas en inglés) toma en cuenta las consideraciones de seguridad cibernética a través de cinco diferentes dimensiones de la capacidad, entendiendo que cada dimensión no es necesariamente independiente de las otras.

Las cinco dimensiones son: Políticas y estrategia nacional de seguridad cibernética; Cultura cibernética y sociedad; Educación, formación y competencias en seguridad cibernética; Marco jurídico y reglamentario; y Normas, organización y tecnologías. Cada dimensión ofrece una serie de factores e indicadores de capacidad cibernética para que una nación comprenda la etapa de madurez en cada consideración específica.

Se identificaron cinco niveles de madurez de la capacidad de seguridad cibernética, de acuerdo con los cuales el más bajo implica un grado de capacidad deficiente, y el nivel más alto indica que se eta en un nivel estratégico con una capacidad de adaptarse dinámicamente o cambiar por consideraciones ambientales (operativas, amenazas, socio-técnicas y políticas).

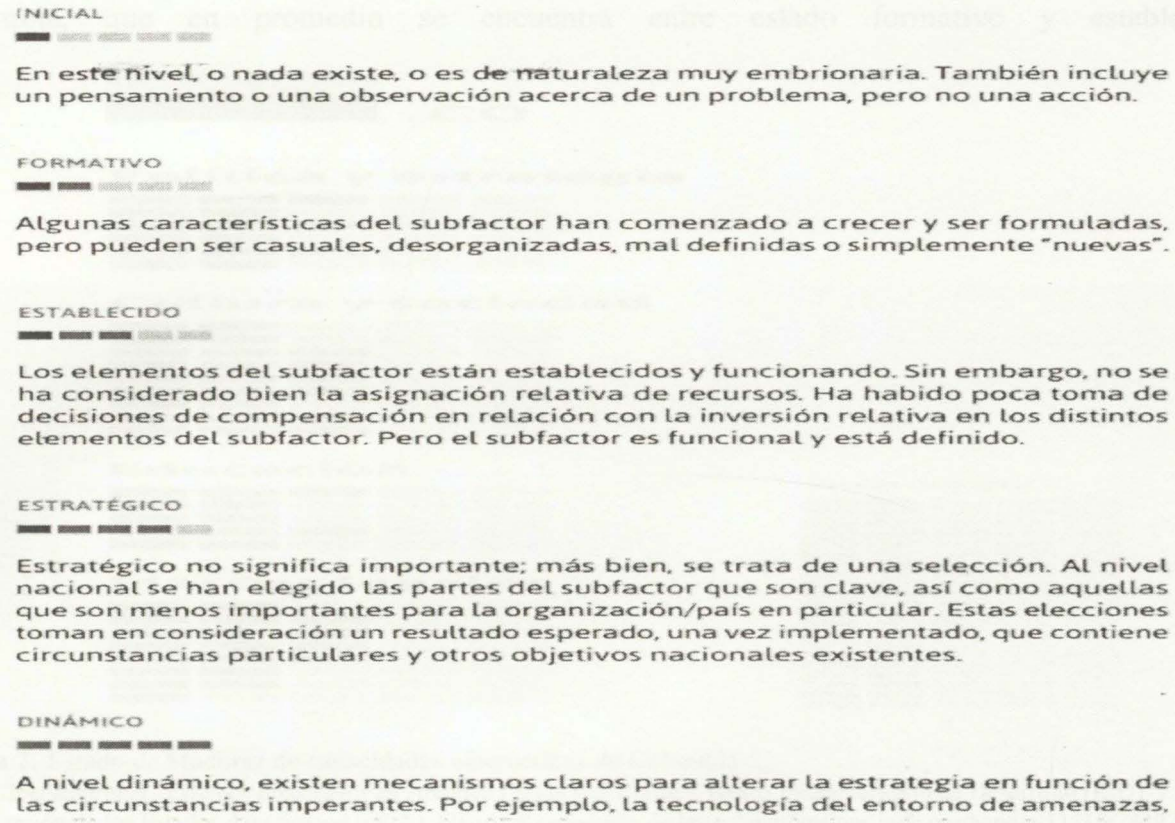


Figura 1. Niveles de Madurez de la capacidad de seguridad cibernética

Nota. Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, Banco Interamericano de Desarrollo (BID). y Organización de los Estados Americanos (OEA), (2016). Recuperado de https://publications.iadb.org/handle/11319/7449?locale-attribute=es.

En las Américas según referencia el informe en mención no es muy uniforme la madurez de sus capacidades y hay necesidad de mejoras. La siguiente gráfica muestra el estado de

Colombia, que en promedio se encuentra entre estado formativo y establecido.

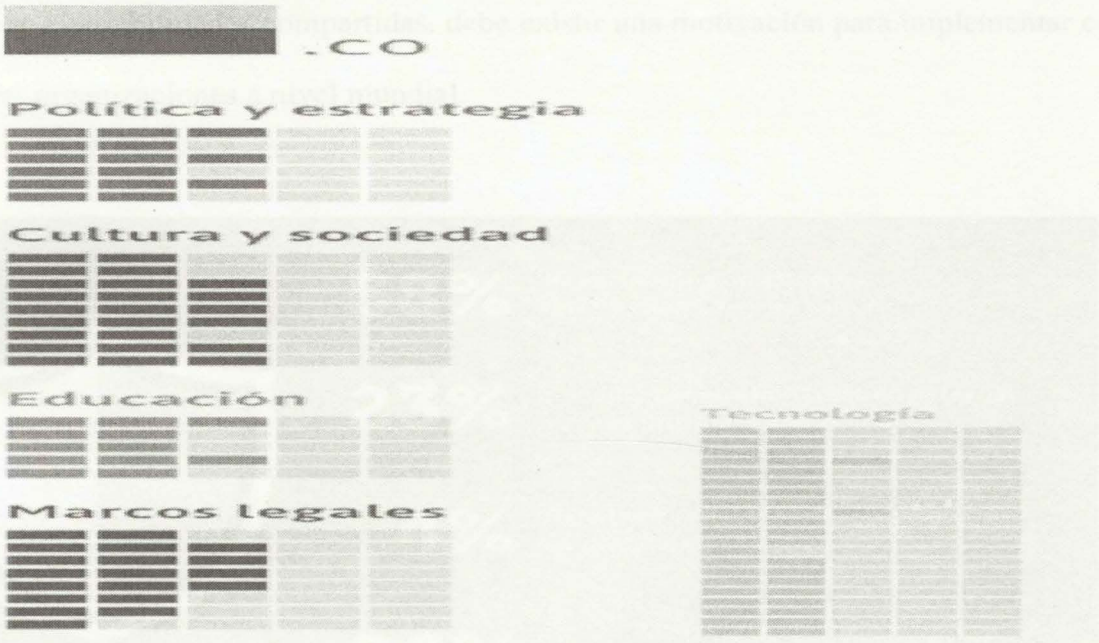


Figura 2: Estado de Madurez de capacidades cibernéticas de Colombia
Nota. Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, Banco Interamericano de Desarrollo (BID). y Organización de los Estados Americanos (OEA), (2016). Recuperado de https://publications.iadb.org/handle/11319/7449?locale-attribute=es.

Con este panorama en donde muchas organizaciones se están enfrentando a esquemas débiles de ciberseguridad, es preocupante el hecho de que la mayoría de los directivos no sabe medir el desempeño de los programas de ciberseguridad al interior de sus instituciones. Es así que Berkeley Research Group –BRG (2016) llevó a cabo, recientemente una evaluación comparativa sobre los niveles de madurez en Ciberseguridad de las empresas, titulada Cybersecurity Preparedness Benchmarking Study, en este estudio se identifica que muchas organizaciones no creen que sus programas sean eficaces, por lo cual resaltan la importancia de contar con un modelo de capacidades y madurez que les permita dimensionar el estado actual en el que se encuentran y el estado futuro deseado.

El análisis realizado por Walter Miron y Kevin Muita (2014), proporciona las etapas a seguir en un camino evolutivo, hacia el desarrollo de políticas y procesos, para la seguridad y

resiliencia de las organizaciones y teniendo en cuenta que la ciberseguridad es una prioridad mundial y de responsabilidades compartidas, debe existir una motivación para implementar estos modelos en las organizaciones a nivel mundial.

Figura 3. Estudio de Benchmarking de Preparación para la Seguridad Cibernética
Nota. *Cybersecurity Preparedness, Benchmarking study report.* Berkeley Research Group. (2016). Recuperado de http://www.thinkbrg.com/expertisecybersecurity-preparedness-benchmarkingstudy.html.

El siguiente cuadro relaciona un compendio de modelos de madurez de capacidad en ciberseguridad:

Table 2. Cybersecurity capability maturity models for critical infrastructure

Model	Publisher	Purpose
C2M2 (tinyurl.com/kvtuacm)	US Dept. of Energy	Assessment of cybersecurity capabilities for any organization comprised of a maturity model and evaluation tool
ES-C2M2 (tinyurl.com/pe62edg)	US Dept. of Energy	C2M2 tailored to energy subsector
ONG-C2M2 (tinyurl.com/mx3qzyk)	US Dept. of Energy	C2M2 tailored to the oil and natural gas subsector
NICE-CMM (tinyurl.com/m3224qv)	US Dept. of Homeland Security	Defines three areas: process and analytics, integrated governance, skilled practitioners and technology for workforce development
CERT-RMM (tinyurl.com/mp85m7y)	CERT/SEI	Defines organizational practices for operational resilience, security, and business continuity
ISO/IEC 15408 (tinyurl.com/myw3dxl)	ISO	Criteria for computer security certification
ISO/IEC 27001 (tinyurl.com/kh2t2uo)	ISO	Information Security Management System (ISMS) specification
ISO/IEC 21827 SSE-CMM (tinyurl.com/obfeup3)	ISO	Evaluation of software security engineering processes
NIST Cybersecurity Framework (tinyurl.com/kugdfug)	NIST	Framework for improving federal critical infrastructure through a set of activities designed to develop individual profiles for operators

Figura 4. Modelos de madurez de capacidad en ciberseguridad.
Nota. Cybersecurity Capability Maturity Models for Providers of Critical Infraestructure. Miron, W. y Muita, K. (2014). Recuperado de https://timreview.ca/article/837.

Modelo MSPI (Modelo de Seguridad y Privacidad de la Información)

MSPI es un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado elaborado por el Ministerio de Tecnologías de la Información y Comunicaciones - MINTIC, en el cual se contemplan entre otros, objetivos tales como:

- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Orientar a las entidades en las mejores prácticas en seguridad y privacidad.

- Optimizar la gestión de la seguridad de la información al interior de las entidades.
- Orientar a las entidades en la adopción de la legislación relacionada con la protección de datos personales.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.

El modelo consta de 6 niveles de madurez y cinco fases como se muestra en la siguiente figura:

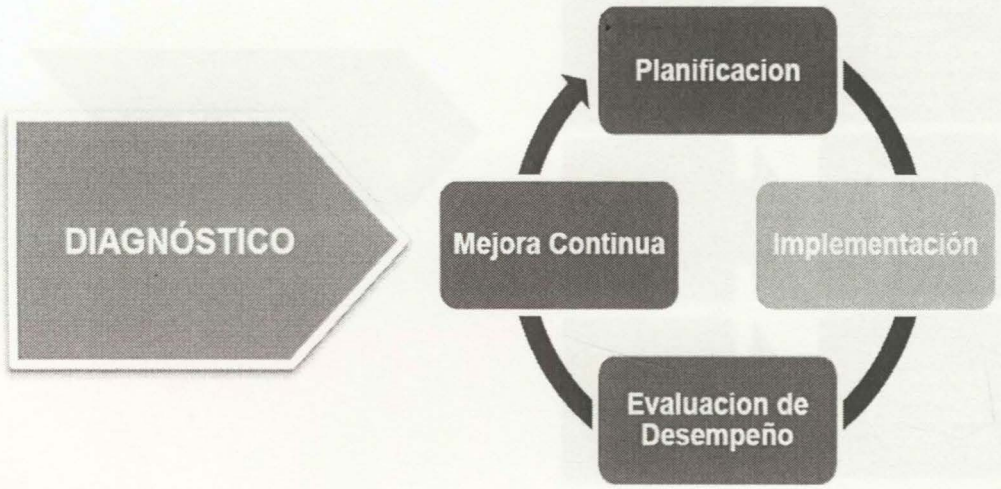


Figura 5. Fases del Modelo de Seguridad y Privacidad de la Información
Nota: Modelo de Seguridad y Privacidad de la Información - MSPI (2016). Recuperado de http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

Dentro de la fase de diagnóstico se requiere identificar el estado actual de la entidad, el nivel de madurez y realizar un levantamiento de información, para el cual se dispone de una herramienta de diagnóstico, las guías y la metodología de efectividad dispuestas para que cada entidad realice su propio levantamiento de información y se diagnostique el estado actual de la misma.

Una vez identificado el estado actual, se debe seguir con la fase de planeación, todo dentro de un esquema de mejora continua, cumpliendo con el ciclo del PHVA – Planear-Hacer-Verificar y Actuar. La fase de planeación, contempla las actividades descriptas en la siguiente figura:

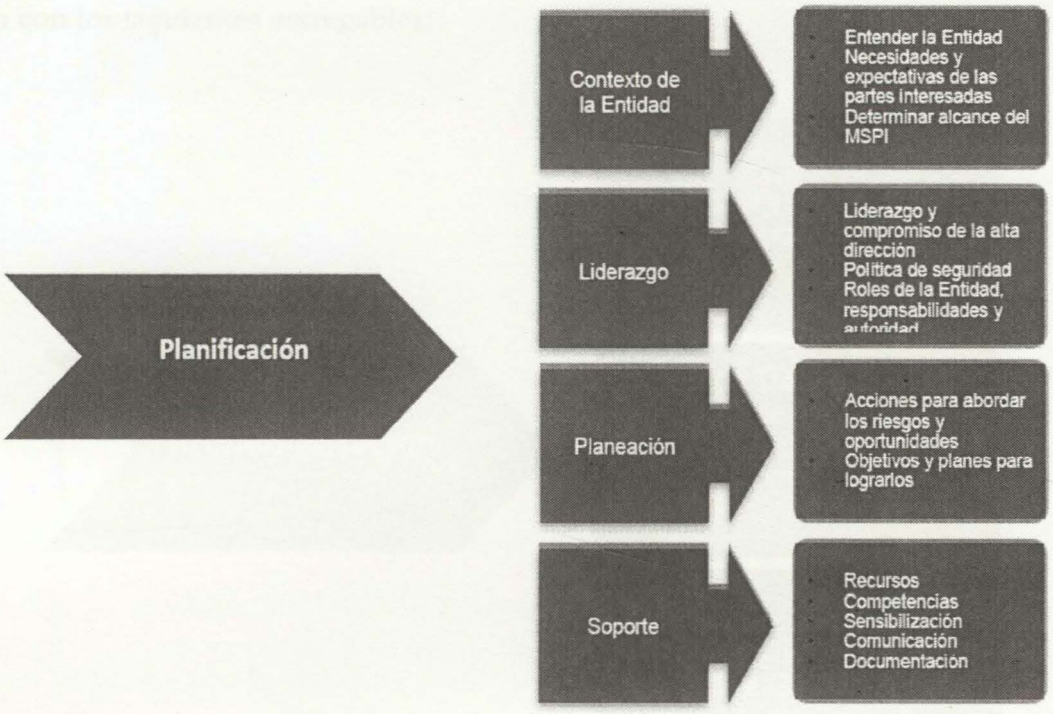


Figura 6. Fase de Planeación
Nota: Modelo de Seguridad y Privacidad de la Información - MSPI (2016). Recuperado de http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

Esta fase contempla los siguientes entregables:

- Política de seguridad y privacidad de la información.
- Políticas de Seguridad y Privacidad de la Información.
- Procedimientos de Seguridad de la Información.
- Roles y Responsabilidades de Seguridad y Privacidad de la Información.
- Inventario de activos de información.

- Integración del MSPI con el Sistema de Gestión documental.
- Identificación, Valoración Y Tratamiento de Riesgos.
- Plan de Comunicaciones.
- Plan de transición de IPv4 a IPv6.

Una vez determinados las anteriores actividades y tareas, se procede con la fase de implementación con los siguientes entregables:

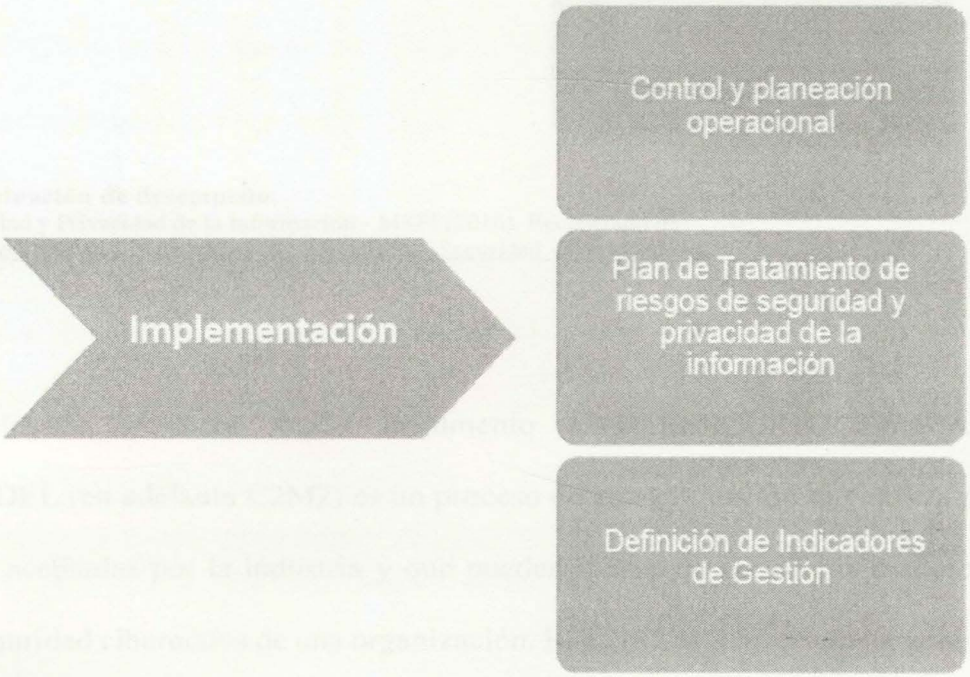


Figura 7. Fase de Implementación
Nota: Modelo de Seguridad y Privacidad de la Información - MSPI (2016). Recuperado de http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

- Planificación y Control Operacional.
- Implementación del plan de tratamiento de riesgos.
- Indicadores de Gestión.
- Plan de Transición de IPv4 a IPv6.

Por último, el modelo contempla la fase de evaluación de desempeño así:

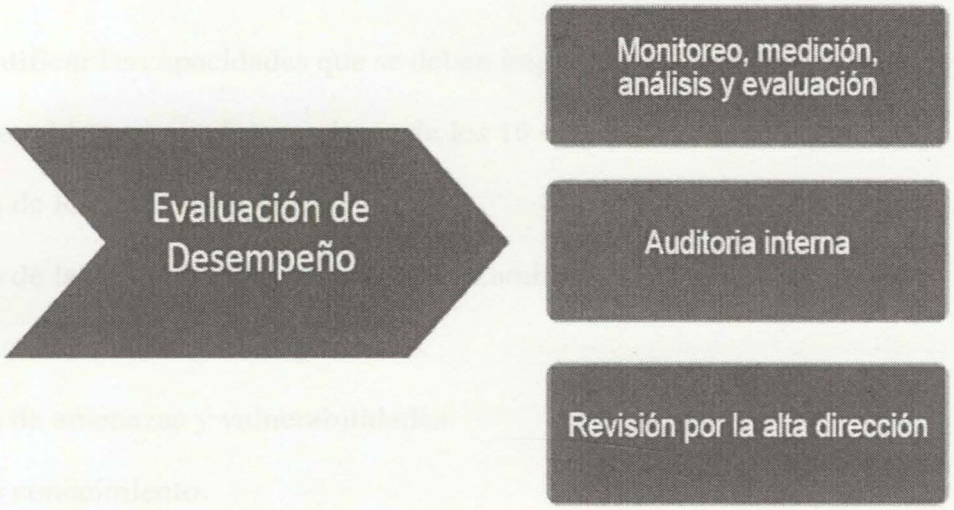


Figura 8. Fase de evaluación de desempeño.
Nota: Modelo de Seguridad y Privacidad de la Información - MSPI (2016). Recuperado de http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

Modelo C2M2

Un modelo de madurez según documento CYBERSECURITY CAPABILITY MATURITY MODEL (en adelante C2M2) es un proceso de autoevaluación que utiliza prácticas de ciberseguridad aceptadas por la industria y que pueden usarse para medir la madurez de las capacidades de seguridad cibernética de una organización. El C2M2 está diseñado para medir tanto la sofisticación como el mantenimiento de un programa de seguridad cibernética. El modelo fue identificado, organizado y documentado por expertos del sector energético de organizaciones públicas y privadas (C2M2, 2017).

Para medir el estado de madurez, se utiliza una escala de niveles de los indicadores de madurez y se entregará como base de este objetivo específico un documento que relacionará lo siguiente:

- Definición del estado actual
- Determinar el estado deseado
- Identificar las capacidades que se deben implementar para llegar al estado deseado.

El modelo establece el nivel de madurez de los 10 dominios definidos así:

1. Gestión de Riesgos
2. Gestión de la configuración y Gestión de Cambios
3. Administración de identidad y accesos
4. Gestión de amenazas y vulnerabilidades
5. Base de conocimiento
6. Protocolo de Comunicación e Información
7. Manejo de respuesta a eventos e incidentes
8. Gestión de cadena de suministro y proveedores
9. Administración de personal
10. Gestión del programa de ciberseguridad

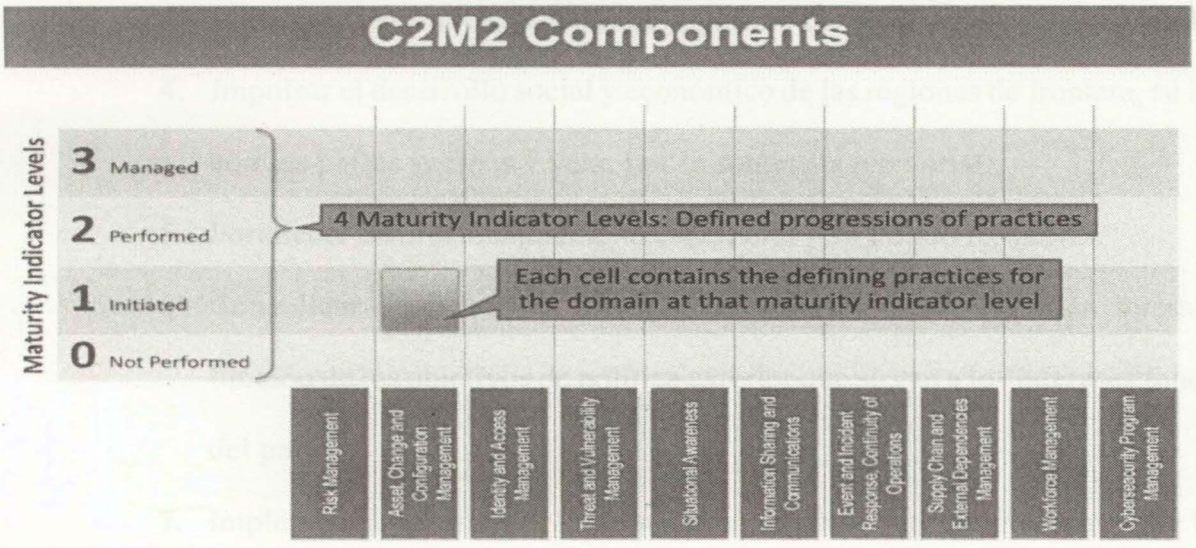


Figura 9. Componentes de evaluación de C2M2.
Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

3. Contexto actual de la cancillería en Ciberseguridad.

Teniendo en cuenta la Misión y visión de la cancillería en la cual se identifica que para el 2018, Colombia consolidará y fortalecerá las relaciones bilaterales y multilaterales, con el fin de contribuir a la paz, la equidad y la educación, y fortalecerá la relación con los connacionales a través de la prestación de un servicio eficiente y efectivo, la cancillería, en desarrollo de sus funciones y comprometido con la mejora continua de la eficacia, eficiencia y efectividad, orienta sus esfuerzos al cumplimiento de sus objetivos estratégicos así:

1. Diversificar la agenda de política exterior hacia sectores ejes del desarrollo nacional, fortaleciendo las relaciones bilaterales y velando por el cumplimiento de los compromisos adquiridos.
2. Promover y consolidar la presencia y posicionamiento de Colombia en instancias globales, multilaterales, regionales y subregionales para la defensa y promoción de los intereses nacionales.
3. Fortalecer la política migratoria, la gestión consular y el servicio al ciudadano.
4. Impulsar el desarrollo social y económico de las regiones de frontera, su integración con los países vecinos y velar por la soberanía territorial.
5. Fortalecer institucionalmente la cancillería y su Fondo Rotatorio.
6. Consolidar y orientar la oferta y la demanda de cooperación internacional en función de los objetivos de política exterior que sirvan a los intereses fundamentales del país.
7. Implementar y fortalecer herramientas y modelos que permitan mejorar la eficacia, eficiencia y efectividad del Sistema Integral de Gestión.

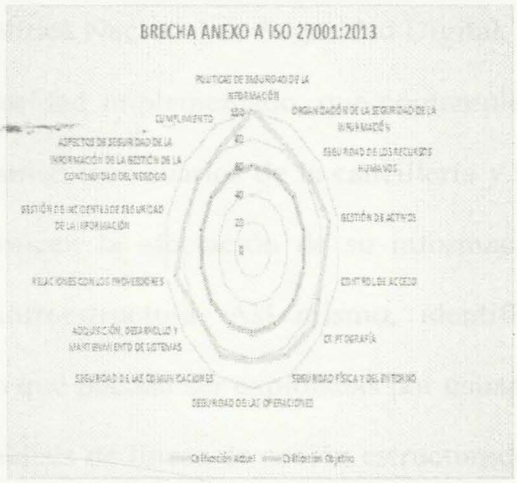
8. Desarrollar y fortalecer las habilidades, aptitudes y conocimientos del Talento Humano.

Igualmente es el responsable de cumplir con la estrategia 5.1 de la Política nacional de seguridad digital, la cual tiene como objetivo, buscar la adhesión de Colombia a convenios internacionales en torno a la seguridad digital, tales como la Convención de Budapest; la presencia activa de las instancias nacionales de seguridad digital en organismos, redes de intercambio y eventos internacionales; e impulsar los trámites de firma de acuerdos de cooperación, colaboración o asistencia a nivel internacional. Del mismo modo, es la encargada de realizar seguimiento a los temas relacionados con la seguridad digital en el ámbito bilateral, subregional, regional y multilateral, seguimiento que debe hacerse desde cada una de las dependencias internas de la entidad, en las que puedan existir temas relacionados con la seguridad digital.

