Publicación retirada de la serie técnica del NIST

Aviso de Advertencia

La publicación adjunta ha sido retirada (archivada), pero la traducción al español de esta publicación está disponible. La versión en inglés de esta publicación ha sido reemplazada por otra publicación (que se indica a continuación).

Publicación retirada	
Série / Número	NIST Special Publication (SP) 800-181
Título	National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework
Fecha(s) de publicación	agosto de 2017
Fecha de retiro	16 de noviembre de 2020
Nota de retiro	SP 800-181 es reemplazada en su totalidad por la publicación SP 800-181 Revision 1.
Publicación(es) vigente(s) *(si aplica)*	
La publicación adjunta ha sido reemplazada por la(s) siguiente publicación(es):	
Série / Número	NIST Special Publication (SP) 800-181 Revision 1
Título	Workforce Framework for Cybersecurity (NICE Framework)
Autor(es)	Rodney Petersen; Danielle Santos; Karen A. Wetzel; Matthew C. Smith; Greg Witte
Fecha(s) de publicación	noviembre de 2020
URL/DOI	https://doi.org/10.6028/NIST.SP.800-181r1
Información adicional *(si aplica)*	
Contacto	NICE Framework: NICEframework@nist.gov
Última versión de la publicación adjunta	
Información relacionada	National Initiative for Cybersecurity Education (NICE): https://nist.gov/nice https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final
Enlace del Anuncio de retiro	

Fecha actualizada: 13 de noviembre de 2020

National Institute of Standards and Technology
U.S. Department of Commerce

Publicación especial 800-181 del NIST

Iniciativa nacional para la educación en ciberseguridad (NICE) Marco para el personal de ciberseguridad

William Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.SP.800-181

National Institute of Standards and Technology
U.S. Department of Commerce

Publicación especial 800-181 del NIST

Iniciativa nacional para la educación en ciberseguridad (NICE) Marco para el personal de ciberseguridad

William Newhouse
División de ciberseguridad aplicada
Laboratorio de tecnología de la información

Stephanie Keith
División de estrategias y políticas del personal de cibernética
Oficina del subdirector de información del Departamento de Defensa

Benjamin Scribner
Sector de concientización y educación cibernética
Dirección nacional de protección y programas del Departamento de Seguridad Nacional

Greg Witte
G2, Inc.
Annapolis Junction, Maryland

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.SP.800-181

Agosto de 2017

Departamento de Comercio de los EE. UU.
Wilbur L. Ross, Jr., secretario

Instituto Nacional de Normas y Tecnología
Kent Rochford, director interino del NIST y subsecretario de Normas y Tecnología del Departamento de Comercio

Autoridad

El Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés) redactó esta publicación de acuerdo con sus responsabilidades reglamentarias en virtud de la Ley federal de modernización de la seguridad de la información (FISMA, por sus siglas en inglés) de 2014; la sección 3551 del título 44 del Código de los EE. UU. y siguientes; y la Ley pública (P.L., por sus siglas en inglés) 113-283. El NIST se encarga de formular las normas y directrices de seguridad de la información, entre las que figuran los requisitos mínimos para los sistemas federales de información. Sin embargo, esas normas y directrices no se aplicarán a los sistemas nacionales de seguridad sin la aprobación expresa de los funcionarios federales correspondientes que ejerzan la autoridad de las políticas sobre estos sistemas. Esta directriz es acorde con los requisitos de la circular A-130 de la Oficina de Administración y Presupuesto (OMB, por sus siglas en inglés).

Ninguna información en esta publicación deberá interpretarse de manera que contradiga las normas y directrices obligatorias y vinculantes establecidas por el secretario de Comercio para los organismos federales conforme con su autoridad legal. Estas directrices tampoco deberán interpretarse como modificaciones o sustituciones de las facultades del secretario de Comercio, del director de la OMB o de cualquier otro funcionario federal. Esta publicación puede ser utilizada por organizaciones no gubernamentales de forma voluntaria y no está sujeta a derechos de autor en los Estados Unidos. Sin embargo, el NIST agradecería que se le atribuya la presente.

Publicación especial 800-181 del Instituto Nacional de Normas y Tecnología
Publicación especial 800-181 del NIST, 165 páginas (Agosto de 2017)
CODEN: NSPUE2

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.SP.800-181

Es posible que en este documento se identifiquen ciertas entidades, equipos o materiales comerciales para describir adecuadamente un procedimiento o concepto experimental. Tal identificación no presupone que el NIST los recomienda o aprueba, ni tampoco que las entidades, los materiales o los equipos sean necesariamente los mejores disponibles para ese fin.

Esta publicación puede hacer referencia a otras publicaciones que el NIST esté preparando actualmente de acuerdo con sus responsabilidades estatutarias asignadas. Los organismos federales pueden usar la información de esta publicación, así como los conceptos y las metodologías, incluso antes de concluir esas publicaciones complementarias. Sin embargo, hasta que se complete cada publicación, los requisitos, las directrices y los procedimientos actuales seguirán vigentes donde se hayan establecido. Con fines de planificación y transición, es conveniente que los organismos federales sigan de cerca la preparación del NIST de estas nuevas publicaciones.

Instamos a las organizaciones a que revisen todos los borradores de las publicaciones durante los períodos en los que se someten a comentarios públicos y a que aporten sugerencias al NIST. Muchas de las publicaciones del NIST sobre ciberseguridad, que no sean las antes mencionadas, están disponibles en http://csrc.nist.gov/publications.

Los comentarios sobre esta publicación se pueden enviar al:

National Institute of Standards and Technology
Attn: NICE, Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Correo electrónico: niceframework@nist.gov

Todo comentario está sujeto a publicación en virtud de la Ley de libertad de información (FOIA, por sus siglas en inglés).

Informes sobre la tecnología de los sistemas informáticos

El Laboratorio de tecnología de la información (ITL, por sus siglas en inglés) del NIST promueve la economía y el bienestar público de los Estados Unidos brindando liderazgo técnico a la infraestructura de medición y normas del país. El ITL elabora pruebas, métodos de pruebas, datos de referencia, implementaciones de pruebas de concepto y análisis técnicos para fomentar el desarrollo y uso productivo de la tecnología de la información. Las responsabilidades del ITL incluyen la formulación de normas y directrices de gestión, administrativas, técnicas y físicas para la seguridad y privacidad rentables de la información en los sistemas federales de información que no sea sobre seguridad nacional. La serie 800 de las publicaciones especiales comunica las investigaciones, directrices e iniciativas de alcance del ITL relacionadas con la seguridad de los sistemas de información, y sus actividades de colaboración con el sector industrial, el gobierno y las organizaciones académicas.

Resumen

Esta publicación describe el Marco para el personal de ciberseguridad (Marco de la NICE) de la Iniciativa nacional para la educación en ciberseguridad (NICE, por sus siglas en inglés), una estructura de referencia que detalla la naturaleza interdisciplinaria del trabajo de ciberseguridad. Sirve como un recurso de referencia fundamental para describir e intercambiar información sobre el trabajo de ciberseguridad, y los conocimientos, habilidades y capacidades (CHC) necesarios para llevar a cabo las tareas que pueden fortalecer la postura de ciberseguridad de una organización. El Marco de la NICE mejora la comunicación sobre la manera de identificar, contratar, formar y retener personas con talento en el campo de la ciberseguridad por medio de un léxico común y uniforme que clasifica y describe el trabajo en materia de ciberseguridad. Este marco sirve de referencia para que las organizaciones o los sectores puedan preparar publicaciones o recursos adicionales que satisfagan sus necesidades de definir u ofrecer orientación sobre diferentes aspectos de la formación, planificación, capacitación y educación del personal de ciberseguridad.

Palabras clave

Capacidad, ciberseguridad, ciberespacio, educación, conocimiento, función, habilidad, área de especialización, tarea, capacitación y función laboral.

Revisiones

Véase el sitio web de revisiones del Marco de la NICE [1] para determinar si ha habido actualizaciones de este.

Contenido complementario

Se puede consultar una hoja de cálculo de referencia para el Marco de la NICE en https://www.nist.gov/file/372581.

Agradecimientos

Los autores agradecen y reconocen las importantes contribuciones hechas por personas y organizaciones de los sectores público y privado, cuyos comentarios reflexivos y constructivos mejoraron la calidad, exhaustividad y utilidad general de esta publicación. Asimismo, reconocen el liderazgo y la labor de Rodney Petersen, director de la Iniciativa nacional para la educación en ciberseguridad (NICE) en el NIST, y agradecen las contribuciones individuales que las personas siguientes hicieron a esta publicación: Tanya Brewer, Dean Bushmiller, Lynne Clarke, Jerri Damavandy, Lisa Dorr, Ryan Farr, Jim Foti, Jodi Guss, Keith Hall, Chris Kelsall, Elizabeth Lennon, Jeff Marron, Joshua Musicante, Stephen Olechnowicz, Lori Pfannenstein, Chuck Romine, Kevin Sanchez-Cherry, Danielle Santos, Stephanie Shively, Matthew Smith, Kevin Stine, Bluma Sussman, Caroline Tan, Baris Yakin y Clarence Williams.

El primer Marco de la NICE se sometió a comentarios públicos en septiembre de 2012 y, en abril de 2013, se publicó la versión final titulada Marco nacional para el personal de ciberseguridad, versión 1.0 [2]. Los autores reconocen a la Dra. Jane Homeyer, Anne Quigley, Rex Min, Noel Kyle, Maya Yankelevich y Peggy Maxson por dirigir su producción, y a Montana Williams y Roy Burgess por su liderazgo en la elaboración del Marco nacional para el personal de ciberseguridad, versión 2.0, publicado en abril de 2014 [3].

Para concluir, los autores reconocen respetuosamente la labor fundamental desempeñada en la década de 1960 en el campo de la seguridad informática. La visión, las perspectivas y el trabajo dedicado de los pioneros en esta disciplina sirven como base filosófica y técnica de las tareas, conocimientos, habilidades y capacidades mencionadas en esta publicación.

Información sobre marcas comerciales

Resumen ejecutivo

La Iniciativa nacional para la educación en ciberseguridad (NICE), dirigida por el Instituto Nacional de Normas y Tecnología (NIST) del Departamento de Comercio de los Estados Unidos, es una colaboración entre el gobierno, el sector académico y el sector privado para energizar y promover una red y un ecosistema sólidos para la educación, capacitación y formación del personal en el campo de la ciberseguridad. La NICE cumple esta misión coordinándose con los socios del gobierno, el sector académico y el sector industrial para ampliar los mejores programas vigentes, facilitar el cambio y la innovación, y aportar liderazgo y visión a fin de aumentar el número de profesionales capacitados en ciberseguridad que ayudan a mantener la protección de nuestro país.