El estado actual de la cancillería en el tema de ciberseguridad, esta referenciado por el modelo MSPI, en el cual se identifica un nivel de madurez entre optimizado y gestionado, con una calificación del 82.5 superior al valor de 60, correspondiente a la meta propuesta por MINTIC para las entidades del estado en exigencia al cumplimiento del año 2017, como se muestra en la siguiente figura:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	60	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	84	60	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	84	60	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	90	60	OPTIMIZADO
A.9	CONTROL DE ACCESO	81	60	OPTIMIZADO
A.10	CRIPTOGRAFÍA	90	60	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	85	60	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	80	60	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	86	60	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	78	60	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	90	60	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	80	60	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	80	60	GESTIONADO
A.18	CUMPLIMIENTO	82,5	60	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		85	60	OPTIMIZADO



AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Figura 10: Instrumento de identificación de la línea base de seguridad.
Nota. Modelo de Seguridad y Privacidad de la Cancillería. Recuperado de documentos fuente de la Cancillería.

Para la implementación del MSPI, MINTIC dispone de 21 Guías en las cuales el modelo está soportado en las buenas prácticas de la ISO 27001:2013, las cuales han sido la base fundamental para la implementación del MSPI en la entidad, las guía mencionadas se relacionan a continuación:

- Guía 1 - Metodología de pruebas de efectividad
- Guía 2 - Política General MSPI v1
- Guía 3 - Procedimiento de Seguridad de la Información
- Guía 4 - Roles y responsabilidades
- Guía 5 - Gestión Clasificación de Activos
- Guía 6 - Gestión Documental
- Guía 7 - Gestión de Riesgos
- Guía 8 - Controles de Seguridad de la Información
- Guía 9 - Indicadores Gestión de Seguridad de la Información
- Guía 10 - Continuidad de Negocio
- Guía 11 - Análisis de Impacto de Negocio
- Guía 12 - Seguridad en la Nube
- Guía 13 - Evidencia Digital (En actualización)
- Guía 14 - Plan de comunicación, sensibilización, capacitación
- Guía 15 - Auditoria
- Guía 16 - Evaluación de Desempeño
- Guía 17 - Mejora continua
- Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas
- Guía 19 - Aseguramiento de protocolo IPv4_IPv6
- Guía 20 - Transición IPv4_IPv6
- Guía 21 - Gestión de Incidentes
- Modelo de Seguridad y Privacidad

Figura 11: Guías implementación Modelo de Seguridad y Privacidad - MSPI.
Nota. Modelo de Seguridad y Privacidad de la Cancillería. Recuperado de http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html.

Es pertinente resaltar la importancia para la cancillería en cumplimiento de sus objetivos estratégicos y como responsable del numeral 5.1 de la Política Nacional de Seguridad Digital, en contar con un programa de Ciberdefensa y de Ciberseguridad implementado, que contemple la monitorización constante sobre las actividades que adelanten los usuarios de la cancillería y sus stakeholders, planeando acciones que impidan o minimicen la afectación de su información sensible, sus redes de telecomunicaciones o su infraestructura. Así mismo, identificar vulnerabilidades inherentes a las tecnologías utilizadas, o que puedan ser explotadas por usuarios internos o externos y la importancia de contar con un análisis de líneas de acción estructurado y desarrollado.

Frente a este panorama, es relevante para la cancillería identificar posibles peligros en la entidad frente a su infraestructura y manejo de la información sensible, evitarlos y saber cómo reaccionar ante alguna eventualidad, fortaleciendo a la entidad y las Misiones en el exterior en procesos y habilidades en Ciberseguridad y Ciberdefensa, por lo cual es importante hacer un análisis del modelo MSPI actual con que cuenta la entidad, frente al framework de ciberseguridad NIST Cybersecurity Framework – conocido como CSF(2017), para establecer si está cumpliendo con todas las fases requeridas del mismo.

Dado lo anterior es importante contextualizar ¿Qué es el Marco de Trabajo de Ciberseguridad del NIST-CSF?, este marco fue creado en respuesta a una orden ejecutiva del 12 de febrero de 2013, en la cual el expresidente Barack Obama, solicita desarrollar un marco voluntario de seguridad cibernética, para gestionar el riesgo de ciberseguridad.

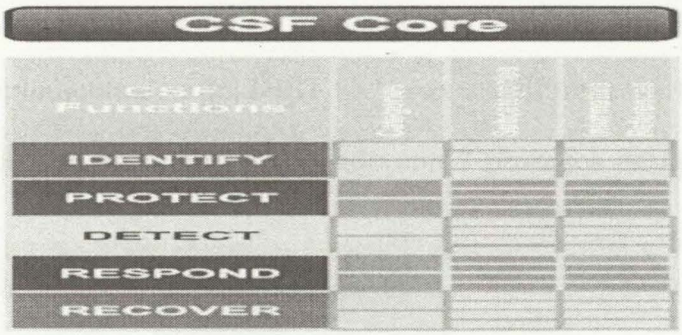


Figura 12: NIST Cybersecurity Framework –CSF.
Nota.Infrastructure Cybersecurity Draft Version 1.1. National Institute of Standards and Technology NIST. (2017) Recuperado de https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.1-with-markup1.pdf.

Dicho marco cuenta con diez dominios relacionados en la siguiente tabla:

Dominio	Descripción
Gestión de activos	**Gestión de Activos (ID.AM):** Se incluye los datos, el personal, dispositivos, sistemas y facilidades para lograr los objetivos del negocio, así como una gestión consistente en una estrategia de gestión de riesgos.
Identifiacción de la organización	**Entorno de negocio (ID.BE):** Se utiliza la información relacionada con la misión, objetivos, interesados y actividades para el entendimiento del negocio y ser utilizada en la definición de roles, responsabilidades y gestión de riesgos en ciberseguridad.
Gobierno de información	**Gobernanza(ID.GV):** Las políticas, procedimientos y procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se entienden e informan a la administración del riesgo de ciberseguridad.
Gobierno de riesgos	**Valoración de riesgos (ID.RA):** La organización entiende el riesgo de ciberseguridad para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.
	Estrategia de gestión de riesgos (ID.RM): Las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización se establecen y se usan para respaldar las decisiones de riesgos operacionales.
Gestión de acceso	**Control de acceso (PR.AC):** El acceso a los activos y las instalaciones asociadas está limitado a usuarios, procesos o dispositivos autorizados, y a actividades y transacciones autorizadas.
Capacitación, sensibilizacion y entrenamiento	**entrenamiento y concienciación (PR.AT): El personal y los socios de la organización reciben educación sobre la conciencia de la seguridad cibernética y están adecuadamente capacitados para desempeñar sus deberes y responsabilidades relacionados con la seguridad de la información de conformidad con las políticas, procedimientos y acuerdos relacionados.**
Gestión de datos y comunicaciones	**Seguridad en datos (PR.DS): La información y los registros (datos) se administran de manera coherente con la estrategia de riesgos de la organización para proteger la confidencialidad, la integridad y la disponibilidad de la información.**
Continuidad de negocio	**Procesos y procedimientos de protección de información (PR.IP): Las políticas de seguridad (que abordan el propósito, el alcance, las funciones, las responsabilidades, el compromiso de la administración y la coordinación entre las entidades de la organización), los procesos y procedimientos se mantienen y utilizan para administrar la protección de los sistemas de información y los activos.**
	Mantenimiento (PR.MA): El mantenimiento y la reparación de los componentes del sistema de control e información industrial se realiza de acuerdo con las políticas y procedimientos.

Figura 13: Instrumento de identificación de la línea base de seguridad.
Nota. Modelo de Seguridad y Privacidad de la Cancillería. Recuperado de https://www.nist.gov/cybersecurity-framework.

En enero de 2015 el Departamento de Energía (en adelante DoE) de Estados Unidos, publicó una guía para la implementación del NIST Cybersecurity Framework, herramienta que se denominó C2M2, la cual provee un estándar alineado con 7 procesos en la implementación del CSF, así:

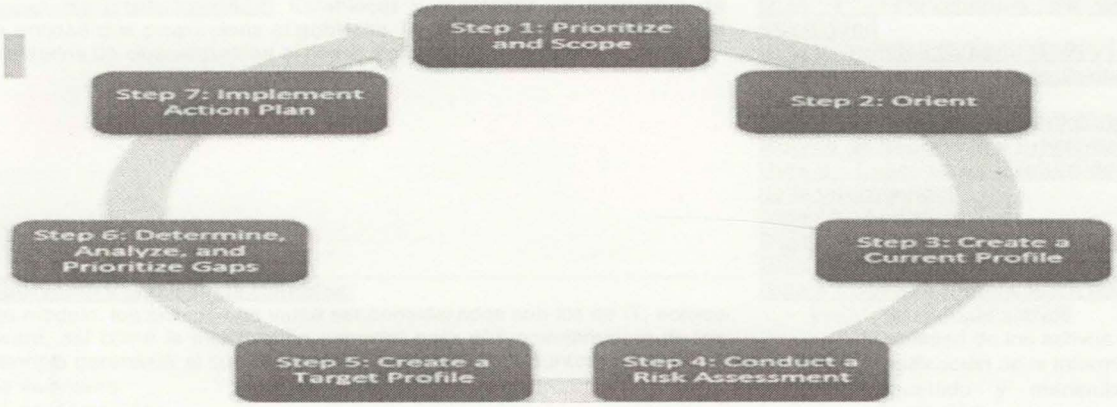


Figura 14. Procesos para la implementación del CSF (NIST Cybersecurity Framework).
Nota. Infrastructure Cybersecurity Draft Version 1.1. National Institute of Standards and Technology NIST. (2017) Recuperado de https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.1-with-markup1.pdf.

Según fuente de SIGP- Smart Grid Inter Operability, en el panel de junio 18 de 2016, recomiendan el uso de C2M2 para implementar el marco del NIST, ya que es de uso extendido para cualquier tipo de industria, es un modelo de madurez genérico, el cual es aplicable a la cancillería y adicionalmente cuenta con un kit de herramientas de autoevaluación.

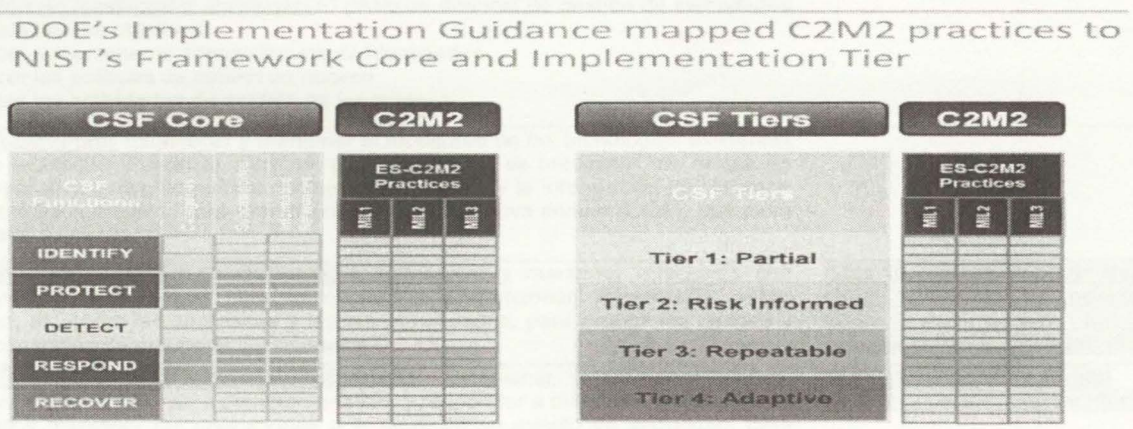


Figura 15. Mapeo del NIST-CSF y C2M2.
Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

Por lo cual nos centraremos en evaluar los vacíos que presenta el modelo MSPI frente al modelo C2M2, para estar completamente alineado con el framework de ciberseguridad CSF.

Tabla 2

Comparación modelo MSPI frente al modelo C2M2.

C2M2	MSPI
Gestión del programa de ciberseguridad: Establecer y mantener un programa de ciberseguridad de la entidad que proporciona el gobierno, la planificación estratégica, y el patrocinio de las actividades de ciberseguridad alineada con los objetivos estratégicos.	**Guía 1 - Metodología de pruebas de efectividad** **Guía 2 - Política General MSPI v1** **Guía 3 - Procedimiento de Seguridad de la Información** **Guía 4 - Roles y responsabilidades** **Modelo de Seguridad y Privacidad** **Guía 9 - Indicadores Gestión de Seguridad de la Información.** **Guía 15 - Auditoria** **Guía 16 - Evaluación de Desempeño** **Guía 17 - Mejora continua**
Gestión de la configuración y Gestión de Cambios: Para los fines de este modelo, los activos que van a ser considerados son los de IT, activos de hardware y software, así como la información esencial para el funcionamiento de los mismos, lo cual contempla garantizar el cumplimiento de los siguientes puntos: • Gestión de inventario • Gestión de configuración • Gestión de Cambios.	**Guía 5 - Gestión Clasificación de Activos** • Inventario de activos • Propiedad de los activos • Clasificación de la información • Etiquetado y manipulado de la información.
	Guía 6 - Gestión Documental
Gestión de Riesgos: Establecer, operar y mantener un programa de gestión de riesgos de ciberseguridad de la entidad que permita identificar, analizar y mitigar los riesgos, incluyendo sus áreas, sedes, misiones en el exterior, relacionadas con la infraestructura interconectada, y los servicios de información prestados a los ciudadanos en general. Para este objetivo específico con base en la arquitectura de red que identifica los elementos críticos y cómo están conectados y cuáles están expuestos a altos riesgos de ser comprometidos, se elaborará una matriz de riesgos, que permita establecer de acuerdo a unos niveles definidos, el plan de tratamiento al riesgo.	**Guía 7 - Gestión de Riesgos** • Proceso. • Objetivo del Proceso. • Identificación de Activos. • Riesgo. • **Causas (Amenazas y Vulnerabilidades).** • Descripción del Riesgo. • Efectos de la materialización del Riesgo.
Gestión de amenazas y vulnerabilidades: Establecer y mantener planes, procedimientos y tecnologías para detectar, identificar, analizar, gestionar y responder a las amenazas de ciberseguridad y vulnerabilidades asociadas con el riesgo de la infraestructura de la organización.	**Guía 8 - Controles de Seguridad de la Información**
Administración de identidad y accesos: El (IAM) de dominio de gestión de identidades y acceso consta de tres objetivos: 1. Establecer y mantener la administración de identidades 2. Establecer las políticas de control de acceso **3.** Establecer las actividades de gestión de las mismas.	
Base de conocimiento: Establecer y mantener el monitoreo de las tecnologías existentes que permitan recolectar y analizar alarmas, o umbrales que se presenten, en el uso de información operativa y ciberseguridad, incluyendo el estado y la información de resumen de los otros dominios modelo, para formar una imagen operativa común (COP), que sirva como línea base.	
Protocolo de Comunicación e Información: Establecer y mantener relaciones con entidades internas y externas para recolectar y proporcionar información sobre ciberseguridad, así como las amenazas y las vulnerabilidades, para reducir los riesgos y aumentar la capacidad de recuperación operativa.	**Guía 10 - Continuidad de Negocio** **Guía 11 - Análisis de Impacto de Negocio** **Guía 14 - Plan de comunicación, sensibilización, capacitación.**
Manejo de respuesta a eventos e incidentes: Establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a eventos e incidentes de ciberseguridad y mantener las operaciones a lo largo de un evento de seguridad, para garantizar la disponibilidad de los servicios y la resiliencia de la entidad.	**Guía 13 - Evidencia Digital** **Guía 21 - Gestión de Incidentes**
Gestión de cadena de suministro y proveedores: Establecer y mantener controles para gestionar los riesgos asociados a la ciberseguridad, servicios y activos que son dependientes de entidades externas, acorde con el riesgo a la infraestructura crítica y objetivos de la entidad.	**Guía 12 - Seguridad en la Nube**

Administración de personal: Establecer y mantener los planes, procedimientos, tecnologías y controles para crear una cultura de ciberseguridad y para asegurar la competencia del personal, en cumplimiento de los objetivos de la entidad.	
	Guía 19 - Aseguramiento de protocolo IPv4 IPv6.

Nota. Recuperado de http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html, https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

Dado lo anterior se identifican unos vacíos del modelo MSPI versus el modelo C2M2, como se resumen a continuación:

Tabla 3

Vacíos modelo MSPI frente al modelo C2M2

Gestión de la configuración y Gestión de Cambios: Para los fines de este modelo, los activos que van a ser considerados son los de IT, activos de hardware y software, así como la información esencial para el funcionamiento de los mismos, lo cual contempla garantizar el cumplimiento de los siguientes puntos: • Gestión de configuración • Gestión de Cambios.
Administración de identidad y accesos: El (IAM) de dominio de gestión de identidades y acceso consta de tres objetivos: 4. Establecer y mantener la administración de identidades 5. Establecer las políticas de control de acceso **6.** Establecer las actividades de gestión de las mismas.
Base de conocimiento: Establecer y mantener el monitoreo de las tecnologías existentes que permitan recolectar y analizar alarmas, o umbrales que se presenten, en el uso de información operativa y ciberseguridad, incluyendo el estado y la información de resumen de los otros dominios modelo, para formar una imagen operativa común (COP), que sirva como línea base.
Protocolo de Comunicación e Información: Establecer y mantener relaciones con entidades internas y externas para recolectar y proporcionar información sobre ciberseguridad, así como las amenazas y las vulnerabilidades, para reducir los riesgos y aumentar la capacidad de recuperación operativa.
Gestión de cadena de suministro y proveedores: Establecer y mantener controles para gestionar los riesgos asociados a la ciberseguridad, servicios y activos que son dependientes de entidades externas, acorde con el riesgo a la infraestructura crítica y objetivos de la entidad.
Administración de personal: Establecer y mantener los planes, procedimientos, tecnologías y controles para crear una cultura de ciberseguridad y para asegurar la competencia del personal, en cumplimiento de los objetivos de la entidad.

Nota.: Vacíos del modelo MSPI frente al Framework de ciberseguridad CSF- C2M2

Es así que establecer el nivel de madurez de los 10 dominios definidos por el modelo C2M2 le permitirá al Ministerio de Relaciones Exteriores complementar de manera adicional al modelo MSPI, gestionando la ciberseguridad, cumpliendo con los estándares internacionales de la NIST, alineada al framework de ciberseguridad CSF.

4. Modelo de madurez y capacidades C2M2

4.1 Alcance del modelo

Teniendo en cuenta el análisis realizado en el numeral 3. Discusión, donde se sustenta porqué el modelo C2M2 es el adecuado para la evaluación del programa de Ciberseguridad y Ciberdefensa de la cancillería, se entrará a profundizar el desarrollo del mismo.

El Departamento de Energía de los Estados Unidos-DOE, desarrolló el C2M2 Versión 1.1, con base en el modelo de madurez de capacidad de ciberseguridad del subsector de electricidad (ES-C2M2) Versión 1.0, eliminando referencias y terminología específicas del sector de la electricidad. El ES-C2M2 fue desarrollado en apoyo de una iniciativa de la Casa Blanca dirigida por el DOE, en colaboración con el Departamento de Seguridad Nacional (DHS), y en colaboración con expertos del sector público y privado (DOE, 2017).

Así mismo el DOE reconoce la dedicación y la experiencia técnica de todas las organizaciones e individuos que participaron en el desarrollo de ES-C2M2, así como de las organizaciones e individuos de diferentes sectores que han proporcionado las críticas, evaluaciones y modificaciones para producir la versión 1.1. del C2M2.

Este proyecto está enfocado en utilizar está versión del modelo C2M2, para aplicarla a la cancillería, de acuerdo con el nivel actual de madurez en el que se encuentre la entidad, es así como a continuación vamos a profundizar en el alcance del modelo.

Este documento permite a las organizaciones de todos los sectores, tipos y tamaños mejorar sus programas de ciberseguridad, si es cierto que el modelo hace énfasis para aplicarlo a infraestructuras críticas, también puede ser utilizado en organizaciones de diferentes tipos que quieran medir su estado actual de ciberseguridad y basado en este, plantear una estrategia para definir el plan de ciberseguridad alineado a los objetivos estratégicos de las organizaciones.

El modelo surge de una combinación de normas, marcos, programas e iniciativas de ciberseguridad existentes y proporciona una guía flexible para ayudar a las organizaciones a desarrollar y mejorar sus capacidades de ciberseguridad, como resultado, las prácticas tienden a estar en un alto nivel de abstracción, por lo que pueden ser interpretadas por organizaciones de diferentes estructuras y tamaños. Así mismo, está organizado en 10 dominios y cada dominio es una agrupación lógica de prácticas de ciberseguridad, las cuales se agrupan en dominios mediante logros de objetivo que soportan el dominio. Dentro de cada objetivo, las prácticas son ordenadas por niveles de indicadores de madurez (MILs), que van del 0 al 3 (DOE, 2017).

Cada uno de los 10 dominios del modelo contiene un conjunto estructurado de prácticas de ciberseguridad y cada conjunto de prácticas representa las actividades que una organización puede implementar de acuerdo con su nivel deseado de capacidades, igualmente proporciona una declaración de propósito, que es un resumen de alto nivel de la intención del dominio, seguido de notas introductorias, que dan contexto al dominio e introducen sus prácticas.

El enfoque recomendado para el uso del modelo es primero realizar una evaluación para identificar brechas en las capacidades actuales, luego se deben priorizar estas brechas y desarrollar un plan de acción que permita abordar estas brechas para llegar al estado de madurez deseado por la organización (DOE, 2017). A medida que se implementan los planes de acción, los objetivos estratégicos en las organizaciones pueden ir cambiando en el tiempo y así mismo el entorno de riesgo evolucionar, es por eso por lo que el enfoque del modelo es un proceso cíclico, como se muestra en la siguiente figura:

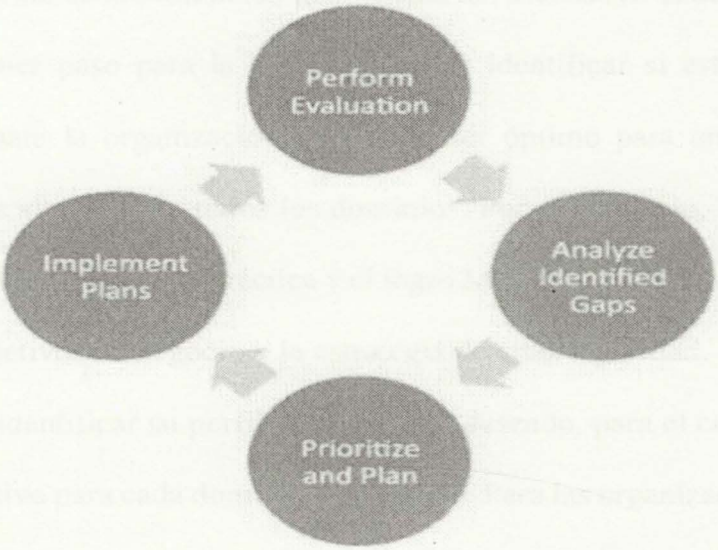


Figura 16. Enfoque recomendado para usar el modelo
Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

Primera Fase: Una de las metas del modelo es permitir a las organizaciones realizar una autoevaluación a través de una herramienta de evaluación y un mecanismo de medición establecido. La autoevaluación se realiza en forma de taller y liderada por un facilitador, en este taller deben participar, representantes de todas las partes interesadas y en términos generales, un facilitador de C2M2 no sólo es alguien que está familiarizado con el modelo y sus artefactos de apoyo, sino también alguien que es eficaz para ayudar a las partes interesadas a comprender sus objetivos comunes y guiarlos en la planificación de sus objetivos sin tomar una posición particular en la toma de decisiones.

El personal seleccionado para participar en la evaluación debe incluir al personal operativo, las partes interesadas en la gestión y cualquier otro que pueda proporcionar información útil sobre el desempeño de la organización en las prácticas de ciberseguridad en el modelo, una vez completada la evaluación, se genera un informe de puntuación que muestra los resultados del nivel del indicador de madurez para cada dominio.

Segunda Fase: El informe de la evaluación identificará las brechas en el desempeño de las prácticas del modelo. El primer paso para la organización es identificar si estas brechas son significativas e importantes para la organización. No suele ser óptimo para una organización esforzarse por alcanzar la más alta MIL en todos los dominios. Por el contrario, la organización debe determinar el nivel de rendimiento de la práctica y el logro MIL para cada dominio que mejor le permita cumplir con sus objetivos de negocio y la estrategia de ciberseguridad.

La organización debe identificar su perfil de capacidad deseado, para el cual se identifica una clasificación de MIL objetivo para cada dominio del modelo. Para las organizaciones que usan el modelo por primera vez, normalmente se identifica un perfil de capacidad deseado después de la evaluación inicial. Esto da a la organización la oportunidad de adquirir destreza en la implementación del modelo. Las organizaciones que tienen más experiencia con el modelo a menudo han identificado un perfil de capacidad objetivo antes de someterse a una evaluación.

Tercera Fase: Una vez se ha finalizado el análisis de la brecha, la entidad puede priorizar cuáles son las acciones necesarias que debe implementar para alcanzar la capacidad en ciberseguridad deseada, en dominios específicos. La priorización debe hacerse teniendo en cuenta las brechas que afectan los objetivos estratégicos de la organización y el costo-beneficio en la implementación. Luego se debe establecer un plan de acción para la implementación de las mismas. La ejecución de estos planes debe identificar los tiempos requeridos, los cuales pueden ser a corto, mediano o largo plazo.

Cuarta fase: Los planes desarrollados en la fase anterior deben implementarse para minimizar las brechas identificadas. Las evaluaciones de modelos son particularmente útiles en el seguimiento de las implementaciones y deben llevarse a cabo periódicamente para asegurar que se logre el progreso deseado, dentro de un proceso de mejora continua, que contemple cambios

importantes en los entornos de negocios, tecnología, o amenazas, que permita alcanzar y mantener el estado deseado en ciberseguridad de la organización.

La siguiente figura muestra un resumen de las fases de implementación del modelo:

	Inputs ➡	Activities ➡	Outputs
Perform Evaluation ⬇	1. C2M2 Self-Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct C2M2 Self-Evaluation Workshop with appropriate attendees	C2M2 Self-Evaluation Report
Analyze Identified Gaps ⬇	1. C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan ⬇	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Cost-benefit analysis (CBA) on actions 3. Prioritize actions (CBA and consequences) 4. Plan to implement prioritize actions	Prioritized implementation plan
Implement Plans	1. Prioritized implementation plan	1. Track progress to plan 2. Reevaluate periodically or in response to major change	Project tracking data

Figura 17. Resumen fases modelo C2M2
Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

4.2 Dominios del modelo

Los diez dominios que se expondrán a continuación responden a los postulados del documento C2M2 del DOE (2017).

4.2.1 Administración del riesgo (RM)

Este dominio tiene como propósito identificar, analizar y mitigar el riesgo de ciberseguridad para la organización, incluyendo sus unidades de negocio, subsidiarias, infraestructura interconectada relacionada y partes interesadas. El riesgo en ciberseguridad se define como un riesgo para las operaciones de la organización (incluida la misión, las funciones,

la imagen y la reputación), los recursos y otras organizaciones debido al potencial de acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de información.

El riesgo en ciberseguridad es uno de los componentes del entorno global de riesgos empresariales y se introduce en la estrategia y el programa de gestión de riesgos empresarial de una organización, no puede eliminarse por completo, pero puede ser mitigado de acuerdo con una estrategia de tratamiento del riesgo.

La estrategia de gestión del riesgo de ciberseguridad corresponde a una estrategia de alto nivel, la cual proporciona orientación para analizar y priorizar este riesgo y permite definir la tolerancia al mismo. Esta estrategia incluye una metodología de evaluación del riesgo, monitoreo y un programa de gobernabilidad de la ciberseguridad.

Se deben tener en cuenta los criterios de riesgo de la organización tales como, umbrales de impacto y enfoques de respuesta al mismo. La estrategia de gestión de riesgos de ciberseguridad debe estar alineada con la estrategia de gestión de riesgos de la organización, garantizando así que los riesgos de ciberseguridad se les formule un plan de tratamiento a esta problemática que esté alineado con la misión de la organización y sus objetivos estratégicos. A continuación, en la Tabla No. 2, se relacionan las actividades de los objetivos de este dominio, identificando el nivel MIL en el que se encuentran:

Tabla 4.

Actividades administración del riesgo.

OBJETIVO 1	**Establecer una estrategia de administración del riesgo.**
MIL1	• No existe.
MIL2	• Existe un documento de administración del riesgo. • La estrategia contiene un enfoque de priorización del riesgo que incluye el impacto.
MIL3	• Define criterios de riesgo organizacional y de disponibilidad.
OBJETIVO 2	**Administrar riesgos de ciberseguridad.**
MIL1	• Los riesgos de ciberseguridad son identificados. • Se hace tratamiento al riesgo.
MIL2	• El aseguramiento al riesgo es ejecutado.

	• Los riesgos identificados son documentados. • Los riesgos son analizados, priorizados y existe una estrategia de tratamiento al riesgo. • Los riesgos identificados son monitoreados de acuerdo con la estrategia al riesgo definida. • El análisis del riesgo es informado.
MIL3	• El programa de administración del riesgo es definido, operado, existen políticas y procedimientos para implementar la estrategia de administración al riesgo. • La arquitectura de ciberseguridad es usada para informar el análisis al riesgo. • Un registro de riesgos es usado para soportar las actividades de administración al riesgo.
OBJETIVO 3	**Actividades de administración**
MIL1	• No hay práctica.
MIL2	• Se siguen prácticas documentadas para las actividades de gestión de riesgos. • Las actividades de gestión de riesgos para los stakeholders son identificadas y tenidas en cuenta. • Se cuenta con los recursos necesarios tales como (personas, presupuesto y herramientas) para apoyar las actividades de gestión de riesgos.
MIL3	• Las actividades de gestión de riesgos están soportadas por políticas documentadas u otras directivas organizativas. • Las políticas de gestión de riesgos incluyen los requisitos de cumplimiento tales como normas y/o directrices especificadas. • Las actividades de gestión de riesgos se revisan periódicamente para garantizar el cumplimiento de la política. • Están definidos los roles y responsabilidades para la gestión de riesgos. • El personal que realiza las actividades de gestión de riesgos tiene las habilidades y conocimientos necesarios para desempeñar las responsabilidades asignadas.

Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

4.2.2 Gestión de Activos, Cambios y Configuración (ACM)

De acuerdo con el modelo de C2M2 este dominio está definido para administrar los activos de TI y OT de la organización, incluyendo hardware y software, de acuerdo con el riesgo de la infraestructura crítica y así mismo, se encuentra alineado a los objetivos de la organización. Un activo es algo de valor para una organización. Según este modelo, los activos a considerar son los activos de hardware y software de TI y OT, así como la información esencial para el funcionamiento de la función.

Este dominio identifica la importancia de contar con un inventario de activos de información de ciberseguridad que incluya componentes tales como versiones del software,

ubicación física, propietario y prioridad entre otros, información requerida para gestionar la ciberseguridad.

La gestión de la configuración de activos implica definir la línea base de configuración para los activos de TI y OT, garantizando que los activos se configuran de acuerdo con esta línea base y que los activos de similares características se configuren de igual forma. La gestión de la configuración de activos implica garantizar la línea de base de configuración del activo cuando está operativo y adicionalmente mantenerla en el tiempo, mientras no sean aprobados cambios.

La gestión de cambios en los activos según el modelo de capacidades C2M2 está enfocada en minimizar los riesgos que puedan presentarse en los entornos productivos, cuando se implementan cambios, por lo anterior se debe evaluar con un comité de cambios, las diferentes variables que introducen los cambios solicitados para asegurar que no existen riesgos asociados que puedan afectar el entorno operativo, garantizando así que todos los cambios sigan el proceso definido y se identifiquen cambios no autorizados. El control de cambios se aplica a todo el ciclo de vida del activo, incluyendo la definición de requisitos, pruebas, despliegues, mantenimiento y retiro de la operación.

La Tabla No. 3, relaciona las actividades de los objetivos de este dominio, identificando el nivel MIL en el que se encuentran:

Tabla 5

Actividades Gestión de Activos, Cambios y Configuración (ACM).

OBJETIVO 1:	**Gestión de inventarios**
MIL1	• Hay un inventario de activos de TI y OT que son importantes para la entrega de la función. • Hay un inventario de activos de información que son importantes para la entrega de la función (por ejemplo, puntos de ajuste SCADA, información de clientes, datos financieros).
MIL2	• Los atributos de inventario incluyen información para respaldar la estrategia de ciberseguridad.

	• Los activos inventariados se priorizan en función de su importancia para el suministro de la función.
MIL3	• Existe un inventario de todos los activos de IT y OT conectados relacionados con la entrega de la función. • El inventario de activos es actual (según lo definido por la organización).
OBJETIVO 2:	**Gestión de configuración de activos.**
MIL1	• Las líneas base de la configuración se establecen para los activos inventariados. • Las líneas base de configuración se utilizan para configurar los recursos en la implementación.
MIL2	• El diseño de las líneas base de configuración incluye los objetivos de ciberseguridad.
MIL3	• La configuración de los activos se monitorea para verificar su coherencia con las líneas base durante todo el ciclo de vida de los activos. • Las líneas base de configuración se revisan y actualizan en una frecuencia definida por la organización.
OBJETIVO 3	**Gestión de cambios de activos**
MIL1	• Los cambios en los activos son evaluados antes de ser implementados. • Los cambios son monitoreados.
MIL2	• Los cambios son probados previamente, antes de ser delegados, en lo posible. • Las prácticas de gestión del cambio se aplican al ciclo de vida completo de los activos (adquisición, despliegue, operación, retiro).
MIL3	• Los cambios en los activos se prueban previamente, antes de su despliegue. • Los registros de cambios incluyen información sobre modificaciones que afectan los requisitos de ciberseguridad.
OBJETIVO 4	Administración de actividades
MIL1	• No hay práctica.
MIL2	• Las prácticas son documentadas para las actividades de inventario de activos, configuración y gestión del cambio. • Las partes interesadas para el inventario de activos, la configuración y las actividades de gestión del cambio se identifican y participan. • Se proporcionan recursos adecuados (personas, fondos y herramientas) para apoyar el inventario de activos, la configuración y las actividades de gestión del cambio. • Se han identificado normas y / o directrices para informar el inventario de activos, la configuración y las actividades de gestión del cambio.
MIL3	• Las actividades de inventario de activos, configuración y gestión de cambios se guían por políticas documentadas u otras directivas organizativas. • Las políticas de inventario de activos, configuración y gestión de cambios incluyen los requisitos de cumplimiento para normas y/o directrices especificadas. • El inventario de activos, la configuración y las actividades de gestión del cambio se revisan periódicamente para garantizar la conformidad con la política. • Los roles y las responsabilidades para el desempeño de inventario de activos, configuración y actividades de gestión de cambios son asignados. • El personal que realiza actividades de inventario de activos, configuración y gestión de cambios tiene las habilidades y conocimientos necesarios para desempeñar las responsabilidades asignadas.

Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

4.2.3 Gestión de Identidad y Acceso (IAM)

De acuerdo con el modelo de C2M2 este dominio está definido para administrar las identidades a las que se les debe dar acceso lógico o físico de los activos de la organización. Las

prácticas inadecuadas de gestión del acceso pueden conducir al uso no autorizado, la divulgación, la destrucción o la modificación, así como la exposición innecesaria a riesgos de ciberseguridad.

Es necesario garantizar el aprovisionamiento y la cancelación de acceso a las identidades cuando ya no se requieran, las identidades pueden ser personas (internas o externas a la organización), así como dispositivos, sistemas o procesos que requieran acceso a activos. En algunos casos, las organizaciones pueden necesitar usar identidades compartidas, en este caso puede requerirse implementar medidas compensatorias que garanticen un nivel adecuado de seguridad.

El control del acceso incluye la activación de permisos de acceso asociados con los activos y se otorga sólo después de considerar el riesgo de la función. Los requisitos de acceso están asociados con los activos y proporcionan orientación para determinar a qué entidades se les permite acceder al activo, los límites del acceso permitido y los parámetros de autenticación. Es importante realizar revisiones periódicas al cumplimiento del perfil de acceso otorgado.

La Tabla No. 4, relaciona las actividades de los objetivos de este dominio, identificando el nivel MIL en el que se encuentran:

Tabla 6

Gestión de Identidad y Acceso.

OBJETIVO 1:	**Establecer y Mantener identidades**
MIL1	• Las identidades se provisionan para personal y otras entidades que requieren acceso a activos. • Las credenciales se otorgan para el personal interno o externo que requiere acceso a activos. • Las identidades se cancelan cuando ya no se requieren.
MIL2	• Los repositorios de identidad se revisan y actualizan periódicamente para garantizar la validez. • Las credenciales se revisan periódicamente para asegurarse de que están asociadas con la persona o entidad correcta. • Las identidades se cancelan dentro de los umbrales de tiempo definidos por la organización cuando ya no se requieren.

MIL3	• Los requisitos para las credenciales están informados por los criterios de riesgo de la organización.
OBJETIVO 2:	**Control de acceso**
MIL1	• Se determinan los requisitos de acceso, incluidos los de acceso remoto. • El acceso se concede a identidades basadas en requisitos previos. • El acceso se revoca cuando ya no se requiere.
MIL2	• Los requisitos de acceso incorporan los principios de privilegios mínimos y separación de funciones. • Las solicitudes de acceso son revisadas y aprobadas por el propietario del activo. • Los privilegios de administrador y las cuentas compartidas reciben monitoreo adicional.
MIL3	• Los privilegios de acceso se revisan y actualizan para garantizar la validez, en un periodo definida por la organización. • El acceso a los activos es otorgado por el propietario del activo en función del riesgo de la función. • Los intentos indebidos de acceso son monitoreados como indicadores de eventos de ciberseguridad.
OBJETIVO 3	**Actividades de administración**
MIL1	• No practicas
MIL2	• Se siguen prácticas documentadas para establecer y mantener identidades y controlar el acceso. • Los accesos autorizados a los stakeholders son monitoreados. • Se proporcionan recursos adecuados (personas, presupuesto y herramientas) para apoyar las actividades de acceso y gestión de la identidad. • Se han identificado normas y / o directrices para informar sobre las actividades de acceso y gestión de la identidad.
MIL3	• Las actividades de acceso y gestión de identidad se guían por políticas documentadas u otras directivas organizativas. • Las políticas de acceso y gestión de identidades incluyen los requisitos de cumplimiento para normas y / o directrices especificadas. • Las actividades de acceso y gestión de identidades se revisan periódicamente para asegurar la conformidad con las políticas. • La responsabilidad y autoridad para el desempeño de las actividades de acceso y gestión de la identidad se asignan al personal. • El personal que realiza actividades de acceso y gestión de identidad tiene las habilidades y conocimientos necesarios para desempeñar las responsabilidades asignadas.

Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

4.2.4 Gestión de vulnerabilidades y amenazas (TVM)

De acuerdo con C2M2, este dominio está enfocado en establecer y mantener planes, procedimientos y tecnologías para detectar, identificar, analizar, gestionar y responder a las amenazas y vulnerabilidades de la ciberseguridad, proporcional al riesgo de los objetivos de la infraestructura de la organización. Igualmente contempla el componente de ciberinteligencia, el

cual permite con base en la recolección de información, identificar, analizar y predecir posibles comportamientos anómalos o amenazas de ciberseguridad que puedan poner en riesgo los activos de información de la entidad.

Una amenaza de ciberseguridad se define como "*cualquier circunstancia o evento con el potencial de afectar adversamente las operaciones organizacionales (incluyendo misiones, funciones, imagen o reputación), recursos u otras organizaciones a través de TI, OT o infraestructura de comunicaciones a través de acceso no autorizado, destrucción, divulgación, Modificación de información y / o denegación de servicio. Las amenazas a los activos de TI, OT e infraestructura de comunicación varían y pueden incluir agentes malintencionados, màlware (por ejemplo, virus y gusanos) y ataques DDoS de denegación de servicio distribuidos.*"

La Tabla No. 5, relaciona las actividades de los objetivos de este dominio, identificando el nivel MIL en el que se encuentran:

Tabla 7
Gestión de vulnerabilidades y amenazas.

OBJETIVO 1	Identificación y respuestas a amenazas
MIL1	• Se identifican fuentes de información para apoyar las actividades de gestión de amenazas • La información sobre la amenaza en ciberseguridad es recopilada e interpretada para la función. • Las amenazas que se consideran importantes para la función se abordan.
MIL2	• Se establece un perfil de amenaza para la función que incluye la caracterización de la intención probable, la capacidad y el objetivo de las amenazas a la función. • Se priorizan y supervisan las fuentes de información sobre amenazas que abordan todos los componentes del perfil de amenaza • Las amenazas identificadas se analizan y priorizan • Las amenazas se abordan de acuerdo con la prioridad asignada.
MIL3	• El perfil de amenaza para la función se valida en un periodo definido por la organización. • El análisis y la priorización de las amenazas se basan en los criterios de riesgo de la función. • La información sobre amenazas se incluye en el registro de riesgos.
OBJETIVO 2	Reducir vulnerabilidades de ciberseguridad
MIL1	• Se identifican fuentes de información para soportar el descubrimiento de la vulnerabilidad.

	• La información sobre la vulnerabilidad se recopila y se analiza. • Se abordan las vulnerabilidades de ciberseguridad que se consideran importantes.
MIL2	• Se supervisan las fuentes de información de la vulnerabilidad. • Se realizan evaluaciones de vulnerabilidad de ciberseguridad. • Las vulnerabilidades de ciberseguridad identificadas se analizan y priorizan. • Las vulnerabilidades de ciberseguridad se tratan de acuerdo con la prioridad asignada. • El impacto operacional de la función se evalúa antes de implementar parches de seguridad.
MIL3	• Las evaluaciones de la vulnerabilidad de ciberseguridad se realizan para todos los activos importantes, en un periodo definido por la organización. • Las evaluaciones de la vulnerabilidad de ciberseguridad son informadas. • Las evaluaciones de vulnerabilidad de ciberseguridad son realizadas por partes independientes de las operaciones de la función. • El análisis y la priorización de las vulnerabilidades de ciberseguridad se basan en los criterios de riesgo de la función. • La información de vulnerabilidad de ciberseguridad se incluye al registro de riesgo. • Las actividades de monitoreo de riesgos validan las respuestas a las vulnerabilidades de ciberseguridad.
OBJETIVO 3	Actividades de administración
MIL1	• No Practica
MIL2	• Se siguen prácticas documentadas para las actividades de gestión de amenazas y vulnerabilidad. • Se informa a las partes interesadas las actividades de gestión de la amenaza y la vulnerabilidad. • Se proporcionan recursos adecuados para apoyar las actividades de manejo de amenazas y vulnerabilidad. • Se han identificado normas y/o directrices para informar sobre las actividades de gestión de amenazas y vulnerabilidad.
MIL3	• Las actividades de gestión de amenazas y vulnerabilidades se guían por políticas documentadas u otras directivas organizativas. • Las políticas de gestión de amenazas y vulnerabilidades incluyen requisitos de cumplimiento para normas y/o directrices especificadas. • Las actividades de gestión de amenazas y vulnerabilidad se revisan periódicamente para garantizar la conformidad con las políticas. • La responsabilidad y autoridad para el desempeño de las actividades de gestión de amenazas y vulnerabilidad se asignan al personal. • El personal que realiza actividades de gestión de amenazas y vulnerabilidad tiene las habilidades y conocimientos necesarios para desempeñar sus responsabilidades asignadas.

Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

4.2.5 Conciencia Situacional. (SA)

De acuerdo con C2M2, este dominio está enfocado en establecer y mantener actividades y tecnologías para recopilar, analizar, alarmar, presentar y utilizar información operativa y de

ciberseguridad, incluyendo información de estado e información resumida de los otros dominios modelo, para formar una imagen operativa común (COP).

Una vez que una organización desarrolla un COP, puede alinear los estados de operación predefinidos con los cambios en el entorno operativo. La capacidad de cambiar de un estado predefinido a otro puede permitir una respuesta más rápida y eficaz a eventos de ciberseguridad o cambios en el entorno de amenaza.

La Tabla No. 6, relaciona las actividades de los objetivos de este dominio, identificando el nivel MIL en el que se encuentran:

Tabla 8

Conciencia Situacional.

OBJETIVO 1	**Ejecutar loggin**
MIL1	• El loggin está ocurriendo para los activos importantes para la función cuando sea posible.
MIL2	• Se han definido los requisitos de loggin para todos los activos importantes para la función. • Los datos de loggin se están agregando dentro de la función.
MIL3	• Los requisitos de loggin se basan en el riesgo para la función.
OBJETIVO 2	**Ejecutar Monitoreo**
MIL1	• Se llevan a cabo actividades de vigilancia de la ciberseguridad. • Los entornos operacionales son monitoreados por el comportamiento anómalo que puede indicar un evento de ciberseguridad.
MIL2	• Se han definido requisitos de monitoreo y análisis para la función y dirección de la revisión oportuna de los datos del evento. • Las alarmas y alertas están configuradas para ayudar en la identificación de eventos de seguridad cibernética. • Los indicadores de actividad anómala han sido definidos y son monitoreados a través del ambiente operacional. • Las actividades de monitoreo están alineadas con el perfil de amenaza de la función.
MIL3	• Los requisitos de supervisión se basan en el riesgo para la función. • El monitoreo se integra con otros procesos comerciales y de seguridad • El monitoreo continuo se realiza a través del entorno operacional para identificar la actividad anómala. • El registro de riesgo se utiliza para identificar indicadores de actividad anómala. • Las alarmas y alertas se configuran según indicadores de actividad anómala.
OBJETIVO 3	**Establecer y mantener un COP.**
MIL1	• No Practica
MIL2	• Se establecen y mantienen métodos para comunicar el estado actual de ciberseguridad para la función.

	• Los datos de monitoreo se agregan para proporcionar una comprensión del estado operacional de la función. • La información de toda la organización está disponible para mejorar la imagen operativa común.
MIL3	• El monitoreo de los datos son agrupados para proporcionar una comprensión casi en tiempo real del estado de ciberseguridad. • Información de fuera de la organización se recopila para mejorar el cuadro operativo común. • Los estados de funcionamiento predefinidos se definen e invocan (proceso manual o automatizado) basado en la imagen de funcionamiento común.
OBJETIVO 4	Actividades de administración
MIL1	• No practica
MIL2	• Las prácticas documentadas, son registradas y monitoreadas, en el COP. • El monitoreo y las actividades de las partes interesadas se identifican e involucran en el COP. • Se proporcionan recursos adecuados para apoyar el monitoreo de las actividades del COP. • Se han identificado normas y/o directrices para informar sobre el monitoreo y las actividades del COP.
MIL3	• Las actividades de registro, monitoreo y COP se guían por políticas documentadas u otras directivas organizativas. • Las políticas de registro, monitoreo y COP incluyen los requisitos de cumplimiento para normas y / o directrices especificadas. • Las actividades de extracción, monitoreo y COP se revisan periódicamente para asegurar la conformidad con la política. • La responsabilidad y autoridad para el desempeño del monitoreo y actividades de COP se asignan al personal. • El personal que realiza actividades de monitoreo y COP tiene las habilidades y conocimientos necesarios para desempeñar las responsabilidades asignadas.

Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

4.2.6 Compartir información y comunicaciones. (ISC)

De acuerdo con C2M2, este dominio está enfocado en establecer y mantener relaciones con entidades internas y externas para recopilar y proporcionar información sobre ciberseguridad, incluyendo amenazas y vulnerabilidades, para reducir riesgos y aumentar la resiliencia operacional, proporcional al riesgo para la infraestructura crítica y los objetivos organizacionales.

El objetivo del intercambio de información es fortalecer la ciberseguridad, dentro de una organización o dentro de un sector de infraestructura crítica, estableciendo y manteniendo un marco para la interacción dentro de una organización, entre organizaciones y entre organizaciones y el gobierno.

La Tabla No. 7, relaciona las actividades de los objetivos de este dominio, identificando el nivel MIL en el que se encuentran:

Tabla 9

Compartir información y comunicaciones.

OBJETIVO 1	**Compartir información de ciberseguridad**
MIL1	• La información se recopila y se proporciona a individuos y/u organizaciones seleccionadas. • La responsabilidad de informar acerca de ciberseguridad se asigna al personal.
MIL2	• Las partes interesadas en el intercambio de información se identifican en función de su importancia para el funcionamiento continuo de la función. • La información se recopila y se proporciona a los interesados identificados que comparten la información. • Se identifican fuentes técnicas que pueden consultarse en cuestiones de ciberseguridad. • Se establecen y mantienen disposiciones para permitir el intercambio seguro de información sensible o clasificada. • Las prácticas de intercambio de información se refieren tanto a las operaciones estándar como a las operaciones de emergencia.
MIL3	• Las partes interesadas en el intercambio de información se identifican basándose en el interés compartido y el riesgo para la infraestructura crítica. • La función o la organización participa en centros de intercambio y análisis de información. • Se han definido requisitos de intercambio de información y la difusión oportuna de la información sobre ciberseguridad. • Existen procedimientos para analizar y entender la información compartida. • Se ha establecido una red de relaciones de confianza interna y externa (formal y/o informal) para examinar y validar información sobre eventos de ciberseguridad.
OBJETIVO 2	**Actividades de administración**
MIL1	• No practica
MIL2	• Se siguen prácticas documentadas para actividades de intercambio de información. • Las partes interesadas para las actividades de intercambio de información se identifican. • Se proporcionan recursos adecuados (personas, recursos y herramientas) para apoyar las actividades de intercambio de información. • Se han identificado normas y/o directrices para informar las actividades de intercambio de información.
• MIL3	• Las actividades de intercambio de información se guían por políticas documentadas u otras directivas organizativas. • Las políticas de intercambio de información incluyen los requisitos de cumplimiento para normas y/o directrices especificadas. • Las actividades de intercambio de información se revisan periódicamente para asegurar su cumplimiento. • La responsabilidad y autoridad para el desempeño de las actividades de intercambio de información se asignan al personal. • El personal que realiza actividades de intercambio de información tiene las habilidades y conocimientos necesarios para desempeñar las responsabilidades asignadas.

	• Las políticas de intercambio de información abordan la información protegida y el uso ético en el intercambio de información, incluida la información confidencial y clasificada según corresponda.

Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

4.2.7 Respuesta a eventos e incidentes y continuidad de operaciones. (IR)

De acuerdo con C2M2, este dominio está enfocado en establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a eventos de ciberseguridad y mantener las operaciones a lo largo de un evento de ciberseguridad, en consonancia con el riesgo para la infraestructura crítica y los objetivos organizacionales.

La Tabla No. 8, relaciona las actividades de los objetivos de este dominio, identificando el nivel MIL en el que se encuentran:

Tabla 10

Respuesta a eventos e incidentes y continuidad de operaciones.

OBJETIVO 1	**Detectar eventos de ciberseguridad**
MIL1	• Hay un punto de contacto (persona o rol) con quien se pueden informar los eventos de ciberseguridad. • Se informan los eventos detectados de ciberseguridad. • Los eventos de seguridad cibernética se registran y se registran.
MIL2	• Se establecen criterios para la detección de eventos de ciberseguridad. • Existe un repositorio donde los eventos de seguridad cibernética se registran en base a los criterios establecidos.
MIL3	• La información del evento se correlaciona para apoyar el análisis de incidentes mediante la identificación de patrones, tendencias y otras características comunes. • Las actividades de detección de eventos de ciberseguridad se ajustan en función de la información del registro de riesgos de la organización. • La imagen de funcionamiento común para la función se supervisa para apoyar la identificación de eventos de ciberseguridad.
OBJETIVO 2	• **Escalar eventos de ciberseguridad y declarar incidentes**
MIL1	• Se establecen los criterios para el escalamiento de eventos de ciberseguridad incluidos los criterios de declaración de incidentes. • Los eventos de ciberseguridad se analizan para apoyar el escalamiento y la declaración de incidentes de ciberseguridad. • Los eventos e incidentes escalados de ciberseguridad son registrados y rastreados.

MIL2	• Los criterios para el escalamiento de eventos de ciberseguridad, incluidos los criterios de incidentes de ciberseguridad, se establecen en función del impacto potencial de la función. • Los criterios para el escalamiento de eventos de ciberseguridad, incluidos los criterios de declaración de incidentes, se actualizan en un periodo definido por la organización. • Hay un repositorio donde los eventos escalados de ciberseguridad y los incidentes se registran y se monitorean hasta el cierre.
MIL3	• Los criterios para el escalamiento de eventos de ciberseguridad, incluidos los criterios de declaración de incidentes de ciberseguridad, se ajustan de acuerdo con la información del registro de riesgos de la organización y el perfil de amenaza. • Los eventos escalados de ciberseguridad e incidentes declarados se informan en el COP para la función. • Los eventos escalados de ciberseguridad y los incidentes declarados se correlacionan para apoyar el descubrimiento de patrones, tendencias y otras características comunes.
OBJETIVO 3	**Responder a incidentes y eventos escalados de ciberseguridad**
MIL1	• El personal de eventos de ciberseguridad y de respuesta a incidentes se identifica y se asignan roles. • Las respuestas a eventos e incidentes escalados de ciberseguridad se implementan para limitar el impacto a la función y restaurar las operaciones a estados normales. • Se realizan informes de eventos e incidentes escalados de ciberseguridad.
MIL2	• El evento de ciberseguridad y la respuesta a incidentes se realizan de acuerdo con procedimientos definidos que abordan todas las fases del ciclo de vida del incidente. • Los eventos de ciberseguridad y los planes de respuesta a incidentes se prueban a una frecuencia definida por la organización. • El evento de ciberseguridad y los planes de respuesta a incidentes abordan los activos de IT y OT importantes para la entrega de la función. • Se lleva a cabo la capacitación para los equipos de eventos de ciberseguridad y de respuesta a incidentes.
MIL3	• El evento de ciberseguridad y el análisis de la causa raíz del incidente y las lecciones aprendidas se realizan y se toman medidas correctivas. • El evento de ciberseguridad y las respuestas a los incidentes se coordinan con las fuerzas del orden y otras entidades gubernamentales según proceda, incluido el apoyo a la recopilación y preservación de pruebas. • El evento de ciberseguridad y el personal de respuesta a incidentes participan en ejercicios conjuntos de seguridad cibernética con otras organizaciones. • El evento de ciberseguridad y los planes de respuesta a incidentes se revisan y actualizan en una frecuencia definida por la organización. • El evento de ciberseguridad y las actividades de respuesta a incidentes se coordinan con entidades externas pertinentes. • El evento de ciberseguridad y los planes de respuesta a incidentes están alineados con los criterios de riesgo de la función y el perfil de amenaza. • Las políticas y procedimientos para reportar el evento de ciberseguridad y la información de incidentes a las autoridades designadas se ajustan a las leyes, reglamentos y acuerdos contractuales aplicables. • Los activos restaurados se configuran adecuadamente y la información de inventario se actualiza después de la ejecución de los planes de respuesta.
OBJETIVO 4	**Plan de continuidad**
MIL1	• Se identifican las actividades necesarias para mantener operaciones mínimas de la función. • Se identifica la secuencia de actividades necesarias para devolver la función al funcionamiento normal.