La NICE tiene el compromiso de cultivar un personal de ciberseguridad integrado y competitivo a nivel mundial, desde su contratación hasta su jubilación, que esté preparado para proteger a nuestro país de los peligros existentes y emergentes que afronta la ciberseguridad. La NICE promueve iniciativas a nivel nacional que aumentan el número de personas que poseen los conocimientos, habilidades y capacidades necesarias para efectuar las tareas del trabajo de ciberseguridad.

A medida que crecen y evolucionan las amenazas que aprovechan las vulnerabilidades de nuestra ciberinfraestructura, un personal de ciberseguridad integrado debe ser capaz de diseñar, preparar, implementar y mantener ciberestrategias defensivas y ofensivas. Un personal de ciberseguridad integrado desempeña funciones técnicas y no técnicas con los conocimientos y la experiencia que posee. Además, puede solventar los obstáculos de ciberseguridad inherentes a la preparación de su organización para implementar con éxito los elementos de los procesos de la misión y de negocios relacionados con el ciberespacio.

Esta publicación brinda una referencia fundamental para ayudar a un personal capaz de satisfacer las necesidades de ciberseguridad de una organización por medio del uso de un léxico común y uniforme que describe el trabajo en materia de ciberseguridad por categoría, área de especialización y función laboral. También ofrece un superconjunto de conocimientos, habilidades y capacidades (CHC) de ciberseguridad y las tareas para cada función laboral. El Marco de la NICE contribuye a la comunicación uniforme entre las organizaciones y los sectores de educación, capacitación y formación del personal en el campo de la ciberseguridad.

Para el usuario del Marco de la NICE, será una referencia de los diferentes aspectos de la formación, educación o capacitación del personal. Asimismo, cuando este material se utilice en los niveles organizativos, el usuario deberá adaptar lo que se extraiga del marco a las normas, los reglamentos, las necesidades y la misión de su organización. El Marco de la NICE es un punto de partida que sirve de referencia para el contenido de orientaciones y directrices relacionadas con trayectorias profesionales, educación, capacitación y programas de acreditación.

El Marco de la NICE es un recurso que fortalecerá la capacidad de una organización para comunicarse uniforme y claramente acerca del trabajo y el personal de ciberseguridad. Las organizaciones o los sectores podrán preparar publicaciones o recursos adicionales que satisfagan sus necesidades de definir u ofrecer orientación sobre diferentes aspectos de la formación, planificación, capacitación y educación del personal.

Hay una hoja de cálculo de referencia [4] disponible en el sitio web del Marco de la NICE [5].

Índice

Lista de apéndices

Lista de tablas

1 Introducción

La Iniciativa nacional para la educación en ciberseguridad (NICE), dirigida por el Instituto Nacional de Normas y Tecnología (NIST) del Departamento de Comercio de los Estados Unidos, es una colaboración entre el gobierno, el sector académico y el sector privado para impulsar y promover una red y un ecosistema sólidos para la educación, capacitación y formación del personal en el campo de la ciberseguridad. La NICE cumple esta misión coordinándose con los socios del gobierno, el sector académico y el sector industrial para ampliar programas vigentes exitosos, facilitar el cambio y la innovación, y aportar liderazgo y visión a fin de aumentar el número de profesionales capacitados en ciberseguridad que ayudan a mantener nuestra nación protegida y económicamente competitiva.

La NICE tiene el compromiso de cultivar un personal de ciberseguridad integrado y competitivo a nivel mundial, desde su contratación hasta su jubilación, que esté preparado para proteger a nuestro país de los peligros existentes y emergentes que afronta la ciberseguridad.

En este documento, se emplean los términos combinados de “personal de ciberseguridad” para hacer referencia a los empleados cuyas funciones laborales repercuten en la capacidad de una organización para proteger sus datos, sistemas y operaciones. Se incluyen nuevas funciones laborales que han sido conocidas tradicionalmente como funciones de seguridad de la tecnología de la información (TI). Esas funciones se añadieron a este marco con objeto de destacar su importancia para la postura general de ciberseguridad de una organización. Además, algunas de las funciones laborales que se describen aquí cuentan con el prefijo *ciber* para incluir sectores en los que la cibernética se ha convertido en la norma de conversación de ese campo.

El personal de ciberseguridad incluye no solo a los empleados dedicados al aspecto técnico, sino también a quienes aplican sus conocimientos de ciberseguridad al preparar a su organización

para implementar satisfactoriamente su misión. Es necesario que el personal de ciberseguridad esté bien informado y capacitado para hacer frente a los riesgos a la ciberseguridad en el proceso general de gestión de riesgos de una organización.

1.1 Antecedentes del Marco de la NICE

El concepto del Marco de la NICE comenzó antes del establecimiento de la NICE en 2010, y surgió del reconocimiento de que el personal de ciberseguridad no había sido definido ni evaluado. Para solucionar esta dificultad, en 2008, el Consejo federal de directores de sistemas de información (CIO, por sus siglas en inglés) emprendió la tarea de presentar un marco normalizado para conocer las funciones de ciberseguridad en el gobierno federal. Los aportes de los grupos de discusión, con expertos en el tema provenientes de numerosos organismos federales, ayudaron al Consejo federal de directores de sistemas de información a preparar un informe de investigación en el que se hacía referencia a los lugares en los que ya estaban en marcha otros trabajos de desarrollo profesional en materia de tecnología de la información, y se identificaron 13 funciones específicas según las necesidades de los organismos para llevar a cabo el trabajo de ciberseguridad.

De acuerdo con esta exploración inherentemente multidisciplinaria del “campo” de la ciberseguridad, la Iniciativa nacional integral de ciberseguridad se centró en el personal y asignó a varios organismos la tarea de colaborar en la preparación de un marco para el personal de ciberseguridad. El primer borrador fue publicado en septiembre de 2011 para someterlo a comentarios públicos. Los comentarios se incorporaron en la versión 1.0 [2].

En una revisión posterior llevada a cabo en todo el gobierno federal, se señalaron ámbitos específicos que debían examinarse y refinarse. El Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) recopiló la información aportada y validó las recomendaciones finales por medio de grupos de discusión con expertos en el tema de todo el país provenientes y de diversos sectores industriales, académicos y gubernamentales, lo que dio como resultado una segunda versión del Marco de la NICE, la versión 2.0 [3], publicada en 2014.

La Oficina del Secretario de Defensa (OSD, por sus siglas en inglés) amplió la versión 2.0 mediante colaboraciones internas con componentes de servicios y colaboraciones externas con el sector privado. Los coautores del DHS y del NIST trabajaron con la OSD para refinar la ampliación y convertirla en esta publicación, con la meta de enfatizar la aplicabilidad del sector privado y reforzar la visión de que el Marco de la NICE es un recurso de referencia para los sectores público y privado.

1.2 Objetivo y aplicabilidad

Esta publicación sirve como un recurso de referencia fundamental para asistir a un personal capaz de satisfacer las necesidades de ciberseguridad de una organización. Proporciona a las organizaciones un léxico común y uniforme que clasifica y describe el trabajo en materia de ciberseguridad.

El uso del Marco de la NICE como una referencia fundamental mejorará la comunicación necesaria para identificar, contratar y formar a las personas con talento en el campo de la ciberseguridad. El marco de la NICE permitirá a los empleadores usar un lenguaje uniforme y

dirigido en los programas de formación profesional, las certificaciones y credenciales académicas del sector y la selección de oportunidades de capacitación pertinentes para su personal.

El Marco de la NICE facilita el uso de un método más uniforme, comparable y repetible en la selección y la especificación de funciones de ciberseguridad para los cargos en las organizaciones. También proporciona un léxico común que las instituciones académicas pueden utilizar en la creación de planes de estudios de ciberseguridad que preparen mejor a los estudiantes para las necesidades actuales y previstas del personal de ciberseguridad.

La aplicación del Marco de la NICE permite describir todos los trabajos en el ámbito de la ciberseguridad. Una de las metas de la aplicabilidad del Marco de la NICE es poder describir todos los trabajos o puestos en el campo de la ciberseguridad mediante la identificación del material pertinente de uno o más componentes de este marco. Para cada empleo o puesto, el contexto de los procesos de la misión o de negocios y las prioridades determinará la selección del material del Marco de la NICE.

Las organizaciones o los sectores pueden usar el Marco de la NICE para elaborar publicaciones o recursos adicionales que satisfagan sus necesidades de definir u ofrecer orientación sobre diferentes aspectos de la formación, planificación, capacitación y educación del personal.

1.3 Público y usuarios

El Marco de la NICE puede interpretarse como un diccionario no obligatorio para el personal de ciberseguridad. Los usuarios que lo empleen como referencia deben implementarlo a nivel local para fines diversos de formación, educación o capacitación del personal.

1.3.1 Empleadores

El uso del léxico común del Marco de la NICE permite a los empleadores inventariar y formar a su personal de ciberseguridad. Los empleadores y la dirección de la organización pueden usar el marco de la NICE para:

- inventariar y dar seguimiento a su personal de ciberseguridad para entender mejor las fortalezas y deficiencias de sus conocimientos, habilidades y capacidades y de las tareas que desempeña;
- identificar los requisitos de capacitación y cualificación para desarrollar los conocimientos, habilidades y capacidades esenciales para desempeñar las tareas de ciberseguridad;
- mejorar las descripciones de los puestos y anuncios de plazas vacantes seleccionando los CHC y las tareas pertinentes, una vez que se hayan identificado las funciones laborales y las tareas;
- identificar las funciones laborales más importantes y diseñar trayectorias profesionales para orientar al personal en la obtención de las habilidades necesarias para esas funciones; y
- establecer una terminología común entre los encargados de la contratación y el personal de recursos humanos (RR. HH.) para la captación, retención y capacitación de personal altamente especializado.

1.3.2 Personal de ciberseguridad actual y futuro

El Marco de la NICE ayuda a quienes trabajan en el campo de la ciberseguridad, y a quienes aspiran ingresar en este campo, a explorar las tareas en las Categorías de ciberseguridad y las funciones laborales. También es útil para quienes ayudan a este personal (como especialistas en dotación de personal y asesores) a explicar a los solicitantes de empleo y estudiantes cuáles son las funciones laborales de ciberseguridad y los conocimientos, habilidades y capacidades afines que los empleadores valoran para los trabajos y puestos más solicitados en ese campo.