	• Se desarrollan planes de continuidad para sostener y restaurar el funcionamiento de la función.
MIL2	• Los análisis de impacto del negocio sirven para elaborar planes de continuidad. • Los objetivos de tiempo de recuperación (RTO) y los objetivos de punto de recuperación (RPO) para la función se incorporan en los planes de continuidad. • Los planes de continuidad son evaluados y ejercidos.
MIL3	• Los análisis de impacto empresarial se revisan y actualizan periódicamente marido. RTO y RPO están alineados con los criterios de riesgo de la función. • Los resultados de la prueba y/o activación del plan de continuidad se comparan con los objetivos de recuperación y los planes se mejoran en consecuencia. • Los planes de continuidad son revisados y actualizados periódicamente. • Los activos restaurados se configuran adecuadamente y la información de inventario se actualiza después de la ejecución de los planes de continuidad.
OBJETIVO 5	**Actividades de administración**
MIL1	• No practica
MIL2	• Se siguen prácticas documentadas para el evento de ciberseguridad y la respuesta a incidentes, así como para la continuidad de las actividades de las operaciones. • Se identifican y participan las partes interesadas para el evento de ciberseguridad y la respuesta a incidentes, así como la continuidad de las actividades de las operaciones. • Se proporcionan recursos adecuados (personas, presupuesto y herramientas) para apoyar el evento de ciberseguridad y la respuesta a incidentes, así como la continuidad de las actividades de las operaciones. • Se han identificado estándares y/o directrices para informar el evento de ciberseguridad y la respuesta a incidentes, así como la continuidad de las actividades de las operaciones.
MIL3	• El evento de ciberseguridad y la respuesta a incidentes, así como la continuidad de las actividades de operaciones, se guían por políticas documentadas u otras directivas organizativas. • El evento de ciberseguridad y la respuesta a incidentes, así como la continuidad de las políticas de operaciones, incluyen los requisitos de cumplimiento de normas y/o directrices especificadas. • El evento de ciberseguridad y la respuesta a incidentes, así como la continuidad de las actividades de las operaciones, se revisan periódicamente para asegurar la conformidad con la política. • La responsabilidad y autoridad para el desempeño del evento de ciberseguridad y la respuesta a incidentes, así como la continuidad de las actividades de operaciones, se asignan al personal. • El personal que realiza el evento de ciberseguridad y la respuesta a incidentes, así como las actividades de continuidad de las operaciones tienen las habilidades y conocimientos necesarios para desempeñar las responsabilidades asignadas.

Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

4.2.8 Gestión de Cadena de Suministro y Dependencias Externas. (EDM)

De acuerdo con C2M2, este dominio está enfocado en establecer y mantener controles para gestionar los riesgos de ciberseguridad asociados a los servicios y activos que dependen de

entidades externas, en consonancia con el riesgo para la infraestructura crítica y los objetivos organizacionales. A medida que aumentan las interdependencias entre las infraestructuras, los socios operativos, los proveedores, los proveedores de servicios y los clientes, establecen y mantienen relaciones clave, que se deben gestionar ya que existen riesgos asociados de ciberseguridad que se deben contemplar tanto para garantizar la entrega segura, fiable y resiliente de la función.

La Tabla No. 9, relaciona las actividades de los objetivos de este dominio, identificando el nivel MIL en el que se encuentran:

Tabla 11

Gestión de Cadena de Suministro y Dependencias Externas.

OBJETIVO 1	**Identificar dependencias**
MIL1	• Se identifican dependencias importantes de proveedores de IT y OT (es decir, las partes externas de las que depende la entrega de la función, incluidos los socios operativos). • Se identifican importantes dependencias del cliente (es decir, las partes externas que dependen de la entrega de la función, incluidos los socios operativos).
MIL2	• Las dependencias de proveedores se identifican de acuerdo con los criterios establecidos. • Las dependencias del cliente se identifican de acuerdo con los criterios establecidos. • Se identifican dependencias esenciales y otras dependencias esenciales. • Las dependencias son priorizadas.
MIL3	• La priorización e identificación de la dependencia se basan en los criterios de riesgo de la función u organización.
OBJETIVO 2	**Administrar el riesgo de dependencia**
MIL1	• Se identifican y se abordan riesgos significativos de ciberseguridad debido a proveedores y otras dependencias. • Los requisitos de ciberseguridad se consideran al establecer relaciones con proveedores y otros terceros.
MIL2	• Los riesgos de dependencia de ciberseguridad identificados se introducen en el registro de riesgos. • Los contratos y acuerdos con terceros incorporan el intercambio de información sobre la amenaza en ciberseguridad. • Los requisitos de ciberseguridad se establecen para los proveedores de acuerdo con una práctica definida, incluidos los requisitos para prácticas seguras de desarrollo de software cuando sea apropiado. • Los acuerdos con proveedores y otras entidades externas incluyen los requisitos de ciberseguridad. • La evaluación y selección de proveedores y otras entidades externas incluye la consideración de su capacidad para cumplir con los requisitos de ciberseguridad.

	• Los acuerdos con proveedores requieren la notificación de incidentes de ciberseguridad relacionados con la entrega del producto o servicio. • Los proveedores y otras entidades externas son revisados periódicamente por su capacidad para cumplir continuamente con los requisitos de ciberseguridad.
MIL3	• Los riesgos de ciberseguridad debido a dependencias externas se gestionan de acuerdo con los criterios y procesos de gestión de riesgos de la organización. • Los requisitos de ciberseguridad se establecen para las dependencias de proveedores basándose en los criterios de riesgo de la organización. • Los acuerdos con proveedores exigen la notificación de defectos del producto que induzcan la vulnerabilidad durante todo el ciclo de vida previsto de los productos entregados. • Las pruebas de aceptación de los activos adquiridos incluyen pruebas de requisitos de ciberseguridad. • Las fuentes de información son monitoreadas para identificar y evitar las amenazas de la cadena de suministro.
OBJETIVO 3	**Actividades de administración**
MIL1	• No practica
MIL2	• Se siguen prácticas documentadas para administrar el riesgo de dependencia. • Las partes interesadas para la gestión del riesgo de dependencia se identifican. • Se proporcionan recursos adecuados (personas, presupuesto y herramientas) para apoyar las actividades de gestión del riesgo de dependencia. • Se han identificado normas y/o directrices para informar sobre la gestión del riesgo de dependencia.
MIL3	• Las actividades de gestión del riesgo de dependencia se guían por políticas documentadas u otras directivas organizativas. • Las políticas de gestión del riesgo de dependencia incluyen los requisitos de cumplimiento para normas y/o directrices especificadas. • Las actividades de gestión del riesgo de dependencia se revisan periódicamente para garantizar la conformidad con las políticas. • La responsabilidad y autoridad para el desempeño de la gestión del riesgo de dependencia se asignan al personal. • El personal que realiza la gestión del riesgo de dependencia tiene las habilidades y conocimientos necesarios para desempeñar sus responsabilidades asignadas.

Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

4.2.9 Administración del Personal. (WM)

De acuerdo con C2M2, este dominio está enfocado en establecer y mantener planes, procedimientos, tecnologías y controles para crear una cultura de ciberseguridad y asegurar la idoneidad y la competencia del personal, en consonancia con el riesgo para la infraestructura crítica y los objetivos de la organización.

La Tabla No. 10, relaciona las actividades de los objetivos de este dominio, identificando el nivel MIL en el que se encuentran:

Tabla 12

Administración del Personal.

OBJETIVO 1	**Asignar responsabilidades de ciberseguridad**
MIL1	• Se identifican las responsabilidades de seguridad ciberseguridad para la función. • Las responsabilidades de ciberseguridad se asignan a personas específicas.
MIL2	• Las responsabilidades de ciberseguridad se asignan a funciones específicas, incluidos los proveedores de servicios externos. • Las responsabilidades de seguridad ciberseguridad están documentadas.
MIL3	• Las responsabilidades de ciberseguridad y los requisitos de trabajo se revisan y actualizan según corresponda. • Las responsabilidades de ciberseguridad se incluyen en los criterios de evaluación del desempeño laboral. • Las responsabilidades de ciberseguridad asignadas se gestionan para asegurar la cobertura adecuada y redundante.
OBJETIVO 2	**Control del ciclo de vida de la fuerza de trabajo**
MIL1	• La verificación de personal se realiza en el momento de la contratación de puestos que tienen acceso a los activos necesarios para la entrega de la función. • Los procedimientos de terminación de personal abordan la ciberseguridad.
MIL2	• La verificación de personal se realiza a una frecuencia definida por la organización para las posiciones que tienen acceso a los activos necesarios para la entrega de la función. • Los procedimientos de transferencia de personal abordan la ciberseguridad.
MIL3	• Las designaciones de riesgo se asignan a todas las posiciones que tienen acceso a los activos necesarios para la entrega de la función. • Se realizan pruebas para todas las posiciones. • La planificación de la sucesión se realiza para el personal basado en la designación de riesgo. • Se implementa un proceso formal de rendición de cuentas que incluye acciones disciplinarias para el personal que no cumple con las políticas y procedimientos de seguridad establecidos.
OBJETIVO 3	Desarrollar la fuerza de trabajo de ciberseguridad.
MIL1	• La capacitación en seguridad ciberseguridad se pone a disposición del personal con responsabilidades de ciberseguridad asignadas.
MIL2	• Se identifican las brechas de conocimiento y habilidad de ciberseguridad. • Las deficiencias identificadas se abordan mediante la contratación y/o la capacitación. • El entrenamiento en ciberseguridad se proporciona como requisito previo para otorgar acceso a los activos que apoyan la entrega de la función.
MIL3	• Se establecen y mantienen objetivos de gestión de la fuerza de trabajo de ciberseguridad que respaldan las necesidades operacionales actuales y futuras. • El reclutamiento y la retención están alineados para apoyar los objetivos de gestión de la fuerza de trabajo de ciberseguridad. • Los programas de capacitación están alineados para respaldar los objetivos de gestión de la fuerza de trabajo de ciberseguridad. • La eficacia de los programas de formación se evalúa con una frecuencia definida por la organización y se realizan mejoras según proceda. • Los programas de capacitación incluyen oportunidades de educación continua y desarrollo profesional para personal con responsabilidades significativas en ciberseguridad.
OBJETIVO 4	**Aumentar la conciencia sobre ciberseguridad**

MIL1	• Se realizan actividades de concienciación en ciberseguridad
MIL2	• Se establecen y mantienen objetivos de actividades de sensibilización en ciberseguridad. • El contenido de conciencia de ciberseguridad se basa en el perfil de amenaza de la organización.
MIL3	• Las actividades de concienciación de ciberseguridad están alineadas con los estados de operación predefinidos. • La eficacia de las actividades de concienciación en ciberseguridad se evalúa a una frecuencia definida por la organización y se realizan mejoras según proceda.
OBJETIVO 5	Actividades de administración
MIL1	• No practica
MIL2	• Se siguen prácticas documentadas para las actividades de gestión de la fuerza laboral en ciberseguridad. • Las partes interesadas en las actividades de gestión de la fuerza de trabajo de ciberseguridad se identifican y participan. • Se proporcionan recursos adecuados (personas, presupuesto y herramientas) para apoyar las actividades de gestión de la fuerza laboral de ciberseguridad.
MIL3	• Las actividades de gestión de la fuerza laboral de ciberseguridad se guían por políticas documentadas u otras directivas organizativas. • Las políticas de gestión de mano de obra de ciberseguridad incluyen los requisitos de cumplimiento para normas y/o directrices especificadas. • Las actividades de gestión de la fuerza de trabajo de ciberseguridad se revisan periódicamente para garantizarlas. • La responsabilidad y autoridad para el desempeño de las actividades de gestión de la fuerza de trabajo de ciberseguridad se asignan al personal. • El personal que realiza actividades de gestión de personal de ciberseguridad tiene las habilidades y conocimientos necesarios para desempeñar las responsabilidades asignadas.

Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

4.2.10 Programa de administración de ciberseguridad. (CPM)

De acuerdo con C2M2, este dominio está enfocado en establecer y mantener un programa de ciberseguridad empresarial que proporcione gobernabilidad, planificación estratégica y patrocinio para las actividades de ciberseguridad de la organización, de una manera que alinee los objetivos de ciberseguridad con los objetivos estratégicos de la organización y el riesgo a la infraestructura crítica.

Un programa de ciberseguridad es un grupo integrado de actividades diseñadas y administradas para cumplir los objetivos de ciberseguridad para la organización y/o la función. Puede ser implementado en la organización o en el nivel de función, se requiere una

implementación de nivel superior y un punto de vista empresarial para beneficiar a la organización integrando actividades y aprovechando las inversiones de recursos en toda empresa.

La Tabla No. 11, relaciona las actividades de los objetivos de este dominio, identificando el nivel MIL en el que se encuentran:

Tabla 13

Programa de administración de ciberseguridad.

OBJETIVO 1	**Estrategia para establecer un programa de ciberseguridad**
MIL1	• La organización tiene una estrategia de un programa de ciberseguridad
MIL2	• La estrategia del programa de ciberseguridad define objetivos para las actividades de ciberseguridad de la organización. • La estrategia y las prioridades del programa de ciberseguridad están documentadas y alineadas con los objetivos estratégicos de la organización y el riesgo para la infraestructura crítica. • La estrategia del programa de ciberseguridad define el enfoque de la organización para proporcionar supervisión de programas y gobernanza para las actividades de ciberseguridad. • La estrategia del programa de ciberseguridad define la estructura y organización del programa de ciberseguridad. • La estrategia del programa de ciberseguridad es aprobada por la alta dirección.
MIL3	• La estrategia del programa de ciberseguridad se actualiza para reflejar los cambios en el negocio, los cambios en el entorno operativo y los cambios en el perfil de amenaza.
OBJETIVO 2	**Programa de ciberseguridad**
MIL1	• Se proporcionan recursos (personas, herramientas y financiamiento) para apoyar el programa de ciberseguridad. • La alta gerencia brinda patrocinio para el programa de ciberseguridad.
MIL2	• El programa de ciberseguridad se establece de acuerdo con la estrategia. • Se proveen fondos adecuados y otros recursos para establecer y operar un programa de ciberseguridad alineado con la estrategia. • El patrocinio de la alta dirección para el programa de ciberseguridad es visible y activo (por ejemplo, la alta importancia y el valor de las actividades de ciberseguridad son comunicados regularmente por la alta dirección). • Si la organización desarrolla o adquiere software, las prácticas seguras de desarrollo de software son patrocinadas como un elemento del programa de ciberseguridad. • El desarrollo y mantenimiento de políticas de seguridad cibernética es patrocinado. • La responsabilidad del programa de ciberseguridad se asigna a un rol con la autoridad necesaria.
MIL3	• El desempeño del programa de ciberseguridad es monitoreado para asegurar que se alinee con la estrategia del programa de ciberseguridad. • El programa de ciberseguridad es revisado de forma independiente (es decir, por revisores que no están en el programa) para el logro de los objetivos del programa de ciberseguridad.

	• El programa de ciberseguridad aborda y permite el cumplimiento normativo según corresponda. • El programa de ciberseguridad monitorea y/o participa en estándares o iniciativas de ciberseguridad de la industria.
OBJETIVO 3	**Establecer y mantener una arquitectura de ciberseguridad.**
MIL1	• Una estrategia de Arquitectura aísla los sistemas IT implementados de los OT.
MIL2	• Se ha establecido una arquitectura de ciberseguridad para permitir la segmentación, el aislamiento y otros requisitos que apoyan la estrategia de ciberseguridad. • La segmentación y el aislamiento se mantienen de acuerdo con un plan documentado.
MIL3	• La arquitectura de ciberseguridad se actualiza con una frecuencia definida por la organización para mantenerla actualizada.
OBJETIVO 4	**Realizar desarrollo de software seguro**
MIL1	• No practica
MIL2	• El software que se desplegará en activos que son importantes para la entrega de la función se desarrolla utilizando prácticas seguras de desarrollo de software.
MIL3	• Las políticas requieren que el software que se va a desplegar en activos que sean importantes para la entrega de la función se desarrolle utilizando prácticas seguras de desarrollo de software.
OBJETIVO 5	**Actividades de administración**
MIL1	• No practica
MIL2	• Se siguen prácticas documentadas para las actividades de gestión del programa de ciberseguridad. • Las actividades de la administración del programa de ciberseguridad son identificadas e incluidas. • Se han identificado normas y/o directrices para informar sobre las actividades de gestión del programa de ciberseguridad.
MIL3	• Las actividades de gestión del programa de ciberseguridad se guían por políticas documentadas u otras directivas organizativas. • Las actividades de gestión del programa de ciberseguridad se revisan periódicamente para garantizarlas. • El personal que realiza actividades de gestión del programa de ciberseguridad tiene las habilidades y conocimientos necesarios para desempeñar las responsabilidades asignadas.

Nota. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). Departamento de Energía de los Estados Unidos de América (2014). Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

4.3 Evaluación del modelo C2M2 en la cancillería.

Para el uso del modelo, se inició con solicitar al DOE copia del instrumento y aprobación del uso del mismo para la cancillería, para lo cual ellos enviaron un email con la aprobación y la documentación requerida para hacer uso de la misma.

Seguidamente se identificaron las partes interesadas en la cancillería para la aplicación de la herramienta y se elaboró una matriz de riesgos, la cual se anexa en el Apéndice No. 1 y el plan

de tratamiento al riesgo de la implementación del modelo C2M2, es el que se detalla a continuación:

Tabla 14

Respuesta a Riesgos en la implementación del modelo C2M2.

Categoría	ID	Factores de Riesgos	Acciones de Mitigación	Acciones de Emergencia
Administración	A1	Errores en la definición del Alcance y Entregables del Proyecto	Utilización de una metodología probada y basada en el PMI	Redefinición del alcance y entregables
	A2	Ampliación del cronograma	Validar los tiempos acordes a los recursos a implementar	Redefinición del trabajo Ampliación del grupo Humano Ampliación del horario
	A3	Incorrecta gestión de Cambios en el Alcance	Implementar un proceso de Gestión de Cambios en caso de no existir en el Cliente del proyecto	
	A4	Roles & Responsabilidades mal o no Definidas Completamente	Gestionar los stakeholders y lograr documentar definiciones adecuadas	Renegociar roles, solicitar autorizaciones, definir responsabilidades
	A5	Inadecuada Administración de la Calidad	Utilización de Gerentes de Proyecto con experiencia positiva demostrada en proyectos similares	
	A6	Inadecuada Administración del Cambio	Implementar un proceso de Gestión de Cambios en caso de no existir en el Cliente del proyecto	
	A7	Métodos de Estimación inadecuados	Validar los tiempos acordes a los recursos a implementar Evaluar de acuerdo con expertos y estimación de 3 puntos	
	A8	Uso inadecuado de las disciplinas del proyecto	Utilización de Gerentes de Proyecto con experiencia positiva demostrada en proyectos similares	La PMO gestionará recursos para apoyar los requerimientos de acciones correctivas

Recursos	A9	Calidad inadecuada en el plan del proyecto	Utilización de Gerentes de Proyecto con experiencia positiva demostrada en proyectos similares Utilización de Expertos con amplia experiencia	
	R1	Deficiencia en la asignación de recursos	Desarrollar los Recursos del Proyecto Negociar Recursos Requeridos Conseguir nuevos recursos	Negociar recursos requeridos
	R2	Deficiencias en las Habilidades del Equipo	Inclusión al Equipo del proyecto de personal con las habilidades Requeridas Desarrollo de las habilidades a los miembros del Equipo	Inclusión al Equipo del proyecto de personal con las habilidades Requeridas Desarrollo de las habilidades a los miembros del Equipo
	R3	Desviación de Recursos	Preparar hojas de vida de personal de apoyo que pudiese colaborar en el proyecto Negociar disponibilidad con personal Extra, en caso de requerirse	Preparar hojas de vida de personal de apoyo que pudiese colaborar en el proyecto Negociar disponibilidad con personal Extra, en caso de requerirse
	R4	No Disponibilidad de algún Bien o Servicio	Adquirir el bien o servicio que pudiese requerirse	Preparar la adquisición del Bien o Servicio Requerido
	R5	Conflictos de recursos con otros proyectos	Conseguir el aval del Sponsor y mostrar la posición estratégica del proyecto. Entender la posición estratégica del proyecto Conseguir una formalización de la prioridad del proyecto, respecto a otros	Negociar recursos con los proyectos Conseguir recursos Externos
Complejidad	C1	Deficiencias en el entendimiento de la Integración de Productos	Contratar Experto Agregar capacitación y sensibilización para el equipo completo por parte del experto	Hacer acuerdo de prioridad de apoyo con terceros
	C2	Prioridades del Proyecto en Conflicto	Conseguir el aval del Sponsor y mostrar la posición estratégica del proyecto. Entender la posición estratégica del proyecto Conseguir una formalización de la prioridad del proyecto, respecto a otros	Evaluar impacto y revisar el plan del proyecto

Cultura Organizacional	C3	Infraestructura requerida deficiente o inexistente	Adquirir infraestructura requerida Definir planes de contingencia Evaluar y adquirir nueva infraestructura Definir plan alterno de operación
	C4	Ambiente de Producción deficiente o inexistente	Implementar buenas prácticas de desarrollo y pruebas Adquirir ambientes de producción externos Transferir la producción a un proveedor con los acuerdos de niveles de servicio requeridos Adquirir elementos para salida a producción Contratar servicio de hosting para entrada en producción Mejorar ambiente de producción
	C5	Objetivos de desempeño esperados no reales	Renegociar objetivos Evaluar competencias del equipo y renegociar recursos Renegociar objetivos Evaluar competencias del equipo y renegociar recursos
	O1	Ocultación de la información	Generar confianza y firmar acuerdos de confidencialidad para accesar la información Identificar e inventariar la información requerida y realizar continuos ajustes Evidenciar la ausencia de información Buscar nuevas fuentes de información
	O2	Influencias Políticas en contra del proyecto	Conseguir el aval del Sponsor y mostrar la posición estratégica del proyecto. Entender la posición estratégica del proyecto Conseguir una formalización de la prioridad del proyecto, respecto a otros
	O3	Resistencia al Cambio	Agregar capacitación y sensibilización para el equipo completo Realizar una Gestión del Cambio humana formal y detallada con objetivos del proyecto Realizar actividades de sensibilización y de los beneficios esperados del proyecto
	O4	Falta de compromiso Gerencial	Conseguir el aval del Sponsor y mostrar la posición estratégica del proyecto. Entender la posición estratégica del proyecto Conseguir una formalización de la prioridad del proyecto, respecto a otros Entrevista con la gerencia para determinar acciones con respecto al proyecto

	O5	Objetivos de tiempo inconsistente	Utilización de una metodología probada y basada en el PMI Utilización de Gerentes de Proyecto con experiencia positiva demostrada en proyectos similares	Evaluar impacto y revisar el plan del proyecto
	O6	Objetivos de costos inconsistente	Utilización de una metodología probada y basada en el PMI Utilización de Gerentes de Proyecto con experiencia positiva demostrada en proyectos similares	Evaluar impacto y revisar el plan del proyecto
	O7	Objetivos de alcance inconsistente	Utilización de una metodología probada y basada en el PMI Utilización de Gerentes de Proyecto con experiencia positiva demostrada en proyectos similares	Evaluar impacto y revisar el plan del proyecto
	O8	Deficiencia en la definición del alcance	Utilización de una metodología probada y basada en el PMI Utilización de Gerentes de Proyecto con experiencia positiva demostrada en proyectos similares	Evaluar impacto y revisar el plan del proyecto
	O9	Falta de priorización de los proyectos	Conseguir el aval del Sponsor y mostrar la posición estratégica del proyecto. Entender la posición estratégica del proyecto Conseguir una formalización de la prioridad del proyecto, respecto a otros	Entrevista con la gerencia para determinar acciones con respecto al proyecto
	O10	Fondos inadecuados o interrumpidos	Conseguir el aval del Sponsor y mostrar la posición estratégica del proyecto. Entender la posición estratégica del proyecto Conseguir una formalización de la prioridad del proyecto, respecto a otros	Entrevista con la gerencia para determinar acciones con respecto al proyecto
Externos	E1	Cambio del ambiente legal o regulatorio		Evaluar impacto y revisar el plan del proyecto
	E2	Cambio de prioridades del dueño		Evaluar impacto y revisar el plan del proyecto
	E3	Otros Riesgos: del país, clima, terremotos, inundaciones etc.		Evaluar impacto y revisar el plan del proyecto

Nota. Matriz de riesgos para la implementación del modelo C2M2.

Evaluada la respuesta al riesgo se procedió con el desarrollo del instrumento para los 10 dominios, en la figura 11 y 12 se presenta la evaluación de dominio de administración del riesgo y administración de inventario de activos así:

1. Establish Cybersecurity Risk Management		Self Evaluation Notes
a. There is a documented cybersecurity risk management strategy	Largely Implemented	El objetivo del Manual de seguridad de la información se establece que los lineamientos para velar por el cumplimiento son los principios de confidencialidad, integridad y disponibilidad aplicable a la información que se maneja al interior del Ministerio de Relaciones Exteriores y su Fondo Rotatorio, tanto en medio físico como magnético, los cuales se dictan como políticas de seguridad de la información. Adicionalmente la Resolución 7035 El Ministerio de Relaciones Exteriores crea el comité de TICs con el cual se informa sus funciones así: Apoyar la definición e implementación de los diferentes temas de seguridad de la información, aprobar las políticas de seguridad de la información y sus actualizaciones. revisión periódica del estado de seguridad de la información, realizar actividades de alto nivel en esta materia.
b. The strategy provides an approach for risk prioritization, including consideration of impact	Largely Implemented	Mediante el documento "MRE - Documento con la definición y descripción de la metodología de evaluación del riesgo.pdf" se formaliza la metodología de análisis y gestión de riesgos se seguridad de la información de MRE está basada en los principios de ISO 31000 y el modelo MAGERIT.
c. Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available	Largely Implemented	El documento "MRE - Documento con el Informe de evaluación de riesgos (RiskAssessment).pdf" contiene el detalle de los riesgos identificados y valorados conforme a la metodologia.
d. The risk management strategy is periodically updated to reflect the current threat environment	Largely Implemented	El documento "MRE - Documento con el plan de tratamiento del riesgo.pdf" contiene los planes de tratamiento de los riesgos identificados.
e. An organization-specific risk taxonomy is documented and is used in risk management activities	Largely Implemented	El documento "MRE - Documento con el plan de tratamiento del riesgo.pdf" contiene los planes de tratamiento de los riesgos identificados.

Figura 18. Evaluación Dominio Administración del Riesgo.
Nota. Evaluación de la herramienta C2M2 para el dominio 1 Gestión del Riesgo

		Self Evaluation Notes
1. Manage Asset Inventory		
a. There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc	Fully Implemented	Pagina web: http://www.cancilleria.gov.co/transparencia-acceso-informacion-publica-0 item: 10.3 Índice de Información Clasificada y Reservada
b. There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data); management of the inventory may be ad hoc	Largely Implemented	Pagina web: http://www.cancilleria.gov.co/transparencia-acceso-informacion-publica-0 item: 10.3 Índice de Información Clasificada y Reservada
c. Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards)	Fully Implemented	Pagina web: http://www.cancilleria.gov.co/transparencia-acceso-informacion-publica-0 item: 10.3 Índice de Información Clasificada y Reservada
d. Inventoried assets are prioritized based on their importance to the delivery of the function	Fully Implemented	Pagina web: http://www.cancilleria.gov.co/transparencia-acceso-informacion-publica-0 item: 10.3 Índice de Información Clasificada y Reservada
e. There is an inventory for all connected IT and OT assets related to the delivery of the function	Largely Implemented	Pagina web: http://www.cancilleria.gov.co/transparencia-acceso-informacion-publica-0 item: 10.3 Índice de Información Clasificada y Reservada
f. The asset inventory is current (as defined by the organization)	Fully Implemented	Pagina web: http://www.cancilleria.gov.co/transparencia-acceso-informacion-publica-0 item: 10.3 Índice de Información Clasificada y Reservada
2. Manage Asset Configuration		
a. Configuration baselines are established, at least in an ad hoc manner, for inventoried assets where it is desirable to ensure that multiple assets are	Largely Implemented	GESTION DE CONFIGURACION Y ACTIVOS DE LOS SERVICIOS DE TI. https://sigc.cancilleria.gov.co
b. Configuration baselines are used, at least in an ad hoc manner, to configure assets at deployment	Largely Implemented	GESTION DE CONFIGURACION Y ACTIVOS DE LOS SERVICIOS DE TI. https://sigc.cancilleria.gov.co

Figura 19. Evaluación Dominio Administración inventario de activos.
Nota. Evaluación de la herramienta C2M2 para el dominio 2 Gestión de Inventario de Activos.

Se realizó la evaluación de los 10 dominios y por último se procedió con la generación del reporte, el cual se anexa en el Apéndice No. 2.

De acuerdo al informe de evaluación es importante resaltar el resumen que se muestra en la Figura 13, en el cual se evidencia una constante en los diez dominios, para los 3 niveles de madurez, en que la cancillería se encuentra en general en un nivel de madurez largamente implementado y totalmente implementado para la mayoría de los dominios, aunque en el dominio IR- Respuesta a eventos e incidentes y continuidad de operaciones, en el nivel 3 de madurez MIL3, se encuentran componentes-que están en nivel parcialmente implementados.

Para claridad en la revisión del informe es importante tener en cuenta las abreviaciones de los 10 dominios del modelo C2M2, como se detalla a continuación:

1. Administración del riesgo: RM
2. Gestión de Activos, Cambios y Configuración: (ACM)
3. Gestión de Identidad y Acceso: (IAM)
4. Gestión de vulnerabilidades y amenazas: (TVM)
5. Conciencia Situacional. (SA)
6. Compartir información y comunicaciones. (ISC)
7. Respuesta a eventos e incidentes y continuidad de operaciones. (IR)
8. Gestión de Cadena de Suministro y Dependencias Externas. (EDM)
9. Administración del Personal. (WM)
10. Programa de administración de ciberseguridad. (CPM)

3. SUMMARY OF RESULTS BY DOMAIN

The ONG-C2M2 includes 10 domains, or logical groupings of cybersecurity practices. A description of the each domain is provided in Section 2.1. *Domains*. This section provides a summary of MIL scores and answer input by MIL for each of the 10 domains included in the ONG-C2M2. See Appendix A: *Evaluation Scoring Process* for a detailed explanation of the scoring process and Section 5. *Using the Evaluation* Results for further detail regarding interpretation of evaluation results.

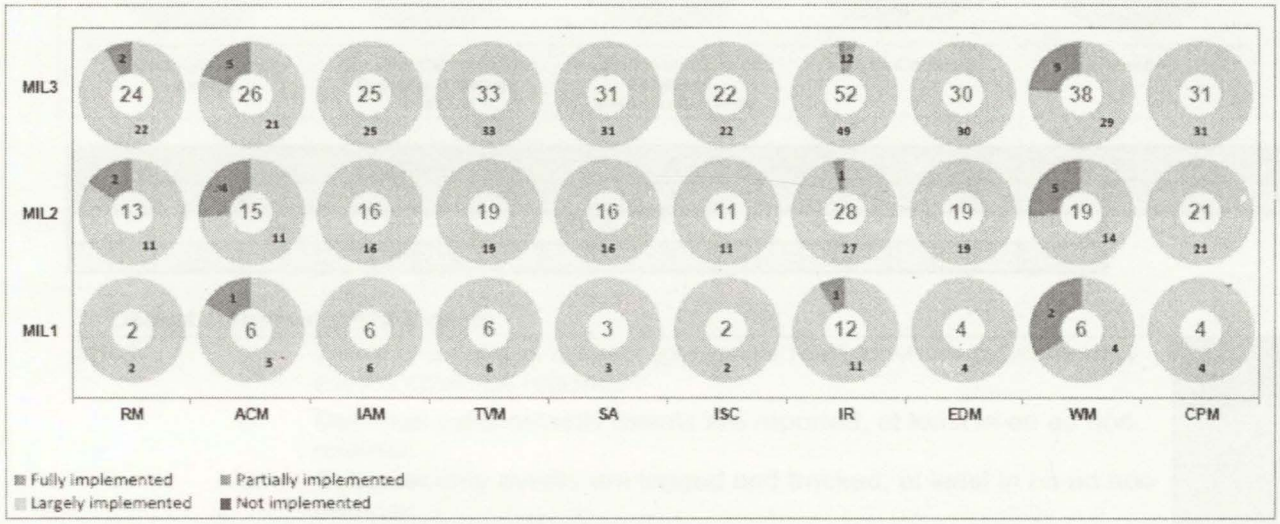
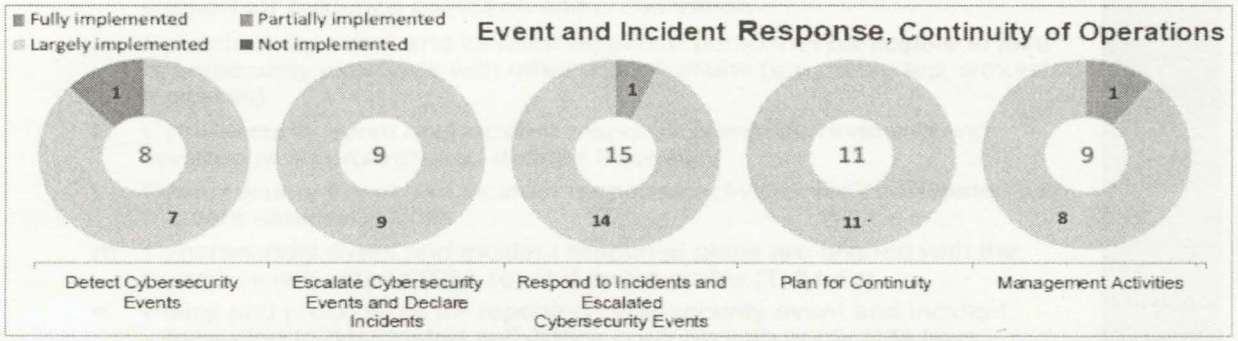


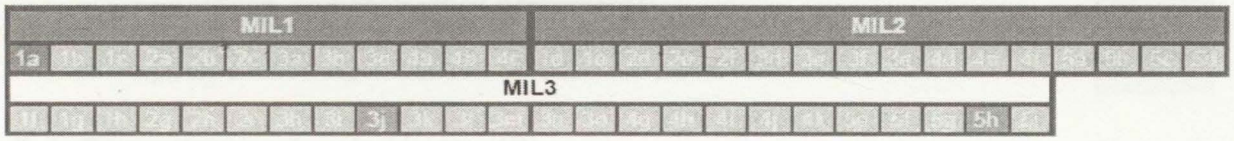
Figura 20. Resumen evaluación modelo C2M2 cancillería.
Nota. Resumen del resultado de la evaluación de la herramienta C2M2

Es así como se enfatiza en detalle el informe de este dominio, representado en las Figuras de la 14 a la 16:

4.7 Event and Incident Response, Continuity of Operations

Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.





1. Detect Cybersecurity Events

MIL1	a.	There is a point of contact (person or role) to whom cybersecurity events could be reported	FI
	b.	Detected cybersecurity events are reported, at least in an ad hoc manner	LI
	c.	Cybersecurity events are logged and tracked, at least in an ad hoc manner	LI
MIL2	d.	Criteria are established for cybersecurity event detection (e.g., what constitutes an event, where to look for events)	LI
	e.	There is a repository where cybersecurity events are logged based on the established criteria	LI
MIL3	f.	Event information is correlated to support incident analysis by identifying patterns, trends, and other common features	LI
	g.	Cybersecurity event detection activities are adjusted based on information from the organization's risk register (RM-2j) and threat profile (TVM-1d) to help detect known threats and monitor for identified risks	LI
	h.	The common operating picture for the function is monitored to support the identification of cybersecurity events (SA-3a)	LI

Figura 21. Detallado dominio Respuesta a eventos e incidentes (IR), continuidad de operaciones.
Nota. Resumen del resultado de la evaluación de la herramienta C2M2.

3. Respond to Incidents and Escalated Cybersecurity Events (continued)		
MIL3	h. Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken	U
	i. Cybersecurity event and incident responses are coordinated with law enforcement and other government entities as appropriate, including support for evidence collection and preservation	U
	j. Cybersecurity event and incident response personnel participate in joint cybersecurity exercises with other organizations (e.g., table top, simulated incidents)	PI
	k. Cybersecurity event and incident response plans are reviewed and updated at an organization-defined frequency	U
	l. Cybersecurity event and incident response activities are coordinated with relevant external entities	U
	m. Cybersecurity event and incident response plans are aligned with the function's risk criteria (RM-1c) and threat profile (TVM-1d)	U
	n. Policy and procedures for reporting cybersecurity event and incident information to designated authorities conform with applicable laws, regulations, and contractual agreements	U
	o. Restored assets are configured appropriately and inventory information is updated following execution of response plans	U

Figura 22. Detallado Respuesta a eventos e incidentes. (IR).
Nota. Resumen del resultado de la evaluación de la herramienta C2M2.

De acuerdo con el objetivo 3 en el nivel MIL3, numeral J: Respuesta a eventos e incidentes de ciberseguridad, el evento de ciberseguridad y el personal de respuesta a incidentes participan en ejercicios conjuntos de seguridad cibernética con otras organizaciones, se encuentra en estado parcialmente implementado.

5. Management Activities		
MIL1	*No practice at MIL1*	
MIL2	a. Documented practices are followed for cybersecurity event and incident response as well as continuity of operations activities	L
	b. Stakeholders for cybersecurity event and incident response as well as continuity of operations activities are identified and involved	L
	c. Adequate resources (people, funding, and tools) are provided to support cybersecurity event and incident response as well as continuity of operations activities	L
	d. Standards and/or guidelines have been identified to inform cybersecurity event and incident response as well as continuity of operations activities	L
MIL3	e. Cybersecurity event and incident response as well as continuity of operations activities are guided by documented policies or other organizational directives	L
	f. Cybersecurity event and incident response as well as continuity of operations policies include compliance requirements for specified standards and/or guidelines	L
	g. Cybersecurity event and incident response as well as continuity of operations activities are periodically reviewed to ensure conformance with policy	L
	h. Responsibility and authority for the performance of cybersecurity event and incident response as well as continuity of operations activities are assigned to personnel	PI
	i. Personnel performing cybersecurity event and incident response as well as continuity of operations activities have the skills and knowledge needed to perform their assigned responsibilities	L

Figura 23. Detallado Actividades de administración.
Nota. Resumen del resultado de la evaluación de la herramienta C2M2.

Igualmente, en el objetivo No. 5. MIL 3, numeral i: Actividades de administración, la responsabilidad y autoridad para el desempeño del evento de ciberseguridad y la respuesta a incidentes, así como la continuidad de las actividades de operaciones, se asignan al personal, se encuentra en estado parcialmente implementado.

4.4 Definición del Plan de Acción a implementar.

De acuerdo con C2M2, el dominio número 10 está enfocado en establecer y mantener un programa de ciberseguridad empresarial que proporcione gobernabilidad, planificación estratégica y patrocinio para las actividades de ciberseguridad de la organización, de una manera que alinee los objetivos de ciberseguridad con los objetivos estratégicos de la organización y el riesgo a la infraestructura crítica.

Actualmente la cancillería cuenta con un programa de ciberseguridad y de acuerdo con el resultado del instrumento del modelo C2M2, hay que fortalecer dos objetivos el objetivo 3 en el nivel MIL3, numeral J: Respuesta a eventos e incidentes de ciberseguridad y el objetivo No. 5. MIL 3, numeral i: Actividades de administración, la responsabilidad y autoridad para el desempeño del evento de ciberseguridad y la respuesta a incidentes, así como la continuidad de las actividades de operaciones todo dentro de un proceso de mejora continua.

A continuación, se presenta el plan de acción propuesto:

Tabla 15

Plan de acción de ciberseguridad 2018.

1	Elaborar plan de sensibilización (4 fases)
2	Implementar plan de sensibilización (4 fases)

3	Boletines de ciberseguridad actualizados y promoción de los mismos, en diferentes mecanismos tales como carteleras virtuales, pendones e intranet.
3	Trabajar en conjunto con el CSIRT de Mintic, para compartir experiencias y apoyo en la gestión del incidentes y vulnerabilidades
4	Auditorías internas en el cumplimiento de las políticas de seguridad y privacidad de la información
5	Mejora continua en los 10 dominios del modelo C2M2
6	Certificación de 4 procesos de la entidad en la ISO 21000:2013
5	Capacitación al personal de seguridad de la información
6	Reforzar el cumplimiento de políticas de cifrado de dispositivos móviles, en apoyo con el nivel directivo.
7	Reforzar el cumplimiento de políticas de cifrado de portátiles, en apoyo con el nivel directivo.
8	Reforzar el cumplimiento de políticas cifrado de correo, en apoyo con el nivel directivo.
9	Cumplir con los indicadores de ciberseguridad establecidos

Nota. Plan de acción a implementar en el Programa de Ciberseguridad y Ciberdefensa en el año 2018

Es importante resaltar que este plan será presentado en comité Directivo para su aprobación y ejecución dentro del plan de acción 2018.

Conclusiones

Es importante concluir la importancia para el Ministerio de Relaciones Exteriores en cumplimiento de sus objetivos estratégicos y como responsable del numeral 5.1 de la Política Nacional de Seguridad Digital, cumplir con el programa de ciberdefensa y de ciberseguridad, implementado, mantener una monitorización constante sobre las actividades que adelanten los usuarios de la cancillería y sus stakeholders, planeando acciones que impidan o minimicen la afectación de su información sensible, sus redes de telecomunicaciones o su infraestructura.

Así mismo, identificar vulnerabilidades inherentes a las tecnologías utilizadas, o que puedan ser explotadas por usuarios internos o externos y la importancia de contar con un análisis de líneas de acción estructurado y desarrollado.

Igualmente teniendo en cuenta que el eslabón más débil para la entidad, es el usuario final, es relevante contar con un programa de concienciación, que de manera gradual y de forma sencilla, permita motivar y hacer conscientes a los usuarios de la importancia de cada uno en el buen manejo y uso de la información. Sí se logra mejorar en este aspecto, la Cancillería tendrá una muy alta probabilidad de minimizar los riesgos cibernéticos y que el programa de ciberseguridad de la entidad sea exitoso. Para lo anterior es imprescindible contar con el apoyo del nivel directivo en el cumplimiento del programa de ciberseguridad establecido.

Y por último analizado el cuestionamiento de sí está preparada la Cancillería para identificar posibles peligros en la entidad frente a su infraestructura y manejo de la información sensible, evitarlos y saber cómo reaccionar ante alguna eventualidad, fortaleciendo a la entidad y las Misiones en el exterior en procesos y habilidades en Ciberseguridad y Ciberdefensa, con base en el modelo propuesto, según el modelo C2M2, la entidad se encuentra en un nivel largamente implementado, es importante seguir en un proceso de mejora continua, monitoreando el programa y auditando el mismo, para garantizar que se actualice en caso de requerirlo y lo más importante dar estricto cumplimiento al mismo, incluyendo al cuerpo directivo.

Referencias

Banco Interamericano de Desarrollo (BID). y Organización de los Estados Americanos (OEA). (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? https://publications.iadb.org/handle/11319/7449?locale-attribute=es.

Berkeley Research Group. (2016). Cybersecurity Preparedness, Benchmarking study report. Recuperado de http://www.thinkbrg.com/expertisecybersecurity-preparedness-benchmarkingstudy.html.

Departamento de Energía de los Estados Unidos de America (2014). CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2). EE. UU Recuperado de https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf.

Departamento Nacional de Planeación (2011). Documento CONPES 3701, Lineamientos de política para la Ciberseguridad y Ciberdefensa. Bogotá, D.C. Recuperado de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.

Departamento Nacional de Planeación (2016) Documento CONPES 3854, Política nacional de seguridad digital. Bogotá D.C. Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

Miron, W. y Muita, K. (2014). Cybersecurity Capability Maturity Models for Providers of Critical Infraestructure. Recuperado de https://timreview.ca/article/837.

Ministerio de Tecnologías de la Información y Comunicaciones. (2016). Modelo de Seguridad y Privacidad de la Información (MSPI). Recuperado de http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html.

National Institute of Standards and Technology NIST. (2017). Infrastructure Cybersecurity Draft Version 1.1. Recuperado de https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.1-with-markup1.pdf

Planeación Estratégica Ministerio de Relaciones Exteriores y su Fondo Rotatorio, Cancillería, (2017). Recuperado de: http://www.cancilleria.gov.co/ministerio/mision_vision_objetivos_normas_principios_lineamientos#8.

.

Bibliografía consultada

Blog de Internet Security Auditors (2016) Guía rápida para entender el marco de trabajo de ciberseguridad del NIST Recuperado de http://blog.isecauditors.com/2016/12/guia-rapida-para-entender-marco-trabajo-de-ciberseguridad-del-NIST.html

Chapin, D. y Akridge, S. (2005). ¿Cómo Puede Medirse la Seguridad? Recuperado de http://www.iso27000.es/download/HowCanSecurityBeMeasured-SP.pdf.

Departamento Nacional de Planeación. (2014). Bases del Plan Nacional de Desarrollo, Todos por un nuevo País. Bogotá. D.C. Recuperado de https://www.minagricultura.gov.co/planeacion-control-gestion/Gestin/Plan%20de%20Acci%C3%B3n/PLAN%20NACIONAL%20DE%20DESARROLLO%202014%20-%202018%20TODOS%20POR%20UN%20NUEVO%20PAIS.pdf.

Endsley, M.R., (2000). Theoretical underpinnings of situation awareness: A critical review. In M. R. Endsley and D. J. Garland (Eds.), Situation Awareness Analysis and Measurement. Lawrence Erlbaum Associates.

ITIL (2011) Key facts on the update for Practitioners. Recuperado de https://www.isaca.org/groups/professional-english/itil/groupdocuments/edition_key_facts_for_practitioners_final.pdf

Pillitteri, V. (2015). C2M2 and the NIST Cyber Framework: Applying DOE's NIST Cyber Security Framework Guidance Recuperado de http://www.sgip.org/wp-content/uploads/SGIP_June18_Webinar_C2M2_powerpoint.pdf

Unión Internacional de Telecomunicaciones (UIT). (2014). La búsqueda de la confianza en el ciberespacio. Recuperado de http://www.itu.int/pub/S-GEN-WFS.02-1-2014/es.

Tablas y Figuras

1. Tablas

2. Figuras

Apéndice No. 1

Matriz de Riesgos C2M2 Cancillería

Identificación de Riesgos				Valoración del Riesgo						
				Cualitativo			Cuantitativo			
Categoría	**ID**	**Titulo**	**Tipo**	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Valor probabilidad**	**Valor del Impacto**	**Valor del Riesgo**	**Valor del Impacto**
Estrategicos	E 1	Cambio de prioridades de los directivos	Amenaza	Probable	Muy alto	**Inaceptable**	3	5	15	35
	E 2	No apoyo en la implementación del modelo a nivel directivo	Amenaza	Improbable	Muy alto	**Importante**	1	5	5	15
	E 3	Crear conciencia desde el nivel directivo	Oportunidad	Muy probable	Muy alto	**Inaceptable**	4	5	20	45
Comunicaciones	C 1	Falta de apoyo por los comunicadores en la campaña de expectativa del modelo	Amenaza	Poco Probable	Medio	**Moderado**	2	3	6	23

	C 3	Divulgación efectiva del Modelo a nivel institucional	Oportunidad	Muy probable	Muy alto	**Inaceptable**	4	5	20	45
Tecnológicos	T 1	No disponibilidad de recursos tecnológicos	Amenaza	Improbable	Alto	**Moderado**	1	4	4	14
	T 2	Asignación de nuevo proyectos a cargo del area de seguridad de la información	Amenaza	Poco Probable	Alto	**Importante**	2	4	8	24
	T 3	Cumplimiento de los lineamientos de Mintic	Oportunidad	Muy probable	Muy alto	**Inaceptable**	4	5	20	45
Politica Exterior	P 1	Falta de apoyo del comité que formula la ley de ciberdelitos	Amenaza	Improbable	Muy alto	**Importante**	1	5	5	15
	P 2	Insertar adecuadamente a Colombia en los ejes de integración en ciberseguridad	Oportunidad	Muy probable	Muy alto	**Inaceptable**	4	5	45	45
Administrativos	A 1	Falta de apoyo en la creación del modelo	Amenaza	Poco Probable	Alto	**Importante**	2	4	24	24

	A 2	Roles y Responsabilidades mal definidos	Amenaza	Poco Probable	Medio	**Moderado**	2	3	23	23
	A 3	No cumplimiento del cronograma	Amenaza	Poco Probable	Medio	**Moderado**	2	3	23	23
	A 4	Fondos insuficientes	Amenaza	Poco Probable	Medio	**Moderado**	2	3	23	23
Cultura Organizacional	O 1	Ocultación de la información	Amenaza	Improbable	Alto	**Moderado**	1	4	14	14
	O 2	Falta de ompromiso de los directivos	Amenaza	Improbable	Muy alto	**Importante**	1	5	15	15
	O 3	Objetivos de tiempo inconsistente	Amenaza	Improbable	Alto	**Moderado**	1	4	14	14
	O 4	Objetivos de costos inconsistente	Amenaza	Improbable	Alto	**Moderado**	1	4	14	14
	O 5	Objetivos de alcance inconsistente	Amenaza	Improbable	Alto	**Moderado**	1	4	14	14
	O 6	Resistencia al Cambio	Amenaza	Probable	Alto	**Inaceptable**	3	4	34	34
	O 7	Crear conciencia a todos los usuarios	Oportunidad	Probable	Alto	**Inaceptable**	3	4	34	34

Recursos	R 1	Deficiencia en la asignación de personal	Amenaza	Poco Probable	Medio	**Moderado**	2	3	23	23
	R 2	Deficiencias en las Habilidades del personal	Amenaza	Probable	Medio	**Importante**	3	3	33	33
	R 3	No Disponibilidad de algún Bien o Servicio	Amenaza	Poco Probable	Bajo	**Tolerable**	2	2	22	22
	R 4	Conflictos de recursos con otras responsabilidades	Amenaza	Poco Probable	Bajo	**Tolerable**	2	2	22	22

Respuesta al Riesgo

Identificación de Riesgos				Respuesta al Riesgo				
Categoría	**ID**	**Titulo**	**Tipo**	**Estrategia**	**Acciones de Respuesta**	**Dueño del riesgo**	**Duración estimada**	**Recursos Especiales**

Estrategicos	E1	Cambio de prioridades de los directivos	Amenaza	Mitigar	Incentivar una campaña fuerte de concientización en las misiones en el exterior y el cumplimiento del modelo C2M2	Oficial de Seguridad de la Información	1 año	El costo se estima en horas ingeniero de dedicación, mínimo 2 horas 3 días a la semana, una vez al mes durante 1 año. Así mismos videos publicados en la intranet, boletines y apoyo a nivel directivo en el cumplimiento del modelo a nivel institucional (Recursos con los que actualmente cuenta la entidad)
	E2	No apoyo en la implementación del modelo a nivel directivo	Amenaza	Mitigar	Lograr la aprobación de la implementación del modelo en el comité directivo	Oficial de Seguridad de la Información	3 meses	Los comités directivos se realizan trimestralmente
	E3	Crear conciencia desde el nivel directivo	Oportunidad	Mejorar	Incentivar a nivel directivo la continuidad y la importancia del apoyo en la aplicación del modelo	Oficial de Seguridad de la Información	3 meses	Los comités directivos se realizan trimestralmente
Comunicaciones	C1	Falta de apoyo por los comunicadores en la campaña de expectativa del modelo	Amenaza	Mitigar	En el comité directivo lograr el apoyo de la Jefe de Prensa	Oficial de Seguridad de la Información	3 meses	Los comités directivos se realizan trimestralmente
	C3	Divulgación efectiva del Modelo a nivel institucional	Oportunidad	Mejorar	Realizar camapañas frecuentes y transferencia de conocimiento en la Intranet de a implementación del modelo	Oficial de Seguridad de la Información	6meses	Iniciar con una campaña de expectativa y luego reforzando la importancia de aplicación y cumplimiento del mismo
Tecnológicos	T1	No disponibilidad de recursos tecnológicos	Amenaza	Mitigar	Incluirlos en el plan de compras	Oficial de Seguridad de la Información	1 año	Incluirlo en el plan de compras para adquisición en el 2018