El empleo del léxico común del Marco de la NICE en los anuncios y descripciones de plazas vacantes también ayuda a estos empleados ya que ofrece descripciones claras y uniformes de las tareas y la capacitación en materia de ciberseguridad necesarias para esos puestos.

Cuando los proveedores de capacitación y certificación del sector usan el léxico común del Marco de la NICE, el personal del campo de ciberseguridad o los aspirantes a ingresar en este campo pueden encontrar instructores o certificadores que enseñen las tareas necesarias para obtener un empleo de ciberseguridad o para avanzar a nuevos puestos. El uso del léxico común ayuda a los estudiantes y a los profesionales a obtener los CHC que suele demostrar una persona cuyo puesto de ciberseguridad incluye una función laboral determinada. Este conocimiento les permite encontrar programas académicos que incluyan resultados de aprendizaje y unidades de conocimiento relacionados con los CHC y las tareas que los empleadores valoran.

1.3.3 Educadores e instructores

El Marco de la NICE ofrece una referencia para que los educadores preparen planes de estudios, programas de certificación o licenciatura, programas de capacitación, cursos, seminarios y ejercicios u oportunidades que abarquen los CHC y las tareas descritas en el Marco de la NICE.

Los especialistas en dotación de personal y asesores pueden usar el Marco de la NICE como un recurso para explorar profesiones.

1.3.4 Proveedores de tecnología

Con el uso del Marco de la NICE, un proveedor de tecnología puede identificar las funciones laborales de ciberseguridad y las tareas y los CHC asociados con los productos y servicios de hardware y software que proporciona. El proveedor creará luego materiales de ayuda adecuados para facilitar al personal de ciberseguridad la configuración y la gestión correctas de sus productos.

1.4 Organización de esta publicación especial

El resto de esta publicación especial está organizado de la siguiente manera:

- El capítulo 2 define los componentes del Marco de la NICE: (i) categorías; (ii) áreas de especialización; (iii) funciones laborales; (iv) superconjuntos de conocimientos, habilidades y capacidades afines; y (v) tareas para cada función laboral.
- El capítulo 3 describe el uso del Marco de la NICE.

- El capítulo 4 señala las áreas en las que otras publicaciones, directrices, orientación y herramientas podrían ampliar el efecto del Marco de la NICE.
- El 4.3Apéndice A: describe la lista de categorías, áreas de especialización, funciones laborales, CHC y tareas del Marco de la NICE.
- El Apéndice B: proporciona una lista detallada de cada función laboral, incluidos los CHC y las tareas afines.
- El Apéndice C: incluye algunos ejemplos de recursos para la formación del personal.
- El Apéndice D: proporciona algunos ejemplos de referencia cruzada entre parte del contenido de los documentos de orientación o directrices y los componentes del Marco de la NICE.
- El Apéndice E: enumera las siglas y abreviaturas seleccionadas que se usan en este documento.
- El Apéndice F: incluye las fuentes citadas en este documento.

2 Componentes del Marco de la NICE y sus relaciones

2.1 Componentes del Marco de la NICE

El marco de la NICE organiza el trabajo de ciberseguridad y de áreas afines. En esta sección, se presentan y definen los componentes principales del marco compatibles con esas áreas.

2.1.1 Categorías

Las Categorías proporcionan la estructura organizativa completa del Marco de la NICE. Hay siete Categorías y todas están compuestas de áreas de especialización y funciones laborales. Esta estructura organizativa se basa en amplios análisis de empleos, en los cuales se agrupan los trabajos y el personal que desempeña funciones principales comunes, independientemente de los cargos u otros términos ocupacionales.

2.1.2 Áreas de especialización

Las Categorías contienen agrupaciones del trabajo de ciberseguridad que se denominan áreas de especialización. En la versión 1.0 del Marco nacional para el personal de ciberseguridad [2], se mencionaron 31 áreas de especialización, y en la versión 2.0 de este documento [3], se mencionaron 32. Cada área de especialización representa un área de trabajo concentrado, o función, dentro del trabajo de ciberseguridad y de áreas afines. En versiones previas del Marco de la NICE, los CHC y las tareas se relacionaban con cada área de especialización. Los CHC y las tareas están ahora asociados con las funciones laborales.

2.1.3 Funciones laborales

Las funciones laborales son las agrupaciones más detalladas del trabajo de ciberseguridad y de áreas afines e incluyen una lista de los atributos necesarios para desempeñar esa función, como los conocimientos, habilidades y capacidades (CHC) y las tareas efectuadas en esa función.

El trabajo que se desempeña en un empleo o puesto se describe seleccionando una o más funciones laborales del Marco de la NICE correspondientes a ese empleo o puesto, compatibles con los procesos de la misión o de negocios.

Para ayudar a la organización y comunicación de las responsabilidades de ciberseguridad, las funciones laborales se agrupan en clases específicas de categorías y áreas de especialización, como se muestra en el Apéndice A:.

2.1.4 Conocimientos, habilidades y capacidades (CHC)

Los conocimientos, habilidades y capacidades (CHC) son los atributos necesarios para desempeñar las funciones laborales, y generalmente se demuestran por medio de la experiencia, educación o capacitación pertinentes.

> El **conocimiento** es un cúmulo de información que se aplica directamente al desempeño de una función.

La **habilidad** suele definirse como una competencia observable para desempeñar un acto psicomotor aprendido. Las habilidades en el ámbito psicomotor describen la capacidad para manejar físicamente una herramienta o un instrumento, como una mano o un martillo. Las habilidades necesarias en el campo de la ciberseguridad dependen menos del manejo físico de herramientas e instrumentos y más de la aplicación de herramientas, marcos, procesos y controles que repercuten en la postura de ciberseguridad de una organización o de una persona.

La **capacidad** es la competencia para desempeñar un comportamiento observable o un comportamiento que da lugar a un producto observable.

2.1.5 Tareas

Una tarea es una parte específica y definida del trabajo que, cuando se combina con otras tareas identificadas, conforma el trabajo en un área de especialización o función laboral específica.

2.2 Relaciones de los componentes del Marco de la NICE

Los componentes del Marco de la NICE describen el trabajo de ciberseguridad. Como se ilustra en la Figura 1, cada Categoría se compone de áreas de especialización y cada una de esas áreas se compone de una o más funciones laborales. Cada función laboral, a su vez, incluye CHC y tareas.

Agrupar los componentes de esta manera simplifica la comunicación acerca de los temas del personal de ciberseguridad y facilita la correspondencia con otros marcos. En el Apéndice B y en la hoja de cálculo de referencia [4] publicada en el sitio web [5] del Marco de la NICE, se muestran las relaciones específicas entre las funciones laborales, los CHC y las tareas.

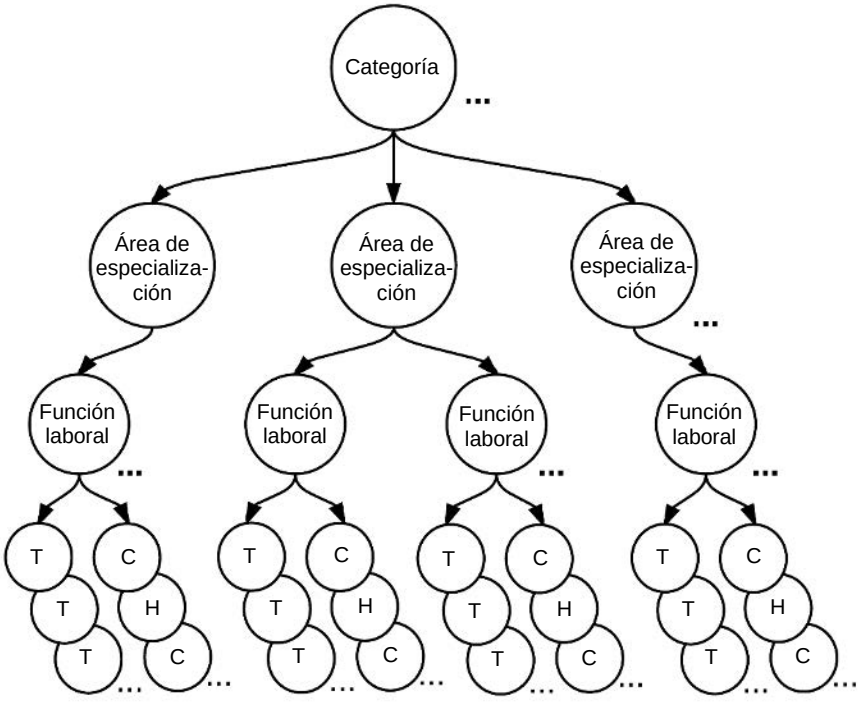

Figura 1: Relaciones entre los componentes del Marco de la NICE

3 Uso del Marco de la NICE

El uso del Marco de la NICE para conocer las necesidades organizativas y evaluar el grado en que se satisfacen dichas necesidades puede ayudar a una organización a planificar, implementar y vigilar un programa de ciberseguridad satisfactorio.

3.1 Identificación de las necesidades del personal de ciberseguridad

La ciberseguridad es un campo que cambia y se expande rápidamente. Para esta expansión, se requiere un grupo de empleados capacitados que ayuden a la organización a desempeñar las funciones de ciberseguridad. A medida que las organizaciones identifiquen lo que se necesita para gestionar adecuadamente el riesgo actual y futuro a la ciberseguridad, los dirigentes deberán considerar las competencias y capacidades necesarias del personal de ciberseguridad.

La Figura 2 ilustra la manera en que el Marco de la NICE sirve de referencia central para ayudar a los empleadores a formar personal de ciberseguridad capaz y preparado.

Figura 2: Elementos básicos de un personal de ciberseguridad capaz y preparado

Las flechas circulares en la parte izquierda de la Figura 2 son actividades que probablemente repercutan en la capacidad de una organización para formar personal capaz y preparado:

- Usar el léxico común del Marco de la NICE aclara la comunicación entre educadores, instructores o certificadores, empleadores y empleados en el campo de la ciberseguridad.
- Efectuar un análisis de criticidad identificará los CHC y las tareas esenciales para el desempeño competente de una función laboral determinada, y los CHC y las tareas clave para varias funciones laborales.
- Hacer un análisis de competencias guiará las expectativas de una organización en cuanto al nivel de los puestos (por ejemplo, nivel básico, experto), que suele incluir más de una función laboral. El análisis de competencias debe permitir refinar la selección de las

tareas pertinentes y los CHC necesarios para desempeñar las funciones laborales que conforman ese puesto.