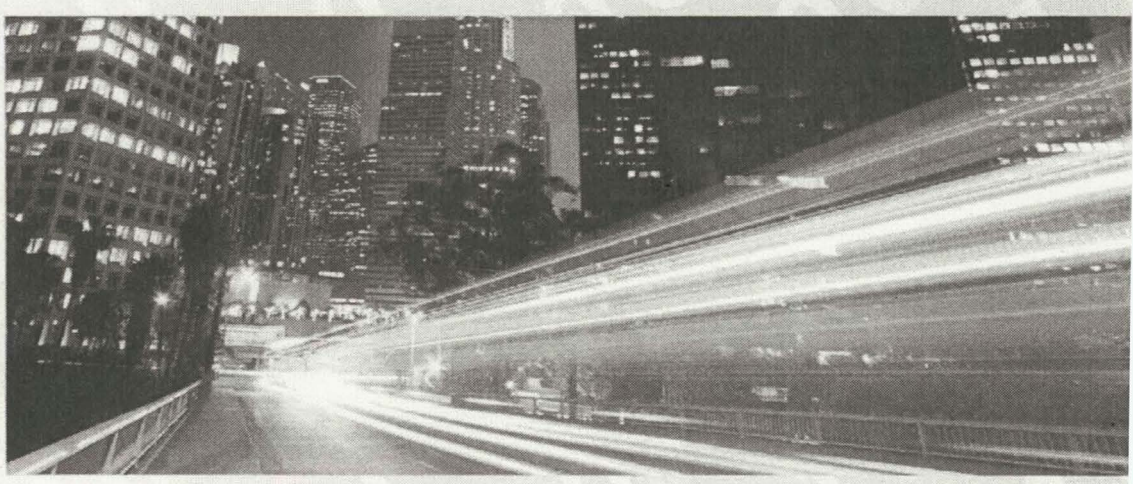
	T2	Asignación de nuevo proyectos a cargo del area de seguridad de la información	Amenaza	Mitigar	Establecer priorización de proyectos, dandeole prioridad alta a este proyecto, solicitud de un ingeniero adicional.	Directora de Gestión de Informción y Tecnología	1 año	Asignación de recursos adicionales al área de seguridad
	T3	Cumplimiento de los lineamientos de Mintic	Oportunidad	Mejorar	Incentivar la implementación del modelo, para dar cumplimiento a los lineamientos de Mintic	Oficial de Seguridad de la Información	3 meses	Los comités directivos se realizan trimestralmente
Politica Exterior	P1	Falta de apoyo del comité que formula la ley de ciberdelitos	Amenaza	Mitigar	Lograr la aprobación de la implementación del modelo por el grupo de politica exterior, que aprueba la ley de ciberdelito a nivel Cancillería	Oficial de Seguridad de la Información	3 meses	Los comités directivos se realizan trimestralmente
	P2	Insertar adecuadamente a Colombia en los ejes de integración en ciberseguridad	Oportunidad	Mejorar	Cumplimiento de los objetivos dde implementación del modelo	Oficial de Seguridad de la Información	1 año	
Administrativos	A1	Falta de apoyo en la creación del modelo	Amenaza	Mitigar	Lograr la aprobación de la implementación del modelo en el comité directivo	Oficial de Seguridad de la Información	3 meses	Los comités directivos se realizan trimestralmente
	A2	Roles y Responsabilidades mal definidos	Amenaza	Mitigar	Reasignar responsabilidades al personal encragado del proyecto	Directora de Talento Humano	3 meses	Contratar personal nuevo y exclusivo para el cumplimiento

	A3	No cumplimiento del cronograma	Amenaza	Mitigar				
	A4	Fondos insuficientes	Amenaza	Mitigar				
Cultura Organizacional	O1	Ocultación de la información	Amenaza	Mitigar				
	O2	Falta de ompromiso de los directivos	Amenaza	Mitigar	Lograr la aprobación de la implementación del modelo en el comité directivo	Oficial de Seguridad de la Información	3 meses	Los comités directivos se realizan trimestralmente
	O3	Objetivos de tiempo inconsistente	Amenaza	Mitigar				
	O4	Objetivos de costos inconsistente	Amenaza	Mitigar				
	O5	Objetivos de alcance inconsistente	Amenaza	Mitigar				
	O6	Resistencia al Cambio	Amenaza	Mitigar	Impartir capacitación y sensibilización para el equipo de trabajo. Realizar una Gestión del Cambio humana formal y detallada con objetivos del proyecto, apoyado por Talento Humano.	Oficial de Seguridad de la Información	6 meses	Programación de capacitaciones y campañas de sensibilización, apoyados con la Dirección de talento Humano.
	O7	Crear conciencia a todos los usuarios	Oportunidad	Mejorar	Impartir capacitaciones y campañas de sencibilización	Oficial de Seguridad de la Información	1 año	Videos, boletines, Intranet, correo institucional
Recursos	R1	Deficiencia en la asignación de personal	Amenaza	Mitigar	Reasignar responsabilidades al personal encragado del proyecto	Directora de Talento Humano	3 meses	Contratar personal nuevo y exclusivo para el cumplimiento

	R2	Deficiencias en las Habilidades del personal	Amenaza	Mitigar	Realizar la capacitación de acuerdo a las habilidades requeridas	Oficial de Seguridad de la Información	3 meses	Cursos en centros especializados
	R3	No Disponibilidad de algún Bien o Servicio	Amenaza	Aceptar	Adquirir el bien o servicio que pudiese requerirse	Oficial de Seguridad de la Información	1 año	Incluirlo en el plan de compras para adquisición en el 2018
	R4	Conflictos de recursos con otras responsabilidades	Amenaza	Aceptar	Reasignar responsabilidades al personal encargado del proyecto	Directora de Talento Humano	3 meses	Contratar personal nuevo y exclusivo para el cumplimiento

Apéndice No. 2

MINISTERIO DE RELACIONES EXTERIORES
CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)



Evaluation
Scoring Report
Version 1.1a

Agosto 16, 2017

CANCILLERÍA

TODOS POR UN NUEVO PAÍS
PAZ · EQUIDAD · EDUCACIÓN

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

NOTIFICATION

This report is provided "as is" for informational purposes only. The Department of Energy (DOE) and the Department of Homeland Security (DHS) do 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 and DHS do 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 and DHS official seals 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 Departments. The DOE and DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DOE, DHS, or the United States Government. Use of the DOE and DHS seals without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DOE and DHS policies governing usage of their seals.

1. INTRODUCTION

This report represents the results of an evaluation using the Oil & Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2). The ONG-C2M2 evaluation is designed to assist organizations in identifying specific areas to strengthen their cybersecurity program, prioritize cybersecurity actions and investments, and maintain the desired level of security throughout the IT systems life cycle.

The scope defined for this evaluation includes the following:

visión para 2018, colombia consolidará y fortalecerá las relaciones bilaterales y multilaterales, con el fin de contribuir a la paz, la equidad y la educación, y fortalecerá la relación con los connacionales a través de la prestación de un servicio eficiente y efectivo. objetivos:

1. diversificar la agenda de política exterior hacia sectores ejes del desarrollo nacional, fortaleciendo las relaciones bilaterales y velando por el cumplimiento de los compromisos adquiridos.
2. promover y consolidar la presencia y posicionamiento de colombia en instancias globales, multilaterales, regionales y subregionales para la defensa y promoción de los intereses nacionales.
3. fortalecer la política migratoria, la gestión consular y el servicio al ciudadano.
4. impulsar el desarrollo social y económico de las regiones de frontera, su integración con los países vecinos y velar por la soberanía territorial.
5. fortalecer institucionalmente el ministerio de relaciones exteriores y su fondo rotatorio.
6. consolidar y orientar la oferta y la demanda de cooperación internacional en función de los objetivos de política exterior que sirvan a los intereses fundamentales del país.
7. implementar y fortalecer herramientas y modelos que permitan mejorar la eficacia, eficiencia y efectividad del sistema integral de gestión.
8. desarrollar y fortalecer las habilidades, aptitudes y conocimientos del talento humano.

fuente:
http://www.cancilleria.gov.co/ministerio/mision_vision_objetivos_normas_principios_lineamientos

The results presented in this report are based on participant responses to ONG-C2M2 Evaluation questions. For the purposes of this evaluation, responses to evaluation questions are considered valid

and accurate. The evaluation process did not include document reviews, observation of work, or an examination of security controls in place to support the evaluated function.

2. ONG-C2M2 ARCHITECTURE

The ONG-C2M2 arises from a combination of existing cybersecurity standards, frameworks, programs, and initiatives. The ONG-C2M2 provides flexible guidance to help organizations develop and improve their cybersecurity capabilities. As a result, the ONG-C2M2 practices tend to be at a high level of abstraction, so that they can be interpreted for organizations of various structures and sizes.
The ONG-C2M2 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 MIL. The following sections include additional information about the domains and the MILs.

2.1 Domains

Each of the ONG-C2M2's 10 domains contains a structured set of cybersecurity practices. Each set of practices represents the activities an organization can perform to establish and mature capability in the domain. For example, the Risk Management domain is a group of practices that an organization can perform to establish and mature cybersecurity risk management capability. For each domain, the ONG-C2M2 provides a purpose statement, which is a high-level summary of the intent of the domain. The purpose statement offers context for interpreting the practices in the domain. The practices within each domain are organized into objectives, which represent achievements that support the domain. For example, the Risk Management domain comprises three objectives:

- Establish Cybersecurity Risk Management Strategy
- Manage Cybersecurity Risk
- Management Practices

Each of the objectives in a domain comprises a set of practices, which are ordered by MIL. Figure 2.1 depicts the architecture of the ONG-C2M2.

MODEL STRUCTURE

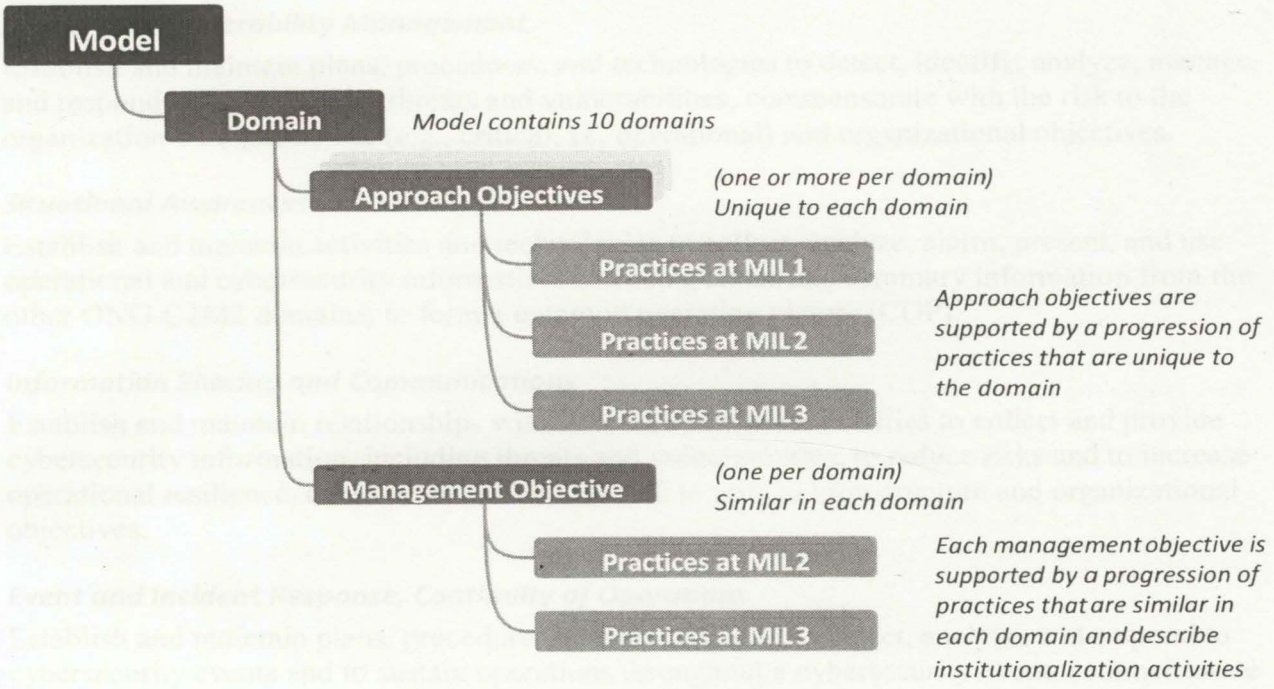


Figure 2.1: ONG-C2M2 Architecture

A brief description of the 10 domains follows in the order in which they appear in the ONGC2M2.

Risk Management

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

Asset, Change, and Configuration Management

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

Identity and Access Management

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.

Threat and Vulnerability Management

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 (e.g., critical, IT, operational) and organizational objectives.

Situational Awareness

Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other ONG-C2M2 domains, to form a common operating picture (COP).

Information Sharing and Communications

Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.

Event and Incident Response, Continuity of Operations

Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.

Supply Chain and External Dependencies Management

Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.

Workforce Management

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.

Cybersecurity Program Management

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 the organization's strategic objectives and the risk to critical infrastructure.

2.2 Maturity Indicator Levels

The ONG-C2M2 defines four maturity indicator levels, MIL0 through MIL3, which apply independently to each domain in the ONG-C2M2.
Four aspects of the MILs are important for understanding and applying the ONG-C2M2:

1. The maturity indicator levels apply independently to each domain. As a result, an organization using the ONG-C2M2 may be operating at different MIL ratings for different domains. For example, an organization could be operating at MIL1 in one domain, MIL2 in another domain, and MIL3 in a third domain.
2. The MILs 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(s). For example, an organization must perform all of the domain practices in MIL1 and MIL2 to achieve MIL2 in the domain. Similarly, the organization would have to perform all practices in MIL1, MIL2, and MIL3 to achieve MIL3.
3. Establishing a target MIL for each domain is an effective strategy for using the ONG-C2M2 to guide cybersecurity program improvement. Organizations should become familiar with the practices in the ONG-C2M2 prior to determining target MILs. Gap analysis activities and improvement efforts should then focus on achieving those target levels.
4. Practice performance and MIL achievement need to align with business objectives and the organization's cybersecurity strategy. Striving to achieve the highest MIL in all domains may not be optimal. Companies should evaluate the costs of achieving a specific MIL against potential benefits. However, the ONG-C2M2 was developed so that all companies, regardless of size, should be able to achieve MIL1 across all domains.

3. SUMMARY OF RESULTS BY DOMAIN

The ONG-C2M2 includes 10 domains, or logical groupings of cybersecurity practices. A description of the each domain is provided in Section 2.1. *Domains*. This section provides a summary of MIL scores and answer input by MIL for each of the 10 domains included in the ONG-C2M2. See Appendix A: *Evaluation Scoring Process* for a detailed explanation of the scoring process and Section 5. *Using the Evaluation* Results for further detail regarding interpretation of evaluation results.

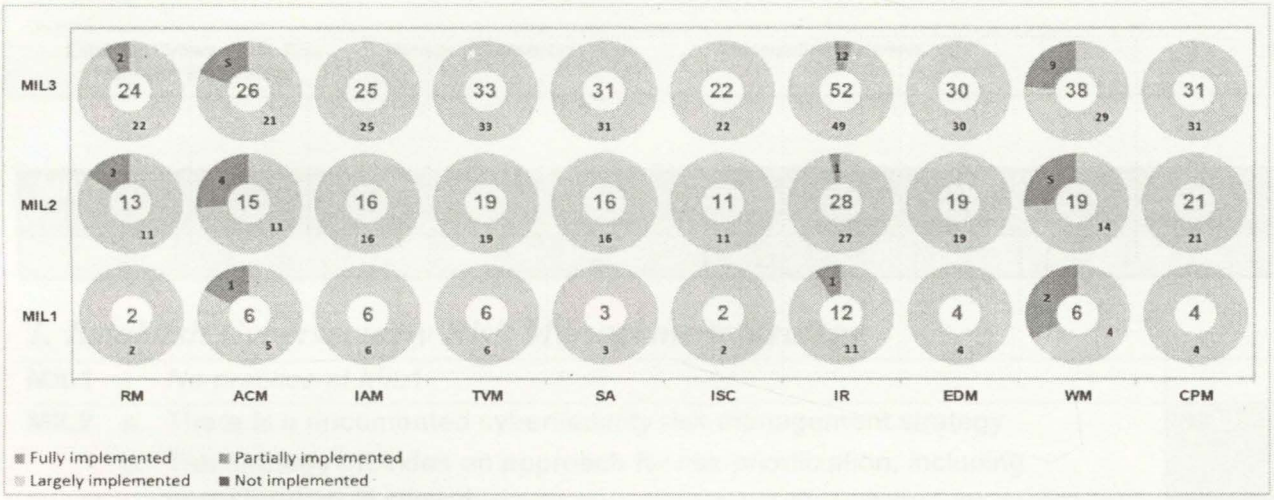


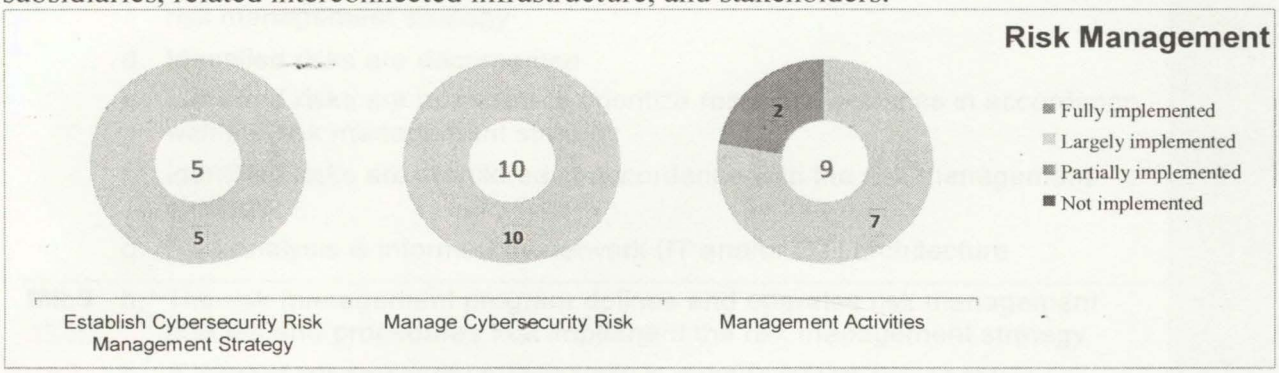
Figure 3.1: Summary of Answer Input by MIL and Domain

4. DETAILED EVALUATION RESULTS

This section provides the level of implementation (i.e., Fully Implemented, Largely Implemented, Partially Implemented, and Not Implemented) input to the Evaluation Survey for each ONG-C2M2 practice by domain, objective, and MIL. See Appendix A: *Evaluation Scoring Process* for a detailed explanation of the scoring process and Section 5. *Using the Evaluation* Results for further detail regarding evaluation results.

4.1 Risk Management

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



MIL1	MIL2											MIL3										
2a	2b	1a	1b	2c	2d	2e	2f	2g	3a	3b	3c	3d	1c	1d	1e	2h	2i	2j	3e	3f	3g	3h	3i

1. Establish Cybersecurity Risk Management Strategy

MIL1		*No practice at MIL1*	
MIL2	a.	There is a documented cybersecurity risk management strategy	LI
	b.	The strategy provides an approach for risk prioritization, including consideration of impact	LI
MIL3	c.	Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available	LI
	d.	The risk management strategy is periodically updated to reflect the current threat environment	LI
	e.	An organization-specific risk taxonomy is documented and is used in risk management activities	LI

MIL1	MIL2											MIL3										
2a	2b	1a	1b	2c	2d	2e	2f	2g	3a	3b	3c	3d	1c	1d	1e	2h	2i	2j	3e	3f	3g	3h	3i

2. Manage Cybersecurity Risk

MIL1			LI

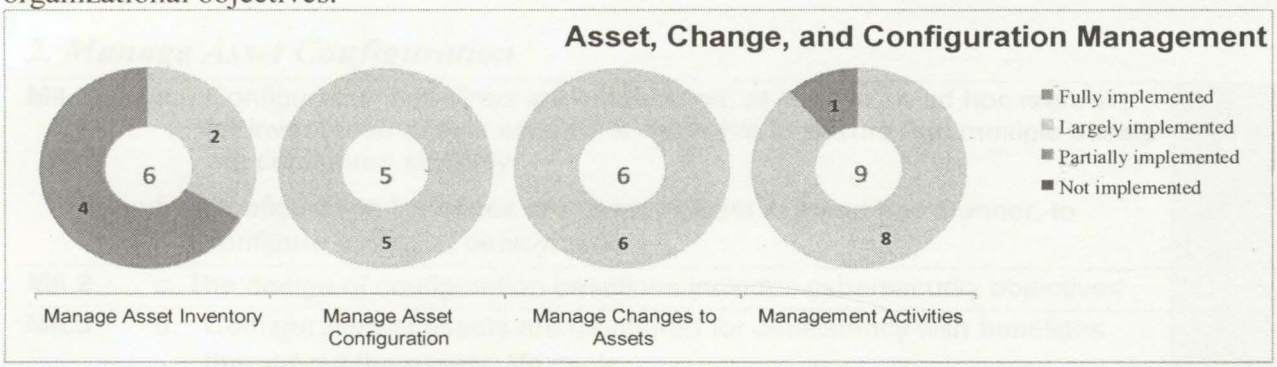
	a. Cybersecurity risks are identified, at least in an ad hoc manner	LI
	b. Identified risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner	
MIL2	c. Risk assessments are performed to identify risks in accordance with the risk management strategy	LI
	d. Identified risks are documented	LI
	e. Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy	LI
	f. Identified risks are monitored in accordance with the risk management strategy	LI
	g. Risk analysis is informed by network (IT and/or OT) architecture	LI
MIL3	h. The risk management program defines and operates risk management policies and procedures that implement the risk management strategy	LI
	i. A current cybersecurity architecture is used to inform risk analysis	LI
	j. A risk register (a structured repository of identified risks) is used to support risk management activities	LI

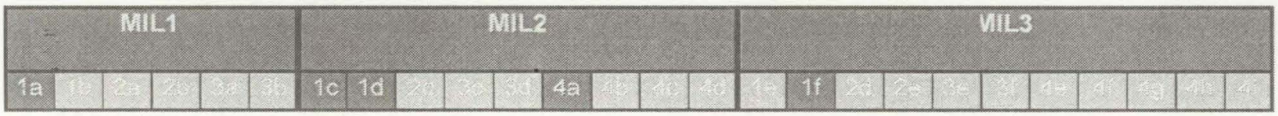
3. Management Activities

MIL1	*No practice at MIL1*	
MIL2	a. Documented practices are followed for risk management activities	FI
	b. Stakeholders for risk management activities are identified and involved	FI
	c. Adequate resources (people, funding, and tools) are provided to support risk management activities	LI
	d. Standards and/or guidelines have been identified to inform risk management activities	LI
MIL3	e. Risk management activities are guided by documented policies or other organizational directives	LI
	f. Risk management policies include compliance requirements for specified standards and/or guidelines	LI
	g. Risk management activities are periodically reviewed to ensure conformance with policy	LI
	h. Responsibility and authority for the performance of risk management activities are assigned to personnel	LI
	i. Personnel performing risk management activities have the skills and knowledge needed to perform their assigned responsibilities	LI

4.2 Asset, Change, and Configuration Management

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





1. Manage Asset Inventory

MIL1	a.	There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc	FI
	b.	There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data); management of the inventory may be ad hoc	LI
MIL2	c.	Inventory attributes include information to support the cybersecurity strategy (e.g., location, asset owner, applicable security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards)	FI
	d.	Inventoried assets are prioritized based on their importance to the delivery of the function	FI
MIL3	e.	There is an inventory for all connected IT and OT assets related to the delivery of the function	LI
	f.	The asset inventory is current (as defined by the organization)	FI

MIL1						MIL2									MIL3									
1a	1b	2a	2b	3a	3b	1c	1d	2c	3c	3d	4a	4b	4c	4d	1e	1f	2d	2e	3e	3f	4e	4f	4g	4h	4i

2. Manage Asset Configuration

MIL1	a. Configuration baselines are established, at least in an ad hoc manner, for inventoried assets where it is desirable to ensure that multiple assets are configured similarly	LI
	b. Configuration baselines are used, at least in an ad hoc manner, to configure assets at deployment	LI
MIL2	c. The design of configuration baselines includes cybersecurity objectives	LI
MIL3	d. Configuration of assets are monitored for consistency with baselines throughout the assets' life cycle	LI
	e. Configuration baselines are reviewed and updated at an organizationally-defined frequency	LI

3. Manage Changes to Assets

MIL1	a. Changes to inventoried assets are evaluated, at least in an ad hoc manner, before being implemented	LI
	b. Changes to inventoried assets are logged, at least in an ad hoc manner	LI
MIL2	c. Changes to assets are tested prior to being deployed, whenever possible	LI
	d. Change management practices address the full life cycle of assets (i.e., acquisition, deployment, operation, retirement)	LI
MIL3	e. Changes to assets are tested for cybersecurity impact prior to being deployed	LI
	f. Change logs include information about modifications that impact the cybersecurity requirements of assets (availability, integrity, confidentiality)	LI

MIL1						MIL2									MIL3									
1a	1b	2a	2b	3a	3b	1c	1d	2c	3c	3d	4a	4b	4c	4d	1e	1f	2d	2e	3e	3f	4e	4f	4g	4h	4i

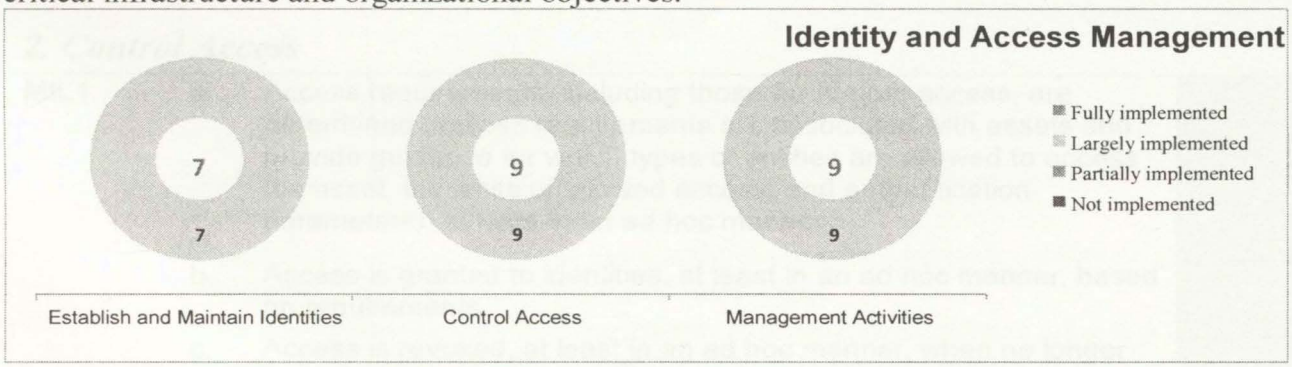
4. Management Activities

MIL1	*No practice at MIL1*	

MIL2	a.	Documented practices are followed for asset inventory, configuration, and change management activities	FI
	b.	Stakeholders for asset inventory, configuration, and change management activities are identified and involved	LI
	c.	Adequate resources (people, funding, and tools) are provided to support asset inventory, configuration, and change management activities	LI
	d.	Standards and/or guidelines have been identified to inform asset inventory, configuration, and change management activities	LI
MIL3	e.	Asset inventory, configuration, and change management activities are guided by documented policies or other organizational directives	LI
	f.	Asset inventory, configuration, and change management policies include compliance requirements for specified standards and/or guidelines	LI
	g.	Asset inventory, configuration, and change management activities are periodically reviewed to ensure conformance with policy	LI
	h.	Responsibility and authority for the performance of asset inventory, configuration, and change management activities are assigned to personnel	LI
	i.	Personnel performing asset inventory, configuration, and change management activities have the skills and knowledge needed to perform their assigned responsibilities	LI

4.3 Identity and Access Management

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.