El Apéndice C: identifica algunos recursos para la formación del personal existente que ayudan a definir las necesidades del personal de ciberseguridad.

3.2 Captación y contratación de talentos en ciberseguridad altamente capacitados

Consultar el Marco de la NICE ayudará a las organizaciones a planificar y contratar personal de manera estratégica. El uso del material del Marco de la NICE en la creación o revisión de las descripciones de puestos para anuncios de plazas vacantes y de empleo ayuda a los candidatos a solicitar los puestos específicos que les interesan, para los que están capacitados o cualificados. Las tareas que se usan para describir las obligaciones y responsabilidades de un puesto, y los CHC utilizados para describir las habilidades y cualificaciones necesarias para el puesto, deben permitir que los candidatos y los encargados de la contratación se comuniquen con más efectividad. Las descripciones de puestos y los anuncios de plazas vacantes en las que se usa la terminología del Marco de la NICE son compatibles con criterios de evaluación más uniformes para la investigación y aprobación de candidatos.

Con una revisión de la lista de tareas del Marco de la NICE, las organizaciones a las que les preocupen las deficiencias de personal pueden determinar las tareas específicas que no se están desempeñando en su organización. Esas tareas permiten a la organización identificar las deficiencias en las funciones laborales y áreas de especialización. La organización puede interactuar mejor con la comunidad de proveedores de educación, capacitación, credenciales y certificaciones que presentan sus productos o servicios en el Marco de la NICE. Asimismo, la organización determina la capacitación para que el personal existente corrija las deficiencias. Además, los encargados de la contratación que usan así los datos extraídos del Marco de la NICE pueden reconocer a los solicitantes que tengan los CHC para desempeñar tareas de ciberseguridad.

3.3 Educación y capacitación del personal de ciberseguridad

El Marco de la NICE identifica las tareas en las funciones laborales para que los educadores puedan preparar a los estudiantes con los CHC específicos con los que podrán demostrar su capacidad para desempeñar las tareas de ciberseguridad.

Las instituciones académicas son parte fundamental de la preparación y la educación del personal de ciberseguridad. La colaboración entre entidades públicas y privadas, como la colaboración por medio del programa de la NICE, facilita que esas instituciones determinen los conocimientos y las capacidades comunes que se necesitan. A su vez, al preparar e impartir planes de estudios armonizados con el léxico del Marco de la NICE, las instituciones prepararán a los estudiantes para que cuenten con las habilidades que necesitan los empleadores. A medida que aumente el número de estudiantes que encuentran los trabajos en ciberseguridad que desean, más estudiantes se interesarán en los programas académicos de ciberseguridad como una trayectoria profesional.

3.4 Retención y formación de talentos en ciberseguridad altamente capacitados

Un aspecto esencial del personal de ciberseguridad capacitado tiene que ver con la formación y la retención del talento experto ya contratado. Un empleado actual tiene las relaciones existentes, el conocimiento institucional y la experiencia organizativa que son difíciles de reemplazar. Llenar un puesto después de que un empleado se va puede acarrear nuevos costos de publicidad y contratación, gastos de capacitación, disminución de la productividad y el espíritu de trabajo. La siguiente lista muestra algunas de las maneras en que el Marco de la NICE contribuye a la retención y la formación de talentos de ciberseguridad:

- Las organizaciones pueden crear trayectorias profesionales que describan las cualificaciones necesarias para conjuntos de las funciones laborales que evolucionan y se vuelven cada vez más interesantes, como las enumeradas en el Marco de la NICE.
- El conocimiento detallado de los CHC y las tareas ayuda al personal existente a entender los pasos específicos que se necesitan para desarrollar sus capacidades, promoviendo la preparación para un puesto deseado.
- Una organización podría ofrecer rotaciones de personal que den oportunidades para la formación y el uso de habilidades nuevas.
- Las organizaciones pueden identificar al personal que mejora diligentemente los CHC en áreas pertinentes, y mostrar reconocimiento a quienes muestren buen desempeño.
- Las organizaciones pueden crear planes de formación o mejoramiento para el personal y ayudarle a determinar la manera de obtener los CHC necesarios para funciones laborales nuevas.
- Se pueden identificar oportunidades de capacitación en grupo para preparar al personal a fin de ampliar los conocimientos, habilidades y capacidades comunes en las funciones laborales de una organización.
- Las organizaciones pueden usar la capacitación y los exámenes que se basen en habilidades y capacidades específicas de ciberseguridad para evaluar la competencia en un entorno realista.
- Las organizaciones pueden emplear al personal existente para satisfacer necesidades críticas de dotación de personal de ciberseguridad, aprovechando la capacidad para revisar los currículos del personal existente e identificar a quienes posean los CHC que se desean.
- El Marco de la NICE es útil para los empleados existentes que desean avanzar a una función laboral de ciberseguridad desde otro puesto. Una organización podrá describir los CHC necesarios para que un empleado confiable, que desempeña una función laboral que no sea de ciberseguridad, pueda formar parte del personal de ciberseguridad y llevar a cabo tareas de esa índole.

4 Ampliaciones

Las organizaciones o sectores pueden utilizar el Marco de la NICE para elaborar publicaciones o herramientas adicionales que satisfagan sus necesidades y definan u ofrezcan orientación sobre diferentes aspectos de la formación, planificación, capacitación y educación del personal.

En el sitio web de la NICE [5], se intercambiarán nuevos recursos de referencia que hagan la referencia cruzada a los componentes del Marco de la NICE.

Estos ámbitos son algunos ejemplos a partir de los cuales se podrían crear publicaciones o herramientas adicionales.

4.1 Competencias

La Administración de Empleo y Capacitación del Departamento del Trabajo [6] define la competencia como la capacidad para aplicar o utilizar los conocimientos, habilidades, capacidades, comportamientos y características personales para desempeñar satisfactoriamente tareas esenciales de un trabajo, funciones específicas o una función o puesto determinado. Además de la enumeración de los CHC técnicos, los modelos de competencia también toman en cuenta los indicadores conductuales y describen las consideraciones no técnicas, como efectividad personal, competencias académicas y del lugar de trabajo. Véase más información sobre estas consideraciones en el sitio CareerOneStop del Departamento del Trabajo [7].

4.2 Cargos

Los cargos son descripciones de los trabajos o puestos de los empleados en una organización. Una asignación de ejemplos de los cargos a las áreas de especialización o las funciones laborales ayudaría a las organizaciones a usar el Marco de la NICE.

4.3 Documentos de orientación y directrices de ciberseguridad

La tercera meta estratégica de la NICE, Guiar la formación profesional y la planificación del personal, tiene por objeto asistir a los empleadores a tomar en cuenta las demandas del mercado y mejorar la captación, contratación, formación y retención de talentos de ciberseguridad. Un objetivo dentro de esta meta estratégica es publicar y promover el conocimiento del Marco de la NICE y su adopción. En este caso, adopción se refiere a usar el Marco de la NICE como recurso de referencia para las acciones relacionadas con el personal, la capacitación y la educación en materia de ciberseguridad.Una forma de fomentar la adopción del Marco de la NICE es animando a los autores de documentos de orientación o de directrices de ciberseguridad a que hagan la referencia cruzada del contenido de esos documentos a los componentes del Marco de la NICE. En el Apéndice D:, se describen tres ejemplos de publicaciones.

Apéndice A: Lista de componentes del Marco de la NICE

A.1 Categorías de personal del Marco de la NICE

En la Tabla 1, se describe cada Categoría detallada en el Marco de la NICE, y se incluye una abreviatura de dos caracteres (por ejemplo, SP) para hacer referencia rápida a la Categoría y ayudar a crear identificadores de las funciones laborales del Marco de la NICE (véase la Tabla 3: Funciones laborales del Marco de la NICE). Esta lista se actualizará periódicamente [1]. Véase la fuente definitiva de la versión más reciente de este material en la Hoja de cálculo de referencia para la Publicación especial 800-181 del NIST [4].

Tabla 1: Categorías de personal del Marco de la NICE

Categorías	Descripciones
Suministrar protección (SP)	Conceptualiza, diseña, procura o establece sistemas seguros de tecnología de la información (TI), asumiendo la responsabilidad de los aspectos de la organización de sistemas o de redes.
Operar y mantener (OM)	Proporciona la gestión y el mantenimiento necesarios para lograr que el funcionamiento y la seguridad del sistema de tecnología de la información (TI) sean efectivos y eficientes.
Supervisar y gobernar (OV)	Ofrece liderazgo, gestión, dirección o desarrollo y promoción para que la organización pueda llevar a cabo con efectividad el trabajo de ciberseguridad.
Proteger y defender (PR)	Identifica, analiza y mitiga las amenazas a los sistemas o las redes de tecnología de la información (TI) internos.
Analizar (AN)	Hace revisiones y evaluaciones muy especializadas de la información entrante sobre ciberseguridad a fin de determinar su utilidad para información de inteligencia.
Recolectar y operar (CO)	Efectúa operaciones especializadas de negación y engaño, y de recolección de información sobre ciberseguridad que pueda ser usada para generar inteligencia.
Investigar (IN)	Investiga los eventos de ciberseguridad o los delitos relacionados con sistemas, redes y pruebas digitales de tecnología de la información (TI).

A.2 Áreas de especialización del Marco de la NICE

En la Tabla 2, se describe cada una de las áreas de especialización del Marco de la NICE. Cada área de especialización cuenta con una abreviatura de tres caracteres (por ejemplo, RSK) para hacer referencia rápida al área de especialización y ayudar a crear identificadores de las funciones laborales del Marco de la NICE (véase la Tabla 3: Funciones laborales del Marco de la NICE). Esta lista se actualizará periódicamente [1]. Véase la fuente definitiva de la versión más reciente de este material en la Hoja de cálculo de referencia para la Publicación especial 800-181 del NIST [4].

Tabla 2: Áreas de especialización del Marco de la NICE

Categorías	Áreas de especialización	Descripciones de las áreas de especialización
Suministrar protección (SP)	Gestión de riesgos (RSK)	Supervisa, evalúa y ayuda a los procesos de documentación, validación, evaluación y autorización necesarios para comprobar que los sistemas de tecnología de la información (TI) existentes y nuevos cumplan los requisitos de ciberseguridad y de riesgo de la organización. Logra el tratamiento acertado del riesgo, el cumplimiento y la garantía desde perspectivas internas y externas.
	Desarrollo de software (DEV)	Elabora y escribe o codifica aplicaciones informáticas, software o programas de utilidades especializadas nuevos (o modifica los existentes) siguiendo las mejores prácticas de garantía de software.
	Arquitectura de sistemas (ARC)	Genera conceptos de sistemas y trabaja en las fases de las capacidades del ciclo de vida de desarrollo de sistemas; convierte la tecnología y las condiciones del entorno (por ejemplo, leyes y reglamentos) en diseños y procesos de sistemas y seguridad.
	Investigación y desarrollo tecnológicos (TRD)	Lleva a cabo procesos de evaluación e integración de la tecnología; proporciona y contribuye a la capacidad de un prototipo o evalúa su utilidad.
	Planificación de requisitos de sistemas (SRP)	Consulta con los clientes para obtener y evaluar los requisitos funcionales y convierte estos requisitos en soluciones técnicas. Ofrece orientación a los clientes sobre la aplicabilidad de los sistemas de información para satisfacer las necesidades empresariales.
	Prueba y evaluación (TST)	Prepara y efectúa pruebas de sistemas para evaluar el cumplimiento con las especificaciones y los requisitos aplicando principios y métodos para la planificación, evaluación, verificación y validación rentables de las características técnicas, funcionales y de rendimiento (incluida la interoperabilidad) de los sistemas o de los elementos de los sistemas que incorporan la TI.
	Desarrollo de sistemas (SYS)	Trabaja en las fases de desarrollo del ciclo de vida de desarrollo de sistemas.

Categorías	Áreas de especialización	Descripciones de las áreas de especialización
Operar y mantener (OM)	Administración de datos (DTA)	Programa y administra los sistemas de bases de datos o de gestión de datos que permiten almacenar, consultar, proteger y utilizar datos.
	Gestión del conocimiento (KMG)	Gestiona y administra procesos y herramientas para que la organización pueda identificar, documentar y acceder al capital intelectual y al contenido de la información.
	Servicio de atención al cliente y soporte técnico (STS)	Trata los problemas; instala, configura, soluciona problemas y proporciona mantenimiento y capacitación en respuesta a los requisitos o las consultas del cliente (por ejemplo, asistencia al cliente por niveles). Proporciona normalmente información inicial sobre incidentes a la especialización de Respuesta a incidentes (CIR).
	Servicios de red (NET)	Instala, configura, pone a prueba, maneja, mantiene y gestiona redes y sus firewalls, incluidos el hardware (por ejemplo, concentradores, puentes, conmutadores, multiplexores, enrutadores, cables, servidores proxy y sistemas protectores de distribución) y el software que permite compartir y transmitir todas las transmisiones de información del espectro que sostienen la seguridad de la información y los sistemas de información.
	Administración de sistemas (ADM)	Instala, configura, soluciona problemas y mantiene las configuraciones del servidor (hardware y software) para lograr su confidencialidad, integridad y disponibilidad. Gestiona cuentas, firewalls y parches. Se encarga del control de acceso, las contraseñas y la creación y administración de cuentas.
	Análisis de sistemas (ANA)	Estudia los sistemas y procedimientos informáticos actuales de una organización y diseña soluciones para los sistemas de información a fin de ayudar a la organización a funcionar de forma más segura, eficiente y efectiva. Integra la empresa y la tecnología de la información (TI) mediante el conocimiento de las necesidades y limitaciones de ambas.
Supervisar y gobernar (OV)	Asesoramiento legal y promoción (LGA)	Ofrece asesoramiento y recomendaciones legalmente acertadas a la dirección y al personal sobre una variedad de temas pertinentes dentro del tema. Promueve cambios legales y de políticas, y argumenta en nombre del cliente por medio de una gran variedad de productos de trabajo escritos y orales, así como instrucciones y procedimientos legales.
	Capacitación, educación y concientización (TEA)	Lleva a cabo la capacitación del personal en el tema pertinente. Elabora, planifica, coordina, imparte o evalúa cursos, métodos y técnicas de capacitación según corresponda.
	Gestión de ciberseguridad (MGT)	Supervisa el programa de ciberseguridad de un sistema o red de información, que incluye gestionar las implicaciones de la seguridad de la información dentro

Categorías	Áreas de especialización	Descripciones de las áreas de especialización
		de la organización, de un programa específico o de otra área de responsabilidad, como recursos estratégicos, personal, infraestructura, requisitos, cumplimiento de las políticas, planificación de emergencias, concientización de la seguridad y otros recursos.
	Políticas y planificación estratégica (SPP)	Elabora políticas y planes, o promueve cambios en las políticas compatibles con las iniciativas organizativas del ciberespacio o los cambios y mejoramientos necesarios.
	Dirección ejecutiva de cibernética (EXL)	Supervisa, gestiona o dirige el trabajo y el personal que desempeña trabajos de cibernética, o relacionados con esta, o las ciberoperaciones.
	Gestión de programas, proyectos y adquisiciones (PMA)	Aplica el conocimiento de datos, información, procesos, interacciones organizativas, habilidades y pericia analítica, así como de sistemas, redes y capacidades de intercambio de información para gestionar programas de adquisición. Desempeña las obligaciones que rigen los programas de adquisición de hardware, software y sistemas de información, así como otras políticas de gestión de programas. Ayuda directamente a las adquisiciones que usan la tecnología de la información (TI) (incluidos los sistemas nacionales de seguridad), aplicando las leyes y políticas relacionadas con la TI, y ofrece orientación relacionada con la TI en todo el ciclo de vida de la adquisición.
Proteger y defender (PR)	Análisis de la defensa de la ciberseguridad (CDA)	Emplea las medidas defensivas y la información recolectada de diversas fuentes para identificar y analizar los eventos que ocurren o podrían ocurrir dentro de la red, e informar de estos, a fin de proteger la información, los sistemas de información y las redes contra amenazas.
	Soporte de la infraestructura de defensa de la ciberseguridad (INF)	Pone a prueba, implementa, distribuye, mantiene, revisa y administra el hardware y el software de la infraestructura necesarios para gestionar efectivamente la red y los recursos del proveedor de servicios de defensa de las redes informáticas. Vigila la red para remediar activamente las actividades no autorizadas.
	Respuesta a incidentes (CIR)	Responde a crisis o situaciones urgentes dentro del dominio pertinente para mitigar amenazas inmediatas y potenciales. Utiliza métodos de mitigación, preparación, respuesta y recuperación, según sea necesario, para maximizar la supervivencia, la preservación de la propiedad y la seguridad de la información. Investiga y analiza todas las actividades de respuesta pertinentes.
	Evaluación y gestión de vulnerabilidades (VAM)	Lleva a cabo evaluaciones de amenazas y vulnerabilidades; determina las desviaciones de las configuraciones aceptables y de las políticas empresariales

Categorías	Áreas de especialización	Descripciones de las áreas de especialización
		o locales; evalúa el nivel de riesgo; y desarrolla o recomienda contramedidas de mitigación apropiadas en situaciones operativas y no operativas.
Analizar (AN)	Análisis de amenazas y advertencias (TWA)	Identifica y evalúa las capacidades y actividades de los delincuentes de la ciberseguridad o de entidades de inteligencia extranjera; produce resultados para dar inicio o ayudar a las investigaciones o actividades del orden público y la contrainteligencia.
	Análisis de explotación (EXP)	Analiza la información recolectada para identificar vulnerabilidades y posibilidades de explotación.
	Análisis de todas las fuentes (ASA)	Analiza la información acerca de amenazas proveniente de diversas fuentes, disciplinas y organismos en toda la comunidad de inteligencia. Sintetiza y contextualiza la información de inteligencia; extrae información sobre las posibles implicaciones.
	Objetivos (TGT)	Aplica los conocimientos actuales de una o más regiones, países, entidades no gubernamentales o tecnologías.
	Análisis lingüístico (LNG)	Aplica la experiencia lingüística, cultural y técnica para ayudar a la recolección y el análisis de información y demás actividades de ciberseguridad.
Recolectar y operar (CO)	Operaciones de recolección (CLO)	Efectúa la recolección utilizando estrategias apropiadas y dentro de las prioridades establecidas por medio del proceso de gestión de la recolección.
	Planificación ciberoperativa (OPL)	Implementa un proceso a fondo y conjunto de selección de objetivos y planificación de la ciberseguridad. Obtiene información y prepara órdenes y planes operativos detallados compatibles con los requisitos. Lleva a cabo planificaciones estratégicas y a nivel operativo en todo el espectro de las operaciones integradas de información y ciberespacio.
	Ciberoperaciones (OPS)	Lleva a cabo actividades de obtención de pruebas de entidades delictivas o de inteligencia extranjera para mitigar amenazas posibles o en tiempo real, proteger contra espionaje o contra amenazas internas, sabotaje extranjero y actividades terroristas internacionales, o para colaborar con otras actividades de inteligencia.
Investigar (IN)	Ciberinvestigación (INV)	Aplica tácticas, técnicas y procedimientos con una gama completa de herramientas y procesos de investigación que incluyen, entre otros, técnicas de entrevistas e interrogatorios, vigilancia, contravigilancia y detección de vigilancia, y equilibra debidamente las ventajas del proceso penal y la obtención de inteligencia.
	Investigación forense digital (FOR)	Recolecta, procesa, conserva, analiza y presenta pruebas digitales compatibles con la mitigación de vulnerabilidades de la red o a las investigaciones penales, policiales, de fraude o de contrainteligencia.

A.3 Funciones laborales del Marco de la NICE

En la Tabla 3, se describe cada una de las funciones laborales detalladas en el Marco de la NICE. Cada función laboral se identifica por medio de la Categoría y el área de especialización, seguidos de un número secuencial (por ejemplo, SP-RSK-001 se refiere a la primera función laboral de la Categoría SP y del área de especialización RSK). Algunas de las descripciones de las funciones laborales provienen de documentos externos (por ejemplo, la instrucción 4009 del Comité de Sistemas de Seguridad Nacional [CNSS, por sus siglas en inglés]) e incluyen esa información en la columna de descripción. Esta lista se actualizará periódicamente [1]. Véase la fuente definitiva de la versión más reciente de este material en la Hoja de cálculo de referencia para la Publicación especial 800-181 del NIST [4].