MIL1						MIL2									MIL3								
1a	1b	1c	2a	2b	2c	1d	1e	1f	2d	2e	2f	3a	3b	3c	3d	1g	2g	2h	2i	3e	3f	3g	3h	3i

1. Establish and Maintain Identities

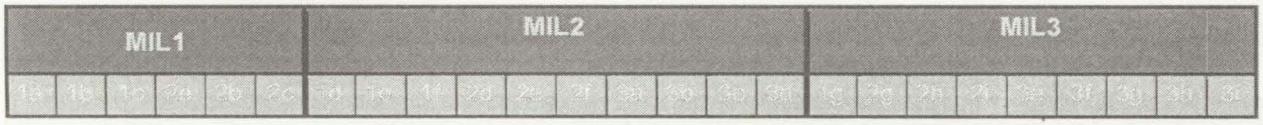
MIL1	a.	Identities are provisioned, at least in an ad hoc manner, for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities)	LI
	b.	Credentials are issued, at least in an ad hoc manner, for personnel and other entities who require access to assets (e.g., passwords, smart cards, certificates, keys)	LI
	c.	Identities are deprovisioned, at least in an ad hoc manner, when no longer required	LI
MIL2	d.	Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access)	LI
	e.	Credentials are periodically reviewed to ensure that they are associated with the correct person or entity	LI
	f.	Identities are deprovisioned within organizationally defined time thresholds when no longer required	LI
MIL3	g.	Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RM-1c)	LI

MIL1						MIL2									MIL3								
1a	1b	1c	2a	2b	2c	1d	1e	1f	2d	2e	2f	3a	3b	3c	3d	1g	2g	2h	2i	3e	3f	3g	3h	3i

2. Control Access

MIL1	a.	Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters), at least in an ad hoc manner	LI
	b.	Access is granted to identities, at least in an ad hoc manner, based on requirements	LI
	c.	Access is revoked, at least in an ad hoc manner, when no longer required	LI

MIL2	d.	Access requirements incorporate least privilege and separation of duties principles	LI
	e.	Access requests are reviewed and approved by the asset owner	LI
	f.	Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring	LI
MIL3	g.	Access privileges are reviewed and updated to ensure validity, at an organizationally defined frequency	LI
	h.	Access to assets is granted by the asset owner based on risk to the function	LI
	i.	Anomalous access attempts are monitored as indicators of cybersecurity events	LI

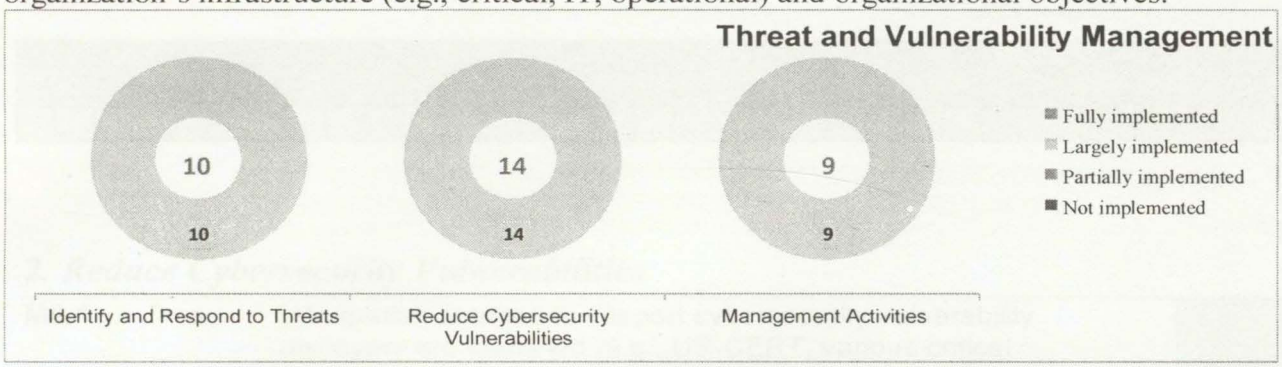


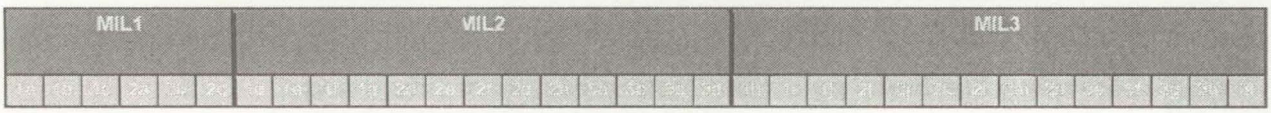
3. Management Activities

MIL1		*No practice at MIL1*	
MIL2	a.	Documented practices are followed to establish and maintain identities and control access	LI
	b.	Stakeholders for access and identity management activities are identified and involved	LI
	c.	Adequate resources (people, funding, and tools) are provided to support access and identity management activities	LI
	d.	Standards and/or guidelines have been identified to inform access and identity management activities	LI
MIL3	e.	Access and identity management activities are guided by documented policies or other organizational directives	LI
	f.	Access and identity management policies include compliance requirements for specified standards and/or guidelines	LI
	g.	Access and identity management activities are periodically reviewed to ensure conformance with policy	LI
	h.	Responsibility and authority for the performance of access and identity management activities are assigned to personnel	LI
	i.	Personnel performing access and identity management activities have the skills and knowledge needed to perform their assigned responsibilities	LI

4.4 Threat and Vulnerability Management

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 (e.g., critical, IT, operational) and organizational objectives.





1. Identify and Respond to Threats

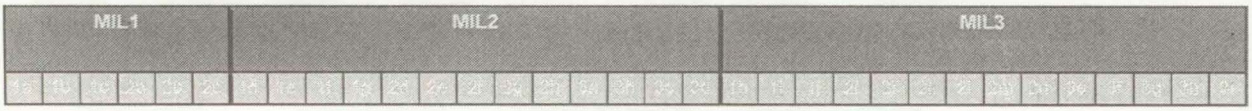
MIL1	a.	Information sources to support threat management activities are identified (e.g., US-CERT, various critical infrastructure sector ISACs, ICS-CERT, US-CERT, industry associations, vendors, federal briefings), at least in an ad hoc manner	LI
	b.	Cybersecurity threat information is gathered and interpreted for the function, at least in an ad hoc manner	LI
	c.	Threats that are considered important to the function are addressed (e.g., implement mitigating controls, monitor threat status), at least in an ad hoc manner	LI
MIL2	d.	A threat profile for the function is established that includes characterization of likely intent, capability, and target of threats to the function	LI
	e.	Threat information sources that address all components of the threat profile are prioritized and monitored	LI
	f.	Identified threats are analyzed and prioritized	LI
	g.	Threats are addressed according to the assigned priority	LI

MIL3	h.	The threat profile for the function is validated at an organizationdefined frequency	LI
	i.	Analysis and prioritization of threats are informed by the function's (or organization's) risk criteria (RM-1c)	LI
	j.	Threat information is added to the risk register (RM-2j)	LI

2. Reduce Cybersecurity Vulnerabilities

MIL1	a.	Information sources to support cybersecurity vulnerability discovery are identified (e.g., US-CERT, various critical infrastructure sector ISACs, ICS-CERT, industry associations, vendors, federal briefings, internal assessments), at least in an ad hoc manner	LI
	b.	Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner	LI
	c.	Cybersecurity vulnerabilities that are considered important to the function are addressed (e.g., implement mitigating controls, apply cybersecurity patches), at least in an ad hoc manner	LI
MIL2	d.	Cybersecurity vulnerability information sources that address all assets important to the function are monitored	LI
	e.	Cybersecurity vulnerability assessments are performed (e.g., architectural reviews, penetration testing, cybersecurity exercises, vulnerability identification tools)	LI
	f.	Identified cybersecurity vulnerabilities are analyzed and prioritized (e.g., Forum of Incident Response and Security Teams (FIRST) Common Vulnerability Scoring System (CVSS) could be used for patches; internal guidelines could be used to prioritize other types of vulnerabilities)	LI
	g.	Cybersecurity vulnerabilities are addressed according to the assigned priority	LI
	h.	Operational impact to the function is evaluated prior to deploying cybersecurity patches	LI

MIL3	i.	Cybersecurity vulnerability assessments are performed for all assets important to the delivery of the function, at an organizationdefined frequency	LI
	j.	Cybersecurity vulnerability assessments are informed by the function's (or organization's) risk criteria (RM-1c)	LI
	k.	Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of the function	LI
	l.	Analysis and prioritization of cybersecurity vulnerabilities are informed by the function's (or organization's) risk criteria (RM-1c)	LI
	m.	Cybersecurity vulnerability information is added to the risk register (RM-2j)	LI
	n.	Risk monitoring activities validate the responses to cybersecurity vulnerabilities (e.g., deployment of patches or other activities)	LI



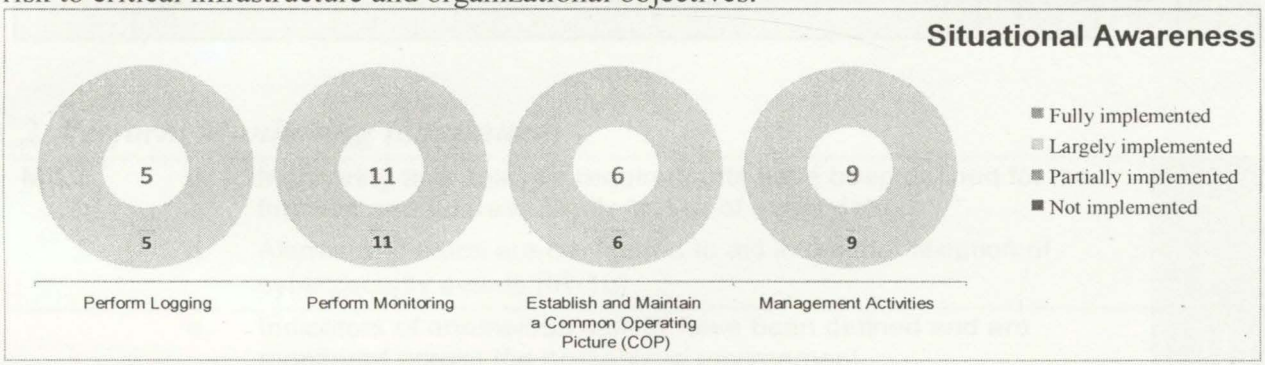
3. Management Activities

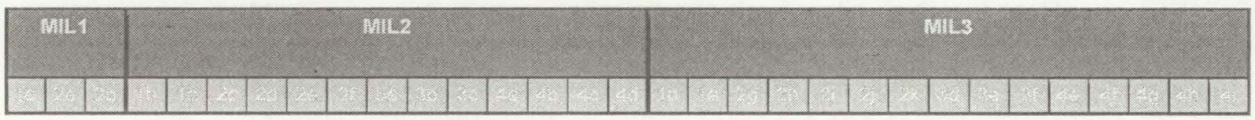
MIL1		*No practice at MIL1*	
MIL2	a.	Documented practices are followed for threat and vulnerability management activities	LI
	b.	Stakeholders for threat and vulnerability management activities are identified and involved	LI
	c.	Adequate resources (people, funding, and tools) are provided to support threat and vulnerability management activities	LI
	d.	Standards and/or guidelines have been identified to inform threat and vulnerability management activities	LI
MIL3	e.	Threat and vulnerability management activities are guided by documented policies or other organizational directives	LI
	f.	Threat and vulnerability management policies include compliance requirements for specified standards and/or guidelines	LI
	g.	Threat and vulnerability management activities are periodically reviewed to ensure conformance with policy	LI
	h.	Responsibility and authority for the performance of threat and vulnerability management activities are assigned to personnel	LI

	i.	Personnel performing threat and vulnerability management activities have the skills and knowledge needed to perform their assigned responsibilities	LI

4.5 Situational Awareness

Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other ONG-C2M2 domains, to form a common operating picture (COP), commensurate with the risk to critical infrastructure and organizational objectives.



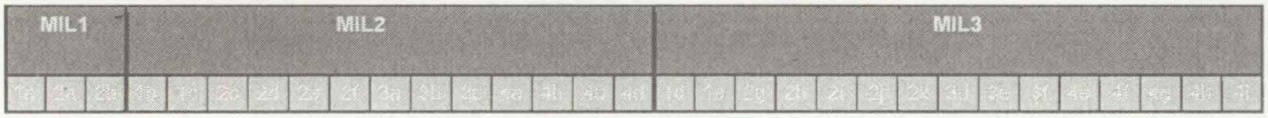


1. Perform Logging

MIL1	a.	Logging is occurring, at least in an ad hoc manner, for assets important to the function, where possible	LI
MIL2	b.	Logging requirements have been defined for all assets important to the function (e.g., scope of activity and coverage of assets, cybersecurity requirements [confidentiality, integrity, availability])	LI
	c.	Log data are being aggregated within the function	LI
MIL3	d.	Logging requirements are based on the risk to the function	LI
	e.	Log data support other business and security processes (e.g., incident response, asset management)	LI

2. Perform Monitoring

MIL1	a.	Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	LI
	b.	Operational environments are monitored, at least in an ad hoc manner, for anomalous behavior that may indicate a cybersecurity event	LI



2. Perform Monitoring (continued)

MIL2	c.	Monitoring and analysis requirements have been defined for the function and address timely review of event data	LI
	d.	Alarms and alerts are configured to aid in the identification of cybersecurity events (IR-1b)	LI
	e.	Indicators of anomalous activity have been defined and are monitored across the operational environment	LI
	f.	Monitoring activities are aligned with the function's threat profile (TVM-1d)	LI
MIL3	g.	Monitoring requirements are based on the risk to the function	LI
	h.	Monitoring is integrated with other business and security processes (e.g., incident response, asset management)	LI
	i.	Continuous monitoring is performed across the operational environment to identify anomalous activity	LI
	j.	Risk register (RM-2j) content is used to identify indicators of anomalous activity	LI
	k.	Alarms and alerts are configured according to indicators of anomalous activity	LI

3. Establish and Maintain a Common Operating Picture (COP)

MIL1	*No practice at MIL1*	
MIL2	Methods of communicating the current state of cybersecurity for the function are established and maintained	LI

	a.	Monitoring data are aggregated to provide an understanding of the operational state of the function (i.e., a common operating picture;	LI
	b.	a COP may or may not include visualization or be presented graphically)	
		Information from across the organization is available to enhance the common operating picture	LI
	c.		
MIL3	d.	Monitoring data are aggregated to provide near-real-time understanding of the cybersecurity state for the function to enhance the common operating picture	LI
	e.	Information from outside the organization is collected to enhance the common operating picture	LI
	f.	Predefined states of operation are defined and invoked (manual or automated process) based on the common operating picture	LI

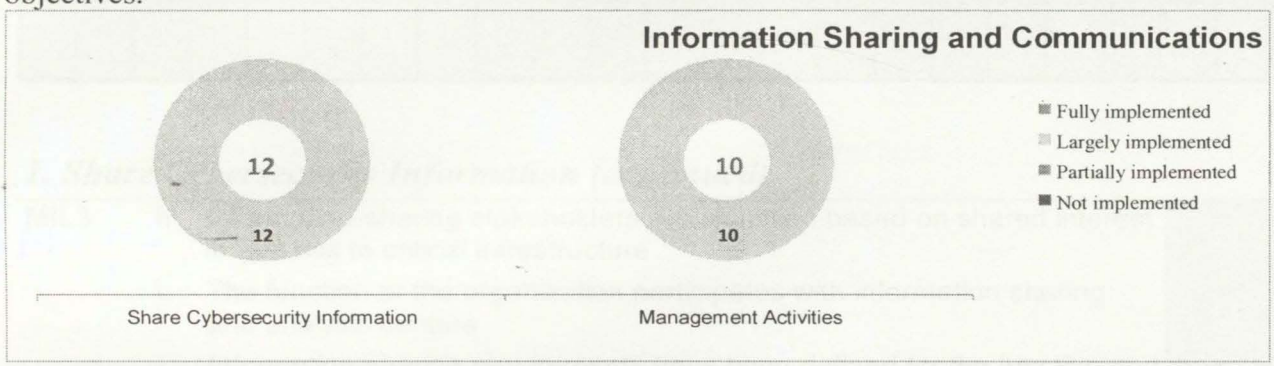
4. Management Activities

MIL1		*No practice at MIL1*	
MIL2	a.	Documented practices are followed for logging, monitoring, and COP activities	LI
	b.	Stakeholders for logging, monitoring, and COP activities are identified and involved	LI
	c.	Adequate resources (people, funding, and tools) are provided to support logging, monitoring, and COP activities	LI
	d.	Standards and/or guidelines have been identified to inform logging, monitoring, and COP activities	LI
MIL3	e.	Logging, monitoring, and COP activities are guided by documented policies or other organizational directives	LI
	f.	Logging, monitoring, and COP policies include compliance requirements for specified standards and/or guidelines	LI
	g.	Logging, monitoring, and COP activities are periodically reviewed to ensure conformance with policy	LI
	h.	Responsibility and authority for the performance of logging, monitoring, and COP activities are assigned to personnel	LI

	i.	Personnel performing logging, monitoring, and COP activities have the skills and knowledge needed to perform their assigned responsibilities	LI

4.6 Information Sharing and Communications

Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.



MIL1		MIL2									MIL3										
1a	1b	1c	1d	1e	1f	1g	2a	2b	2c	2d	1h	1i	1j	1k	1l	2e	2f	2g	2h	2i	2j

1. Share Cybersecurity Information

MIL1	a.	Information is collected from and provided to selected individuals and/or organizations, at least in an ad hoc manner	LI
	b.	Responsibility for cybersecurity reporting obligations are assigned to personnel (e.g., internal reporting, ICS-CERT, law enforcement), at least in an ad hoc manner	LI
MIL2	c.	Information-sharing stakeholders are identified based on their relevance to the continued operation of the function (e.g., connected organizations, vendors, sector organizations, regulators, internal entities)	LI
	d.	Information is collected from and provided to identified informationsharing stakeholders	LI

	e. Technical sources are identified who can be consulted on cybersecurity issues	LI
	f. Provisions are established and maintained to enable secure sharing of sensitive or classified information	LI
	g. Information-sharing practices address both standard operations and emergency operations	LI

MIL1		MIL2									MIL3										
1a	1b	1c	1d	1e	1f	1g	2a	2b	2c	2d	1h	1i	1j	1k	1l	2e	2f	2g	2h	2i	2j

1. Share Cybersecurity Information (continued)

MIL3	h. Information-sharing stakeholders are identified based on shared interest in and risk to critical infrastructure	LI
	i. The function or the organization participates with information sharing and analysis centers	LI
	j. Information-sharing requirements have been defined for the function and address timely dissemination of cybersecurity information	LI
	k. Procedures are in place to analyze and de-conflict received information	LI
	l. A network of internal and external trust relationships (formal and/or informal) has been established to vet and validate information about cyber events	LI

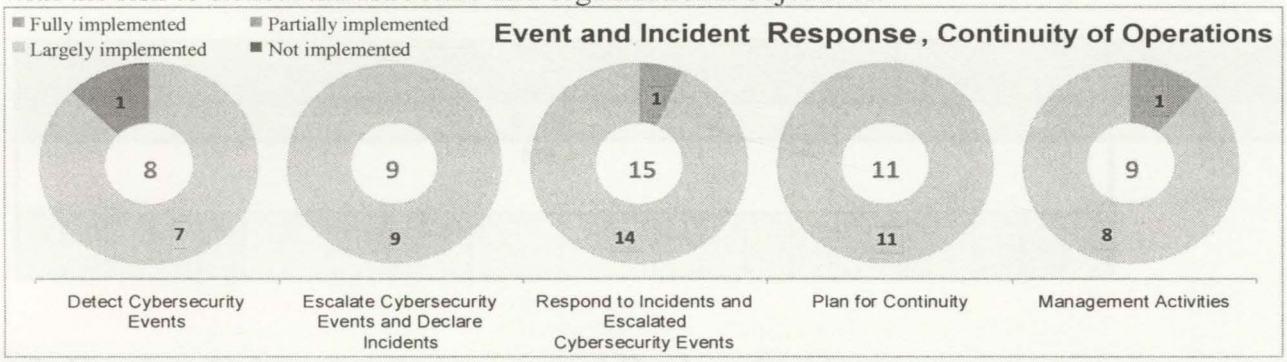
2. Management Activities

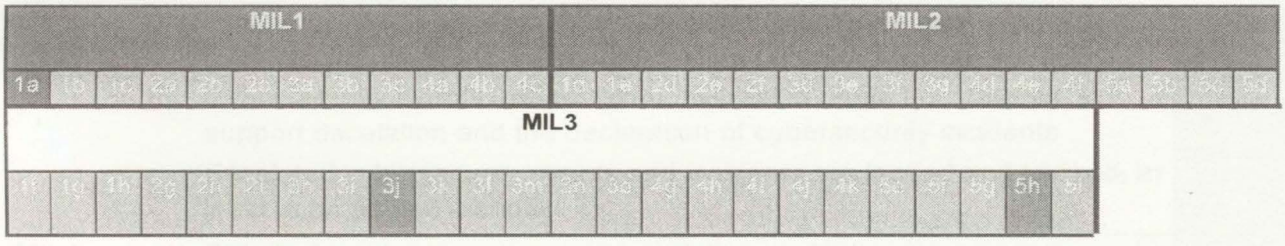
MIL1	*No practice at MIL1*	
MIL2	a. Documented practices are followed for information-sharing activities	LI
	b. Stakeholders for information-sharing activities are identified and involved	LI
	c. Adequate resources (people, funding, and tools) are provided to support information-sharing activities	LI
	d. Standards and/or guidelines have been identified to inform informationsharing activities	LI
MIL3	e. Information-sharing activities are guided by documented policies or other organizational directives	LI

f. Information-sharing policies include compliance requirements for specified standards and/or guidelines	LI
g. Information-sharing activities are periodically reviewed to ensure conformance with policy	LI
h. Responsibility and authority for the performance of information-sharing activities are assigned to personnel	LI
i. Personnel performing information-sharing activities have the skills and knowledge needed to perform their assigned responsibilities	LI
j. Information-sharing policies address protected information and ethical use and sharing of information, including sensitive and classified information as appropriate	LI

4.7 Event and Incident Response, Continuity of Operations

Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.

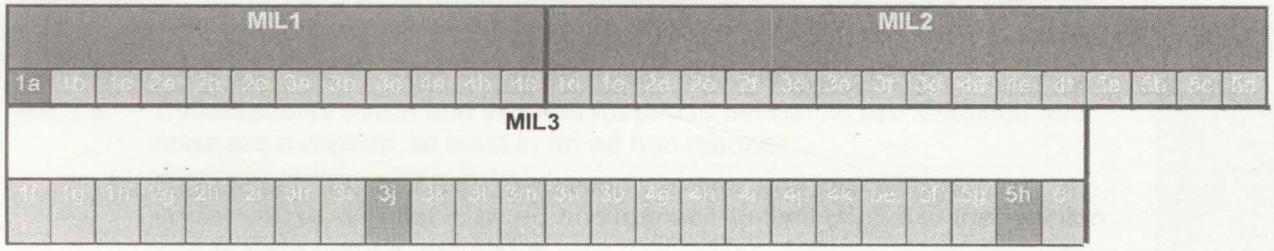




1. Detect Cybersecurity Events

MIL1	There is a point of contact (person or role) to whom cybersecurity events could be reported	FI

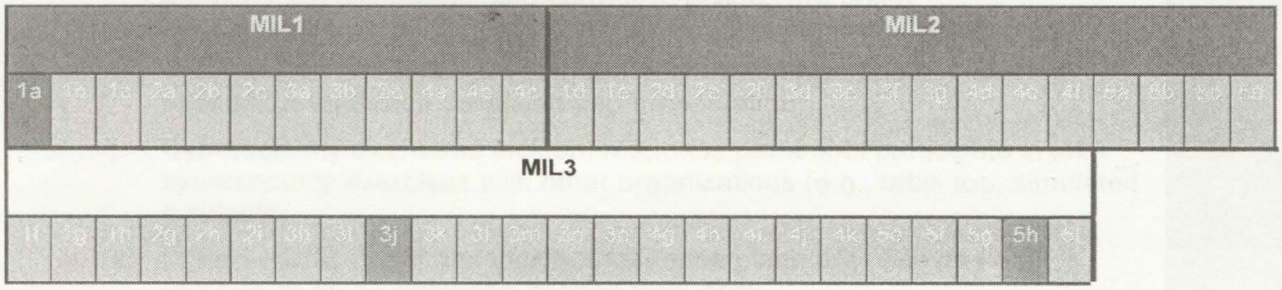
	a.	Detected cybersecurity events are reported, at least in an ad hoc manner	LI
	b.	Cybersecurity events are logged and tracked, at least in an ad hoc manner	LI
	c.		
MIL2	d.	Criteria are established for cybersecurity event detection (e.g., what constitutes an event, where to look for events)	LI
	e.	There is a repository where cybersecurity events are logged based on the established criteria	LI
MIL3	f.	Event information is correlated to support incident analysis by identifying patterns, trends, and other common features	LI
	g.	Cybersecurity event detection activities are adjusted based on information from the organization's risk register (RM-2j) and threat profile (TVM-1d) to help detect known threats and monitor for identified risks	LI
	h.	The common operating picture for the function is monitored to support the identification of cybersecurity events (SA-3a)	LI



2. Escalate Cybersecurity Events and Declare Incidents

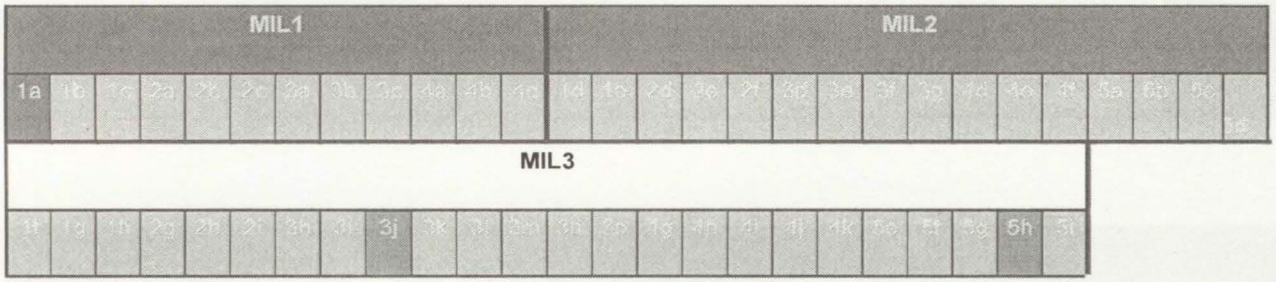
MIL1	a.	Criteria for cybersecurity event escalation are established, including cybersecurity incident declaration criteria, at least in an ad hoc manner	LI
	b.	Cybersecurity events are analyzed, at least in an ad hoc manner, to support escalation and the declaration of cybersecurity incidents	LI
	c.	Escalated cybersecurity events and incidents are logged and tracked, at least in an ad hoc manner	LI
MIL2	d.	Criteria for cybersecurity event escalation, including cybersecurity incident criteria, are established based on the potential impact to the function	LI
	e.	Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are updated at an organization-defined frequency	LI

	f.	There is a repository where escalated cybersecurity events and cybersecurity incidents are logged and tracked to closure	LI
MIL3	g.	Criteria for cybersecurity event escalation, including cybersecurity incident declaration criteria, are adjusted according to information from the organization's risk register (RM-2j) and threat profile (TVM-1d)	LI
	h.	Escalated cybersecurity events and declared cybersecurity incidents inform the common operating picture (SA-3a) for the function	LI
	i.	Escalated cybersecurity events and declared incidents are correlated to support the discovery of patterns, trends, and other common features	LI



3. Respond to Incidents and Escalated Cybersecurity Events

MIL1	a.	Cybersecurity event and incident response personnel are identified and roles are assigned, at least in an ad hoc manner	LI
	b.	Responses to escalated cybersecurity events and incidents are implemented, at least in an ad hoc manner, to limit impact to the function and restore normal operations	LI
	c.	Reporting of escalated cybersecurity events and incidents is performed (e.g., internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner	LI
MIL2	d.	Cybersecurity event and incident response is performed according to defined procedures that address all phases of the incident life cycle (e.g., triage, handling, communication, coordination, and closure)	LI
	e.	Cybersecurity event and incident response plans are exercised at an organization- defined frequency	LI
	f.	Cybersecurity event and incident response plans address OT and IT assets important to the delivery of the function	LI
	g.	Training is conducted for cybersecurity event and incident response teams	LI



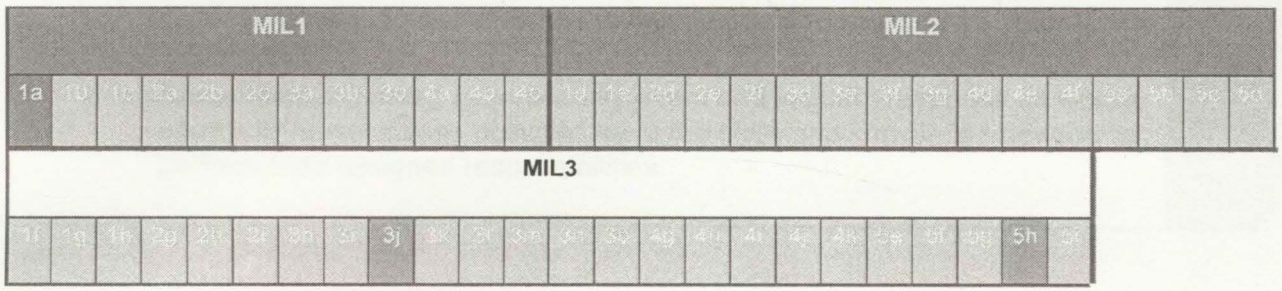
3. Respond to Incidents and Escalated Cybersecurity Events (continued)

MIL3 h.	Cybersecurity event and incident root-cause analysis and lessons-learned activities are performed, and corrective actions are taken	LI
i.	Cybersecurity event and incident responses are coordinated with law enforcement and other government entities as appropriate, including support for evidence collection and preservation	LI
j.	Cybersecurity event and incident response personnel participate in joint cybersecurity exercises with other organizations (e.g., table top, simulated incidents)	PI
k.	Cybersecurity event and incident response plans are reviewed and updated at an organization-defined frequency	LI
l.	Cybersecurity event and incident response activities are coordinated with relevant external entities	LI
m.	Cybersecurity event and incident response plans are aligned with the function's risk criteria (RM-1c) and threat profile (TVM-1d)	LI
n.	Policy and procedures for reporting cybersecurity event and incident information to designated authorities conform with applicable laws, regulations, and contractual agreements	LI
o.	Restored assets are configured appropriately and inventory information is updated following execution of response plans	LI

4. Plan for Continuity

MIL1 a.	The activities necessary to sustain minimum operations of the function are identified, at least in an ad hoc manner	LI
b.	The sequence of activities necessary to return the function to normal operation is identified, at least in an ad hoc manner	LI
c.	Continuity plans are developed, at least in an ad hoc manner, to sustain and restore operation of the function	LI
	Business impact analyses inform the development of continuity plans	LI

MIL2	d.	Recovery time objectives (RTO) and recovery point objectives (RPO) for the function are incorporated into continuity plans Continuity plans are evaluated and exercised	LI
	e.		LI
	f.		