Tabla 3: Funciones laborales del Marco de la NICE

Categoría	Área de especialización	Función laboral	Identificación de la función laboral	Descripción de la función laboral
Suministrar protección (SP)	Gestión de riesgos (RSK)	Funcionario que autoriza o representante que designa	SP-RSK-001	Funcionario o ejecutivo sénior con autoridad para asumir formalmente la responsabilidad de operar un sistema de información a un nivel aceptable de riesgo para las operaciones organizativas (incluida la misión, las funciones, la imagen o la reputación), los recursos organizativos, las personas, otras organizaciones y el país (instrucción 4009 del CNSS).
		Asesor de control de seguridad	SP-RSK-002	Lleva a cabo evaluaciones independientes y completas de los controles de seguridad administrativos, operativos y técnicos y de los mejoramientos hechos a los controles que se emplean en un sistema interior o heredado de tecnología de la información (TI) para determinar la efectividad general de los controles (según se define en la Publicación especial 800-37 del NIST).
	Desarrollo de software (DEV)	Desarrollador de software	SP-DEV-001	Elabora, crea, mantiene y escribe o codifica aplicaciones informáticas, software o programas especializados de utilidades nuevos (o modifica los existentes).

Categoría	Área de especialización	Función laboral	Identificación de la función laboral	Descripción de la función laboral
		Asesor de software seguro	SP-DEV-002	Analiza la seguridad de aplicaciones informáticas, software o programas especializados de utilidades nuevos o existentes, y proporciona resultados procesables.
	Arquitectura de sistemas (ARC)	Arquitecto empresarial	SP-ARC-001	Establece y mantiene los procesos de negocios, sistemas e información compatibles con las necesidades de la misión empresarial; elabora normas y requisitos relacionados con la tecnología de la información (TI) que describen las arquitecturas de referencia y del objetivo.
		Arquitecto de seguridad	SP-ARC-002	Comprueba que los requisitos de seguridad de las partes interesadas, necesarios para proteger que los procesos de la misión y de negocios de la organización se tengan suficientemente en cuenta en todos los aspectos de la arquitectura empresarial, incluidos los modelos de referencia, las arquitecturas de segmentos y soluciones, y los sistemas resultantes compatibles con los procesos de la misión y de negocios.
	Investigación y desarrollo tecnológicos (TRD)	Especialista en investigación y desarrollo	SP-TRD-001	Lleva a cabo la ingeniería de software y de sistemas y la investigación de sistemas de software para crear capacidades nuevas y lograr la integración total de la ciberseguridad. Lleva a cabo investigación tecnológica completa para evaluar las vulnerabilidades potenciales en los sistemas del ciberespacio.
	Planificación de requisitos de sistemas (SRP)	Planificador de requisitos de sistemas	SP-SRP-001	Consulta con los clientes para evaluar los requisitos funcionales y convertir esos requisitos en soluciones técnicas.
	Prueba y evaluación (TST)	Especialista en pruebas y evaluaciones de sistemas	SP-TST-001	Planifica, prepara y pone a prueba los sistemas para evaluar los resultados con respecto a las especificaciones y los requisitos, y para analizar los resultados de las pruebas e informar de estos.

Categoría	Área de especialización	Función laboral	Identificación de la función laboral	Descripción de la función laboral
	Desarrollo de sistemas (SYS)	Promotor de seguridad de sistemas de información	SP-SYS-001	Diseña, desarrolla, pone a prueba y evalúa la seguridad del sistema de información en todo el ciclo de vida de desarrollo de sistemas.
		Desarrollador de sistemas	SP-SYS-002	Diseña, desarrolla, pone a prueba y evalúa los sistemas de información en todo el ciclo de vida de desarrollo de sistemas.
Operar y mantener (OM)	Administración de datos (DTA)	Administrador de bases de datos	OM-DTA-001	Administra los sistemas de bases de datos o de gestión de datos que permiten almacenar, consultar, proteger y utilizar datos de manera segura.
		Analista de datos	OM-DTA-002	Examina datos de varias fuentes distintas con el fin de hacer recomendaciones sobre seguridad y privacidad. Diseña e implementa algoritmos, procesos de flujo de trabajo y diseños personalizados para los conjuntos de datos complejos de escala empresarial que se usan para modelado, extracción de datos e investigación.
	Gestión del conocimiento (KMG)	Administrador de conocimientos	OM-KMG-001	Se encarga de gestionar y administrar procesos y herramientas para que la organización pueda identificar, documentar y acceder al capital intelectual y al contenido de la información.
	Servicio de atención al cliente y soporte técnico (STS)	Especialista en soporte técnico	OM-STS-001	Proporciona soporte técnico a los clientes que necesitan ayuda para usar el hardware y el software a nivel de cliente según los componentes de los procesos organizativos establecidos o aprobados (es decir, un plan maestro de gestión de incidentes, cuando corresponda).
	Servicios de red (NET)	Especialista en operaciones de red	OM-NET-001	Planifica, implementa y maneja servicios y sistemas de redes, incluidos el hardware y los entornos virtuales.

Categoría	Área de especialización	Función laboral	Identificación de la función laboral	Descripción de la función laboral
	Administración de sistemas (ADM)	Administrador de sistemas	OM-ADM-001	Se encarga de configurar y mantener un sistema o componentes específicos de un sistema (por ejemplo, instalar, configurar y actualizar hardware y software; establecer y manejar cuentas de usuarios; supervisar o llevar a cabo tareas de copias de seguridad y recuperación; implementar controles de seguridad operativos y técnicos; y cumplir las políticas y los procedimientos de seguridad de la organización).
	Análisis de sistemas (ANA)	Analista de seguridad de sistemas	OM-ANA-001	Se encarga del análisis y desarrollo de la integración, las pruebas, operaciones y mantenimiento de la seguridad de los sistemas.
Supervisar y gobernar (OV)	Asesoramiento legal y promoción (LGA)	Asesor de derecho informático	OV-LGA-001	Ofrece asesoramiento jurídico y recomendaciones sobre temas pertinentes relacionados con el derecho informático.
		Funcionario de privacidad o administrador de cumplimiento de la privacidad	OV-LGA-002	Establece y supervisa el programa de cumplimiento de privacidad y al personal del programa de privacidad, respaldando el cumplimiento de la privacidad, la gobernanza y las políticas, y atiende las necesidades de respuesta a incidentes de los ejecutivos de privacidad y seguridad y de sus equipos.
	Capacitación, educación y concientización (TEA)	Promotor de planes de estudios de instrucción cibernética	OV-TEA-001	Diseña, planifica, coordina y evalúa cursos, métodos y técnicas de capacitación y educación en cibernética según las necesidades didácticas.
		Instructor de cibernética	OV-TEA-002	Diseña e imparte la capacitación o la formación del personal en el campo de la cibernética.
	Gestión de ciberseguridad (MGT)	Administrador de seguridad de sistemas de información	OV-MGT-001	Se encarga de la ciberseguridad de un programa, organización, sistema o enclave.
		Administrador de seguridad de las comunicaciones (COMSEC, por sus siglas en inglés)	OV-MGT-002	Administra los recursos de seguridad de las comunicaciones (COMSEC) de una organización (instrucción 4009 del CNSS) o custodia las claves de un sistema de gestión de claves criptográficas (CKMS, por sus siglas en inglés).

Categoría	Área de especialización	Función laboral	Identificación de la función laboral	Descripción de la función laboral
	Políticas y planificación estratégica (SPP)	Organizador y administrador del personal de cibernética	OV-SPP-001	Formula planes, estrategias y orientación para el personal del ciberespacio a fin de satisfacer los requisitos de personal, capacitación y educación, y para adoptar los cambios de requisitos de políticas, doctrina, equipos, estructura del personal, educación y capacitación en materia de ciberespacio.
		Planificador de políticas y estrategias cibernéticas	OV-SPP-002	Elabora y mantiene planes, estrategias y políticas de ciberseguridad para adoptar y alinear las iniciativas organizativas de ciberseguridad y de cumplimiento reglamentario.
	Dirección ejecutiva de cibernética (EXL)	Director ejecutivo de cibernética	OV-EXL-001	Ejerce la autoridad para tomar decisiones y establece la visión y la dirección de los recursos o las operaciones de cibernética y afines a la cibernética de la organización.
	Gestión de programas, proyectos y adquisiciones (PMA)	Administrador de programas	OV-PMA-001	Dirige, coordina, comunica, integra y rinde cuentas del éxito general del programa, facilitando su compatibilidad con las prioridades del organismo o la empresa.
		Administrador de proyectos de tecnología de la información (TI)	OV-PMA-002	Administra directamente los proyectos de tecnología de la información.
		Administrador de soporte de productos	OV-PMA-003	Administra el paquete de funciones de soporte necesarias para establecer y mantener la preparación y la capacidad operativa de los sistemas y componentes.
		Administrador de inversiones y carteras de TI	OV-PMA-004	Gestiona una cartera de inversiones de TI que se ajuste a las necesidades generales de las prioridades de la empresa y la misión.
		Auditor de programas de TI	OV-PMA-005	Lleva a cabo evaluaciones de un programa de TI o de sus componentes individuales para determinar el cumplimiento con las normas publicadas.

Categoría	Área de especialización	Función laboral	Identificación de la función laboral	Descripción de la función laboral
Proteger y defender (PR)	Análisis de la ciberdefensa (CDA)	Analista de ciberdefensa	PR-CDA-001	Usa los datos recolectados de una variedad de herramientas de ciberdefensa (por ejemplo, alertas del sistema de detección de intrusiones [IDS, por sus siglas en inglés], firewalls, registros de tráfico de red) para analizar los eventos que ocurren dentro de sus entornos con el fin de mitigar amenazas.
	Soporte de la infraestructura de ciberdefensa (INF)	Especialista en soporte de la infraestructura de ciberdefensa	PR-INF-001	Pone a prueba, implementa, distribuye, mantiene y administra el hardware y el software de la infraestructura.
	Respuesta a incidentes (CIR)	Coordinador de la respuesta a incidentes de defensa de la ciberseguridad	PR-CIR-001	Investiga, analiza y responde a incidentes de ciberseguridad dentro del entorno o enclave de la red.
	Evaluación y gestión de vulnerabilidades (VAM)	Analista de evaluaciones de vulnerabilidades	PR-VAM-001	Lleva a cabo evaluaciones de sistemas y redes dentro del entorno o enclave de la red e identifica los puntos donde esos sistemas o redes se desvían de las configuraciones aceptables, las políticas locales o las del enclave. Mide la efectividad de la arquitectura de defensa en profundidad contra las vulnerabilidades conocidas.
Analizar (AN)	Análisis de amenazas y advertencias (TWA)	Analista de amenazas y advertencias	AN-TWA-001	Establece ciberindicadores para mantener la concientización del estado sumamente dinámico del entorno operativo. Recolecta, procesa, analiza y difunde evaluaciones de ciberamenazas o advertencias.
	Análisis de explotación (EXP)	Analista de explotaciones	AN-EXP-001	Colabora para identificar las deficiencias en el acceso y la recolección que se puedan corregir por medio de actividades de recolección o preparación cibernéticas. Aprovecha todo recurso y técnica analítica autorizados para penetrar en las redes seleccionadas como objetivo.

Categoría	Área de especialización	Función laboral	Identificación de la función laboral	Descripción de la función laboral
	Análisis de todas las fuentes (ASA)	Analista de todas las fuentes	AN-ASA-001	Analiza datos o información de una o varias fuentes para llevar a cabo la preparación del entorno, responder a las solicitudes de información y presentar los requisitos de recolección de inteligencia y producción compatibles con la planificación y las operaciones.
		Especialista en evaluaciones de misiones	AN-ASA-002	Elabora planes de evaluación y medidas del rendimiento o la efectividad. Lleva a cabo evaluaciones estratégicas y operativas de la efectividad según sea necesario para los eventos cibernéticos. Determina si los sistemas funcionan según lo previsto y aporta información para determinar la efectividad operativa.
	Objetivos (TGT)	Desarrollador de objetivos	AN-TGT-001	Efectúa análisis de sistemas de objetivos, establece o mantiene carpetas electrónicas de objetivos que incluyan las aportaciones hechas a la preparación de entornos o las fuentes de inteligencia internas o externas. Se coordina con las organizaciones de inteligencia y actividades de objetivos de los socios, y presenta los objetivos candidatos a investigación y validación.
		Analista de redes de objetivos	AN-TGT-002	Lleva a cabo análisis avanzados de recolección y datos de código abierto para lograr la continuidad de objetivos, generar perfiles de objetivos y sus actividades, y establecer técnicas para obtener más información sobre objetivos. Determina la manera en que los objetivos se comunican, se desplazan, operan y viven en función del conocimiento de sus tecnologías y redes digitales, y las aplicaciones sobre estos.

Categoría	Área de especialización	Función laboral	Identificación de la función laboral	Descripción de la función laboral
	Análisis lingüístico (LNG)	Analista lingüístico multidisciplinario	AN-LNG-001	Aplica la experiencia lingüística y cultural, junto con conocimientos técnicos y sobre amenazas u objetivos, para procesar, analizar o difundir información de inteligencia proveniente de material lingüístico, gráfico o de voz. Establece y mantiene bases de datos y ayudas de trabajo específicas del idioma para facilitar la ejecución de acciones cibernéticas y lograr el intercambio de conocimientos críticos. Aporta experiencia en el tema a proyectos interdisciplinarios o con uso intensivo de idiomas extranjeros.
Recolectar y operar (CO)	Operaciones de recolección (CLO)	Administrador de recolección de todas las fuentes	CO-CLO-001	Identifica las autoridades y el entorno de recolección, incorpora los requisitos de información prioritarios en la gestión de recolección y establece conceptos para lograr los objetivos de la dirección. Determina las capacidades de los recursos de recolección disponibles, define nuevas capacidades de recolección y elabora y difunde planes de recolección. Vigila la ejecución de la tarea asignada de recolección para lograr la ejecución efectiva del plan de recolección.
		Administrador de requisitos de recolección de todas las fuentes	CO-CLO-002	Evalúa las operaciones de recolección y elabora estrategias para los requisitos de recolección en función de los efectos utilizando las fuentes y los métodos disponibles para mejorar la recolección. Elabora, procesa, valida y coordina la presentación de los requisitos de recolección. Evalúa el rendimiento de los recursos de recolección y las operaciones de recolección.

Categoría	Área de especialización	Función laboral	Identificación de la función laboral	Descripción de la función laboral
	Planificación ciberoperativa (OPL)	Planificador de ciberinteligencia	CO-OPL-001	Elabora planes de inteligencia detallados para satisfacer los requisitos de las ciberoperaciones. Colabora con los planificadores de las ciberoperaciones para identificar, validar e imponer requisitos de recolección y análisis. Participa en la selección, validación y sincronización de objetivos, y en la ejecución de acciones cibernéticas. Sincroniza las actividades de inteligencia para lograr los objetivos de la organización en el ciberespacio.
		Planificador de ciberoperaciones	CO-OPL-002	Elabora planes detallados para llevar a cabo o respaldar la gama aplicable de ciberoperaciones mediante la colaboración con otros planificadores, operadores o analistas. Participa en la selección, validación y sincronización de objetivos, y facilita la integración durante la ejecución de acciones cibernéticas.
		Planificador de la integración de los socios	CO-OPL-003	Trabaja para promover la cooperación entre los socios de las ciberoperaciones a través de las fronteras organizativas o nacionales. Contribuye a la integración de los equipos cibernéticos de socios ofreciendo orientación, recursos y colaboración para establecer las mejores prácticas y facilitar el respaldo organizativo a fin de lograr los objetivos de las acciones cibernéticas integradas.
	Ciberoperaciones (OPS)	Ciberoperador	CO-OPS-001	Lleva a cabo la recolección, procesamiento o geolocalización de sistemas para aprovechar las vulnerabilidades, ubicar o dar seguimiento a los objetivos de interés. Efectúa navegación de redes y análisis forenses tácticos y, cuando se le ordena, ejecuta las operaciones en las redes.

Categoría	Área de especialización	Función laboral	Identificación de la función laboral	Descripción de la función laboral
Investigar (IN)	Ciberinvestigación (INV)	Investigador de ciberdelitos	IN-INV-001	Identifica, recolecta, analiza y preserva pruebas utilizando técnicas analíticas y de investigación controladas y documentadas.
	Investigación forense digital (FOR)	Analista forense policial y de contrainteligencia	IN-FOR-001	Lleva a cabo investigaciones a fondo sobre delitos informáticos estableciendo pruebas documentales o físicas, incluidos los medios y registros digitales asociados con incidentes de ciberintrusiones.
		Analista forense de ciberdefensa	IN-FOR-002	Analiza pruebas digitales e investiga incidentes de seguridad informática para obtener información útil compatible con la mitigación de vulnerabilidades del sistema o la red.

A.4 Tareas del Marco de la NICE

La Tabla 4 proporciona una lista de todas las tareas que se han identificado como parte de una función laboral de ciberseguridad. Cada función laboral incluye un subconjunto de las tareas enumeradas aquí. Esta lista se actualizará periódicamente [1]. Véase la fuente definitiva de la versión más reciente de este material en la Hoja de cálculo de referencia para la Publicación especial 800-181 del NIST [4].

Tabla 4: Tareas del Marco de la NICE

Id. de la tarea	Descripción de la tarea
T0001	Adquirir y gestionar los recursos necesarios, lo que incluye ayuda de la dirección, recursos financieros y personal de seguridad clave, para lograr los objetivos y las metas de seguridad de la tecnología de la información (TI) y reducir el riesgo general de la organización.
T0002	Adquirir los recursos necesarios, incluidos los recursos financieros, para operar un programa efectivo de continuidad de operaciones de la empresa.
T0003	Asesorar a la alta dirección (por ejemplo, el director de sistemas de información [CIO]) acerca de los niveles de riesgo y la postura de seguridad.
T0004	Asesorar a la alta dirección (por ejemplo, el CIO) sobre el análisis de costos y beneficios de los programas, políticas, procesos, sistemas y elementos de la seguridad de la información.
T0005	Asesorar a la dirección sénior correspondiente, o al funcionario que autoriza, acerca de los cambios que afectan la postura de ciberseguridad de la organización.
T0006	Defender la postura oficial de la organización en procedimientos jurídicos y legislativos.
T0007	Analizar y definir los requisitos y las especificaciones de datos.
T0008	Analizar y planificar los cambios previstos en los requisitos de la capacidad de datos.
T0009	Analizar información para determinar, recomendar y planificar la elaboración de una nueva aplicación o la modificación de una aplicación existente.
T0010	Analizar las políticas y configuraciones de ciberdefensa de la organización y evaluar el cumplimiento con las directivas y los reglamentos organizativos.
T0011	Analizar las necesidades de los usuarios y los requisitos de software para determinar la factibilidad del diseño considerando las limitaciones de tiempo y costo.
T0012	Analizar las limitaciones de diseño; analizar las compensaciones y el diseño detallado del sistema y la seguridad; y considerar el respaldo al ciclo de vida.
T0013	Aplicar normas de codificación y pruebas; emplear herramientas de pruebas de seguridad, incluidas las herramientas de escaneo de análisis estático de códigos mediante pruebas de vulnerabilidad ante datos aleatorios o inesperados (*fuzzing*); y hacer revisiones de códigos.
T0014	Emplear documentación de código seguro.
T0015	Aplicar políticas de seguridad en aplicaciones interconectadas, como las aplicaciones de empresa a empresa (B2B, por sus siglas en inglés).
T0016	Aplicar políticas de seguridad para cumplir los objetivos de seguridad del sistema.
T0017	Aplicar los principios de la arquitectura de seguridad orientada al servicio para cumplir los requisitos de confidencialidad, integridad y disponibilidad de la organización.
T0018	Evaluar la efectividad de las medidas de ciberseguridad que utilizan los sistemas.
T0019	Evaluar las amenazas a los sistemas informáticos y sus vulnerabilidades para elaborar un perfil de riesgo a la seguridad.
T0020	Elaborar contenido para las herramientas de ciberdefensa.
T0021	Diseñar, poner a prueba y modificar prototipos de productos utilizando modelos de trabajo o modelos teóricos.