4. Plan for Continuity (continued)

MIL3	g.	Business impact analyses are periodically reviewed and updated	LI
	h.	Recovery time objectives (RTO) and recovery point objectives (RPO) are aligned with the function's risk criteria (RM-1c)	LI
	i.	The results of continuity plan testing and/or activation are compared to recovery objectives, and plans are improved accordingly	LI
	j.	Continuity plans are periodically reviewed and updated	LI
	k.	Restored assets are configured appropriately and inventory information is updated following execution of continuity plans	LI

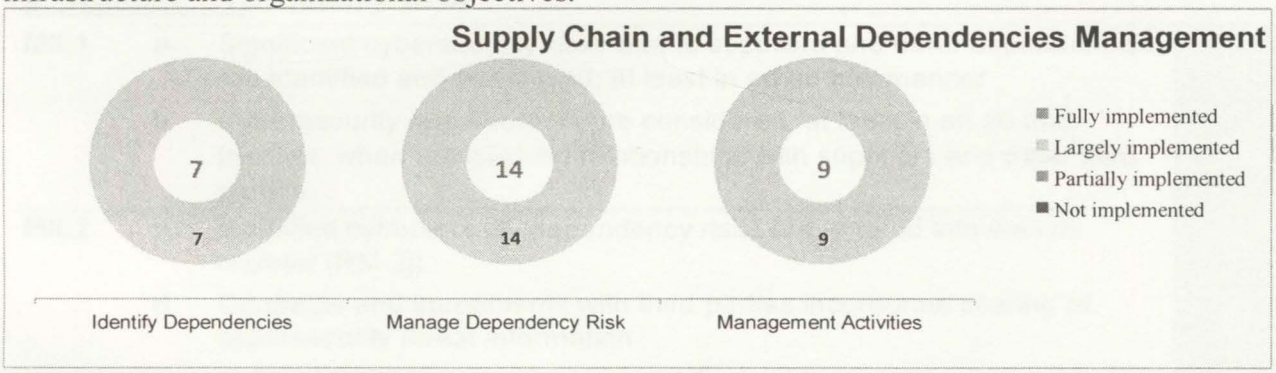
5. Management Activities

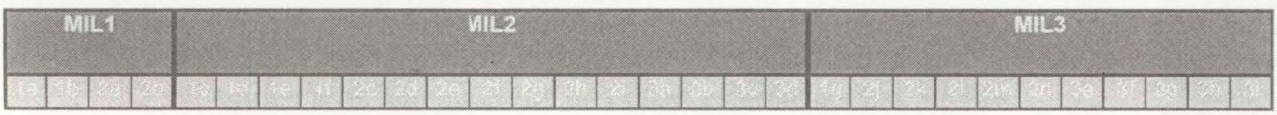
MIL1		*No practice at MIL1*	
MIL2	a.	Documented practices are followed for cybersecurity event and incident response as well as continuity of operations activities	LI
	b.	Stakeholders for cybersecurity event and incident response as well as continuity of operations activities are identified and involved	LI
	c.	Adequate resources (people, funding, and tools) are provided to support cybersecurity event and incident response as well as continuity of operations activities	LI
	d.	Standards and/or guidelines have been identified to inform cybersecurity event and incident response as well as continuity of operations activities	LI
		Cybersecurity event and incident response as well as continuity of operations activities are guided by documented policies or other organizational directives	LI

MIL3 e.	Cybersecurity event and incident response as well as continuity of operations policies include compliance requirements for specified standards and/or guidelines	LI
f.	Cybersecurity event and incident response as well as continuity of operations activities are periodically reviewed to ensure conformance with policy	LI
g.	Responsibility and authority for the performance of cybersecurity event and incident response as well as continuity of operations activities are assigned to personnel	PI
h.	Personnel performing cybersecurity event and incident response as well as continuity of operations activities have the skills and knowledge needed to perform their assigned responsibilities	LI
i.		

4.8 Supply Chain and External Dependencies Management

Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.





1. Identify Dependencies

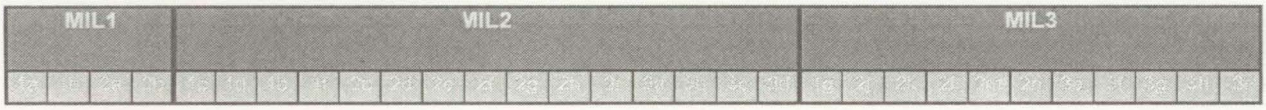
MIL1	Important IT and OT supplier dependencies are identified (i.e., external parties on which the delivery of the function depend, including operating partners), at least in an ad hoc manner	LI

	a.	Important customer dependencies are identified (i.e., external parties that are dependent on the delivery of the function including operating partners), at least in an ad hoc manner	LI
	b.		
MIL2	c.	Supplier dependencies are identified according to established criteria	LI
	d.	Customer dependencies are identified according to established criteria	LI
	e.	Single-source and other essential dependencies are identified	LI
	f.	Dependencies are prioritized	LI
MIL3	g.	Dependency prioritization and identification are based on the function's or organization's risk criteria (RM-1c)	LI

2. Manage Dependency Risk

MIL1	a.	Significant cybersecurity risks due to suppliers and other dependencies are identified and addressed, at least in an ad hoc manner	LI
	b.	Cybersecurity requirements are considered, at least in an ad hoc manner, when establishing relationships with suppliers and other third parties	LI
MIL2	c.	Identified cybersecurity dependency risks are entered into the risk register (RM-2j)	LI
	d.	Contracts and agreements with third parties incorporate sharing of cybersecurity threat information	LI
	e.	Cybersecurity requirements are established for suppliers according to a defined practice, including requirements for secure software development practices where appropriate	LI
	f.	Agreements with suppliers and other external entities include cybersecurity requirements	LI
	g.	Evaluation and selection of suppliers and other external entities includes consideration of their ability to meet cybersecurity requirements	LI
	h.	Agreements with suppliers require notification of cybersecurity incidents related to the delivery of the product or service	LI

	i.	Suppliers and other external entities are periodically reviewed for their ability to continually meet the cybersecurity requirements	LI
MIL3	j.	Cybersecurity risks due to external dependencies are managed according to the organization's risk management criteria and process	LI
	k.	Cybersecurity requirements are established for supplier dependencies based on the organization's risk criteria (RM-1c)	LI
	l.	Agreements with suppliers require notification of vulnerability-inducing product defects throughout the intended life cycle of delivered products	LI
	m.	Acceptance testing of procured assets includes testing for cybersecurity requirements	LI
	n.	Information sources are monitored to identify and avoid supply chain threats (e.g., counterfeit parts, software, and services)	LI

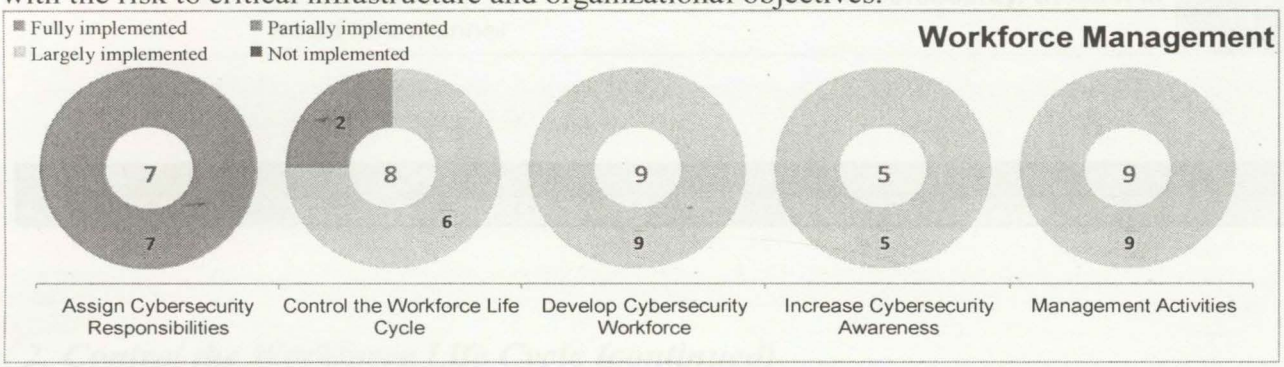


3. Management Activities

MIL1		*No practice at MIL1*	
MIL2	a.	Documented practices are followed for managing dependency risk	LI
	b.	Stakeholders for managing dependency risk are identified and involved	LI
	c.	Adequate resources (people, funding, and tools) are provided to support dependency risk management activities	LI
	d.	Standards and/or guidelines have been identified to inform managing dependency risk	LI
MIL3	e.	Dependency risk management activities are guided by documented policies or other organizational directives	LI
	f.	Dependency risk management policies include compliance requirements for specified standards and/or guidelines	LI
	g.	Dependency risk management activities are periodically reviewed to ensure conformance with policy	LI
	h.	Responsibility and authority for the performance of dependency risk management are assigned to personnel	LI
	i.	Personnel performing dependency risk management have the skills and knowledge needed to perform their assigned responsibilities	LI

4.9 Workforce Management

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.



1. Assign Cybersecurity Responsibilities

MIL1	a.	Cybersecurity responsibilities for the function are identified, at least in an ad hoc manner	FI
	b.	Cybersecurity responsibilities are assigned to specific people, at least in an ad hoc manner	FI
MIL2	c.	Cybersecurity responsibilities are assigned to specific roles, including external service providers	FI
	d.	Cybersecurity responsibilities are documented (e.g., in position descriptions)	FI
MIL3	e.	Cybersecurity responsibilities and job requirements are reviewed and updated as appropriate	FI
	f.	Cybersecurity responsibilities are included in job performance evaluation criteria	FI
	g.	Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage	FI

2. Control the Workforce Life Cycle

MIL1	a.	Personnel vetting (e.g., background checks, drug tests) is performed, at least in an ad hoc manner, at hire for positions that have access to the assets required for delivery of the function	LI
	b.	Personnel termination procedures address cybersecurity, at least in an ad hoc manner	LI

2. Control the Workforce Life Cycle (continued)

MIL2	c.	Personnel vetting is performed at an organization-defined frequency for positions that have access to the assets required for delivery of the function	LI
	d.	Personnel transfer procedures address cybersecurity	FI
MIL3	e.	Risk designations are assigned to all positions that have access to the assets required for delivery of the function	FI
	f.	Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk designation	LI
	g.	Succession planning is performed for personnel based on risk designation	LI
	h.	A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures	LI

3. Develop Cybersecurity Workforce

MIL1	a.	Cybersecurity training is made available, at least in an ad hoc manner, to personnel with assigned cybersecurity responsibilities	LI
MIL2	b.	Cybersecurity knowledge, skill, and ability gaps are identified	LI
	c.	Identified gaps are addressed through recruiting and/or training	LI
	d.	Cybersecurity training is provided as a prerequisite to granting access to assets that support the delivery of the function (e.g., new personnel training, personnel transfer training)	LI
		Cybersecurity workforce management objectives that support current and future operational needs are established and maintained	LI

MIL3	e.	Recruiting and retention are aligned to support cybersecurity workforce management objectives	LI
	f.	Training programs are aligned to support cybersecurity workforce management objectives	LI
	g.	The effectiveness of training programs is evaluated at an organizationdefined frequency and improvements are made as	LI
	h.	appropriate Training programs include continuing education and professional development opportunities for personnel with significant	LI
	i.	cybersecurity responsibilities	

4. Increase Cybersecurity Awareness

MIL1	a.	Cybersecurity awareness activities occur, at least in an ad hoc manner	LI
MIL2	b.	Objectives for cybersecurity awareness activities are established and maintained	LI
	c.	Cybersecurity awareness content is based on the organization's threat profile (TVM-1d)	LI
MIL3	d.	Cybersecurity awareness activities are aligned with the predefined states of operation (SA-3f)	LI
	e.	The effectiveness of cybersecurity awareness activities is evaluated at an organization-defined frequency and improvements are made as appropriate	LI

5. Management Activities

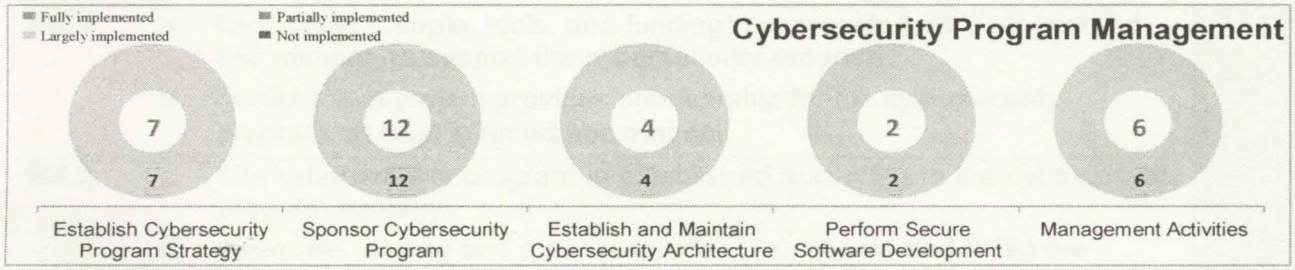
Note: In the following practices, "cybersecurity workforce management activities" refers collectively to all of the above practices in this domain.

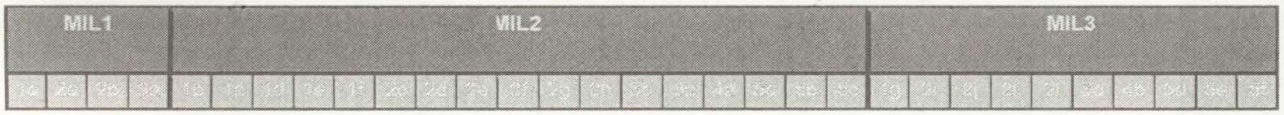
MIL1		*No practice at MIL1*	
MIL2	a.	Documented practices are followed for cybersecurity workforce management activities	LI
	b.	Stakeholders for cybersecurity workforce management activities are identified and involved	LI

	c.	Adequate resources (people, funding, and tools) are provided to support cybersecurity workforce management activities Standards	LI
	d.	and/or guidelines have been identified to inform cybersecurity workforce management activities	LI
MIL3	e.	Cybersecurity workforce management activities are guided by documented policies or other organizational directives	LI
	f.	Cybersecurity workforce management policies include compliance requirements for specified standards and/or guidelines	LI
	g.	Cybersecurity workforce management activities are periodically reviewed to ensure conformance with policy	LI
	h.	Responsibility and authority for the performance of cybersecurity workforce management activities are assigned to personnel	LI
	i.	Personnel performing cybersecurity workforce management activities have the skills and knowledge needed to perform their assigned responsibilities	LI

4.10 Cybersecurity Program Management

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 the organization's strategic objectives and the risk to critical infrastructure.

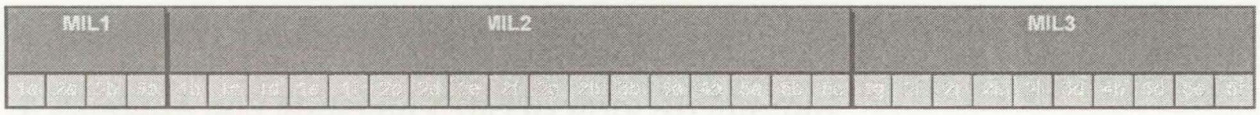




1. Establish Cybersecurity Program Strategy

MIL1	a.	The organization has a cybersecurity program strategy, which may be developed and managed in an ad hoc manner	LI

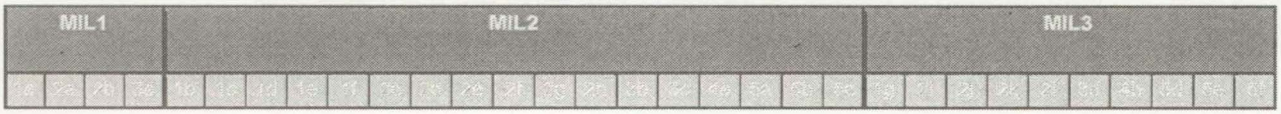
MIL2	b.	The cybersecurity program strategy defines objectives for the organization's cybersecurity activities	LI
	c.	The cybersecurity program strategy and priorities are documented and aligned with the organization's strategic objectives and risk to critical infrastructure	LI
	d.	The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities	LI
	e.	The cybersecurity program strategy defines the structure and organization of the cybersecurity program	LI
	f.	The cybersecurity program strategy is approved by senior management	LI
MIL3	g.	The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile (TVM-1d)	LI



2. Sponsor Cybersecurity Program

MIL1	a.	Resources (people, tools, and funding) are provided, at least in an ad hoc manner, to support the cybersecurity program	LI
	b.	Senior management provides sponsorship for the cybersecurity program, at least in an ad hoc manner	LI
MIL2	c.	The cybersecurity program is established according to the cybersecurity program strategy	LI
	d.	Adequate funding and other resources (i.e., people and tools) are provided to establish and operate a cybersecurity program aligned with the program strategy	LI
	e.	Senior management sponsorship for the cybersecurity program is visible and active (e.g., the importance and value of cybersecurity activities is regularly communicated by senior management)	LI
	f.	If the organization develops or procures software, secure software development practices are sponsored as an element of the cybersecurity program	LI
	g.	The development and maintenance of cybersecurity policies is sponsored	LI

	h.	Responsibility for the cybersecurity program is assigned to a role with requisite authority	LI
MIL3	i.	The performance of the cybersecurity program is monitored to ensure it aligns with the cybersecurity program strategy	LI
	j.	The cybersecurity program is independently reviewed (i.e., by reviewers who are not in the program) for achievement of cybersecurity program objectives	LI
	k.	The cybersecurity program addresses and enables the achievement of regulatory compliance as appropriate	LI
	l.	The cybersecurity program monitors and/or participates in selected industry cybersecurity standards or initiatives	LI



3. Establish and Maintain Cybersecurity Architecture

MIL1	a.	A strategy to architecturally isolate the organization's IT systems from OT systems is implemented, at least in an ad hoc manner	LI
MIL2	b.	A cybersecurity architecture is in place to enable segmentation, isolation, and other requirements that support the cybersecurity strategy	LI
	c.	Architectural segmentation and isolation is maintained according to a documented plan	LI
MIL3	d.	Cybersecurity architecture is updated at an organization-defined frequency to keep it current	LI

4. Perform Secure Software Development

MIL1		*No practice at MIL1*	
MIL2	a.	Software to be deployed on assets that are important to the delivery of the function is developed using secure software development practices	LI
MIL3	b.	Policies require that software that is to be deployed on assets that are important to the delivery of the function be developed using secure software development practices	LI

5. Management Activities

MIL1		*No practice at MIL1*	
MIL2	a.	Documented practices are followed for cybersecurity program management activities	LI
	b.	Stakeholders for cybersecurity program management activities are identified and involved	LI
	c.	Standards and/or guidelines have been identified to inform cybersecurity program management activities	LI
MIL3	d.	Cybersecurity program management activities are guided by documented policies or other organizational directives	LI
	e.	Cybersecurity program management activities are periodically reviewed to ensure conformance with policy	LI
	f.	Personnel performing cybersecurity program management activities have the skills and knowledge needed to perform their assigned responsibilities	LI

5. USING THE EVALUATION RESULTS

The ONG-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. **¡Error! No se encuentra el origen de la referencia.**5.1 summarizes the recommended approach for using the ONG-C2M2. An organization performs an evaluation against the ONG-C2M2, uses that 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.

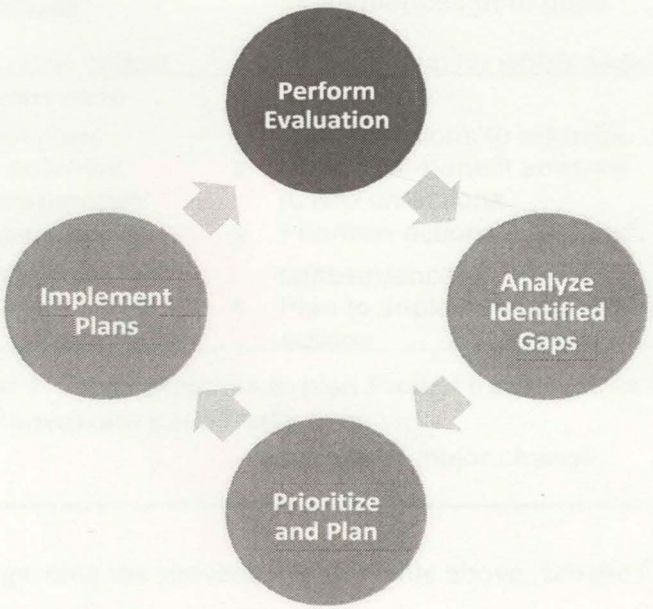


Figure 5.1: Recommended Approach for Using the ONG-C2M2

To aid in the analysis of identified gaps, survey questions that were recorded as either "Partially Implemented" or "Not Implemented" are consolidated in Section 5.1. *Summary of Identified Gaps*.

USING THE EVALUATION RESULTS

Table 5.1 presents a more detailed process for using evaluation results.

Table 5.1:Detailed Process for Using Evaluation Results

	Inputs	Activities	Outputs
Perform Evaluation	1. ES-C2M2 Self-Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct ES-C2M2 Self-Evaluation Workshop with appropriate attendees	ES-C2M2 Self-Evaluation Report
Analyze Identified Gaps	1. ES-C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2. Cost-benefit analysis (CBA) on actions 3. Prioritize actions (CBA and consequences) 4. Plan to implement prioritize actions	Prioritized implementation plan
Implement	1. Prioritized implementation plan	1. Track progress to plan 2. Reevaluate periodically or in response to major change	Project tracking data **Plans**

Note: For further detail regarding the processes in the table above, see the ONG-C2M2 Version 1.1.[1]

[1] 1 The ONG-C2M2 may be downloaded from:
http://energy.gov/oe/downloads/oil-and-natural-gas-subsector-cybersecurity-capability-maturity-model-february-2014

USING THE EVALUATION RESULTS

5.1 Summary of Identified Gaps

Status	MIL	Question	Text	Self Evaluation Notes
Risk Management				
Asset, Change, and Configuration Management				
Identity and Access Management				
Threat and Vulnerability Management				
Situational Awareness				
Information Sharing And Communications				
Event and Incident Response, Continuity of Operations				
Supply Chain and External Dependencies Management				
Workforce Management				
Cybersecurity Program Management				

APPENDIX A: EVALUATION SCORING PROCESS

This appendix describes the ONG-C2M2 evaluation scoring process.
Evaluation scores are derived from responses entered into the ES-C2M2 Self Evaluation Toolkit. Each question includes a four-point answer scale: Fully Implemented (FI), Largely Implemented (LI), Partially Implemented (PI), and Not Implemented (NI). The answers of FI or LI are required for a practice to be considered implemented for scoring. Credit is not applied for answers of PI or NI.
The evaluation questionnaire answer options are explained in more detail in the following table:

Table A.1: Evaluation Answer Scale

Answer Scale	Implementation Description
Fully Implemented	Complete
Largely Implemented	Complete, but with a recognized opportunity for improvement
Partially Implemented	Incomplete, but there are multiple opportunities for improvement
Not Implemented	Absent, the practice is not performed by the organization

Domain Maturity Indicator Level Scoring Process

Achieving a specific MIL for a given domain in the ONG-C2M2 requires the following:

1. Implementation of all of the practices for that level
2. The achievement of all preceding MILs in that domain

For example, to achieve MIL1 in a domain with four MIL1 practices, all four MIL1 practices must be in place. To achieve MIL2 in that same domain, all MIL1 and MIL2 practices must be in place.