Id. de la tarea	Descripción de la tarea
T0022	Captar los controles de seguridad utilizados durante la fase de requisitos para integrar la seguridad en el proceso, identificar los objetivos de seguridad clave y maximizar la seguridad del software, minimizando las interrupciones en planes y calendarios.
T0023	Caracterizar y analizar el tráfico de la red para identificar actividad anómala y amenazas potenciales a los recursos de la red.
T0024	Recolectar y mantener los datos necesarios para cumplir con la preparación de informes de ciberseguridad del sistema.
T0025	Comunicar el valor de la seguridad de la tecnología de la información (TI) a todos los niveles de las partes interesadas de la organización.
T0026	Compilar y redactar documentación acerca de la elaboración de un programa y de las revisiones subsiguientes, insertando comentarios en las instrucciones codificadas para que otros puedan entender el programa.
T0027	Analizar archivos de registros, pruebas y demás información a fin de determinar los mejores métodos para identificar a los perpetradores de una intrusión en la red.
T0028	Llevar a cabo o respaldar las pruebas de penetración autorizadas en los activos de la red empresarial.
T0029	Llevar a cabo pruebas funcionales y de conectividad para comprobar la operatividad continua.
T0030	Llevar a cabo ejercicios de capacitación interactivos para crear un ambiente efectivo de aprendizaje.
T0031	Entrevistar a víctimas y testigos, y efectuar entrevistas o interrogatorios de sospechosos.
T0032	Hacer evaluaciones del impacto en la privacidad del diseño de seguridad (PIA, por sus siglas en inglés) de la aplicación para los controles de seguridad apropiados que protegen la confidencialidad e integridad de la información de identificación personal (PII, por sus siglas en inglés).
T0033	Llevar a cabo análisis de riesgos, estudios de factibilidad o análisis de compensaciones para establecer, documentar y refinar los requisitos y las especificaciones funcionales.
T0034	Consultar con analistas, ingenieros y programadores de sistemas, y otras personas, para diseñar aplicaciones y obtener información sobre limitaciones y capacidades, requisitos de rendimiento e interfaces de un proyecto.
T0035	Configurar y optimizar los concentradores, enrutadores y conmutadores de la red (por ejemplo, protocolos de nivel superior, túneles).
T0036	Confirmar lo que se conoce sobre una intrusión y descubrir información nueva, de ser posible, después de identificar la intrusión por medio de un análisis dinámico.
T0037	Crear rutas de acceso a conjuntos de información (por ejemplo, páginas de enlace) a fin de facilitar el acceso de los usuarios finales.
T0038	Desarrollar un modelo de las amenazas de acuerdo con las entrevistas y los requisitos de los clientes.
T0039	Consultar con los clientes para evaluar los requisitos funcionales.
T0040	Consultar con el personal de ingeniería para evaluar la interfaz entre el hardware y el software.
T0041	Coordinar y proporcionar soporte técnico experto a los técnicos de ciberdefensa de toda la empresa para resolver los incidentes de defensa de la ciberseguridad.
T0042	Coordinarse con los analistas de ciberdefensa con objeto de gestionar y administrar la actualización de normas y firmas (por ejemplo, sistemas de detección de intrusiones o de protección contra estas, antivirus y listas negras de contenido) para las aplicaciones especializadas de ciberdefensa.

Id. de la tarea	Descripción de la tarea
T0043	Coordinarse con el personal de ciberdefensa de toda la empresa para validar las alertas de red.
T0044	Colaborar con las partes interesadas para crear el programa de continuidad de operaciones, la estrategia y la garantía de la misión de la empresa.
T0045	Coordinarse con arquitectos y diseñadores de sistemas, según sea necesario, para supervisar el desarrollo de soluciones de diseño.
T0046	Corregir errores haciendo los cambios necesarios, y volver a verificar el programa para comprobar que se logren los resultados deseados.
T0047	Correlacionar los datos de incidentes para identificar vulnerabilidades específicas y hacer recomendaciones que faciliten su corrección inmediata.
T0048	Crear duplicados forenses apropiados de las pruebas (es decir, imágenes forenses) para evitar que las pruebas originales se modifiquen involuntariamente, y usarlos en en los procesos de recuperación y análisis de datos. Esto incluye, entre otros, discos duros, disquetes, discos compactos, agendas electrónicas, teléfonos móviles, sistemas de posicionamiento global y todos los formato de cintas.
T0049	Descifrar datos incautados utilizando medios técnicos.
T0050	Definir y priorizar las capacidades esenciales del sistema o las funciones de negocios necesarias para la restauración parcial o total del sistema después de un evento de falla catastrófica.
T0051	Definir los niveles apropiados de disponibilidad del sistema de acuerdo con las funciones críticas de este, y comprobar que los requisitos del sistema identifiquen los requisitos apropiados de recuperación ante desastres y de continuidad de operaciones, incluidos los requisitos de conmutación por error o de sitio alternativo adecuado, requisitos de copias de seguridad y requisitos de compatibilidad de materiales para la recuperación o restauración del sistema.
T0052	Definir el alcance y los objetivos del proyecto en función de los requisitos del cliente.
T0053	Diseñar y crear productos de ciberseguridad o habilitados para la ciberseguridad.
T0054	Formular políticas de grupo y listas de control de acceso para garantizar la compatibilidad con las normas, las normas empresariales y las necesidades de la organización.
T0055	Diseñar hardware, sistemas operativos y aplicaciones de software para atender adecuadamente los requisitos de ciberseguridad.
T0056	Diseñar o integrar las capacidades apropiadas de copias de seguridad de datos en los diseños generales del sistema, y comprobar que existan los debidos procesos técnicos y de procedimiento para la protección de las copias de seguridad del sistema y del almacenamiento de los datos de las copias de seguridad.
T0057	Diseñar, establecer y modificar sistemas de software, utilizando análisis científicos y modelos matemáticos para predecir y medir los resultados y las consecuencias del diseño.
T0058	Determinar el nivel de garantía de las capacidades desarrolladas en función de los resultados de pruebas.
T0059	Formular un plan para investigar presuntos delitos, infracciones o actividades sospechosas por medio de computadoras e internet.
T0060	Adquirir conocimiento de las necesidades y los requisitos de información de los usuarios finales.
T0061	Establecer y dirigir los procedimientos y la documentación para las pruebas y la validación de sistemas.
T0062	Determinar y documentar los requisitos, las capacidades y las limitaciones de los procedimientos y los procesos de diseño.

Id. de la tarea	Descripción de la tarea
T0063	Establecer y documentar los procedimientos operativos estándar de la administración de sistemas.
T0064	Revisar y validar los programas, procesos y requisitos de extracción y almacenamiento de datos.
T0065	Elaborar e implementar procedimientos relativos a copias de seguridad y recuperación de la red.
T0066	Elaborar y mantener planes estratégicos.
T0067	Diseñar arquitecturas o componentes de sistemas de acuerdo con las especificaciones técnicas.
T0068	Formular normas, políticas y procedimientos relativos a datos.
T0069	Elaborar documentación detallada sobre el diseño de seguridad para las especificaciones de componentes e interfaces de acuerdo con el diseño y el desarrollo del sistema.
T0070	Elaborar planes de recuperación ante desastres y de continuidad de operaciones para los sistemas en desarrollo y verificar que se prueben antes de introducir los sistemas a un entorno de producción.
T0071	Elaborar e integrar diseños de ciberseguridad para sistemas y redes con requisitos de seguridad de varios niveles o requisitos para el procesamiento de niveles de datos de varias clasificaciones aplicables principalmente a organizaciones gubernamentales (por ejemplo, SIN CLASIFICAR, SECRETO y ULTRASECRETO).
T0072	Establecer métodos para vigilar y medir las iniciativas de riesgos, cumplimiento y garantía.
T0073	Elaborar materiales nuevos para promover el conocimiento y la capacitación, o identificar los existentes, que sean apropiados para el público al que van dirigidos.
T0074	Formular políticas, programas y directrices sobre implementación.
T0075	Proporcionar un resumen técnico de las conclusiones, de conformidad con los procedimientos establecidos para la preparación de informes.
T0076	Formular estrategias de mitigación de riesgos para resolver vulnerabilidades y recomendar cambios de seguridad en el sistema o los componentes de este, según sea necesario.
T0077	Diseñar códigos seguros y control de errores.
T0078	Establecer contramedidas específicas de ciberseguridad y estrategias de mitigación de riesgos para sistemas o aplicaciones.
T0079	Elaborar especificaciones para comprobar que las iniciativas de riesgos, cumplimiento y garantía se ajusten a los requisitos de seguridad, resiliencia y confiabilidad, a nivel de la aplicación del software, el sistema y el entorno de la red.
T0080	Elaborar planes para pruebas que incluyan las especificaciones y los requisitos.
T0081	Diagnosticar problemas de conectividad de red.
T0082	Documentar y tomar en cuenta los requisitos de seguridad de la información, arquitectura de la ciberseguridad e ingeniería de la seguridad de sistemas de la organización durante todo el ciclo de vida de la adquisición.
T0083	Redactar declaraciones acerca de los riesgos a la seguridad preliminares o residuales para el funcionamiento del sistema.
T0084	Emplear procesos seguros para la gestión de configuraciones.
T0085	Comprobar que todas las operaciones de seguridad y las actividades de mantenimiento de los sistemas estén debidamente documentadas y actualizadas según sea necesario.
T0086	Comprobar que la aplicación de parches de seguridad para los productos comerciales integrados en el diseño del sistema cumpla el calendario prescrito por la autoridad de gestión para el entorno operativo previsto.

Id. de la tarea	Descripción de la tarea
T0087	Comprobar que se siga la cadena de custodia para todos los medios digitales adquiridos de conformidad con las Normas federales sobre pruebas.
T0088	Comprobar que los productos habilitados para la ciberseguridad u otras tecnologías compensadoras para el control de seguridad reduzcan los riesgos identificados a un nivel aceptable.
T0089	Comprobar que las acciones de mejoramiento de la seguridad se evalúen, validen e implementen según sea necesario.
T0090	Comprobar que las arquitecturas y los sistemas adquiridos o desarrollados sean compatibles con las directrices de la arquitectura de ciberseguridad de la organización.
T0091	Comprobar que las inspecciones, pruebas y revisiones de ciberseguridad estén coordinadas para el entorno de la red.
T0092	Comprobar que los requisitos de ciberseguridad estén integrados en la planificación de continuidad de ese sistema o de las organizaciones.
T0093	Comprobar que las capacidades de protección y detección se adquieran o desarrollen usando el método de ingeniería de seguridad de los sistemas de información y que sean compatibles con la arquitectura de ciberseguridad a nivel de organización.
T0094	Establecer y mantener canales de comunicación con las partes interesadas.
T0095	Establecer la arquitectura de seguridad de la información empresarial (EISA, por sus siglas en inglés) con la estrategia de seguridad general de la organización.
T0096	Establecer relaciones, si corresponde, entre el equipo de respuesta a incidentes y otros grupos, tanto internos (por ejemplo, el departamento legal) como externos (por ejemplo, organismos del orden público, proveedores, profesionales de relaciones públicas).
T0097	Evaluar y aprobar las iniciativas de desarrollo y comprobar que las salvaguardias de seguridad de referencia se instalen correctamente.
T0098	Evaluar los contratos para lograr el cumplimiento con los requisitos legales, de financiación y de programas.
T0099	Evaluar los análisis económicos, de costos y beneficios y de riesgos en el proceso de toma de decisiones.
T0100	Evaluar factores como los formatos de informes requeridos, las limitaciones de costos y la necesidad de restricciones de seguridad para determinar la configuración del hardware.
T0101	Evaluar la efectividad y la integridad de los programas de capacitación existentes.
T0102	Evaluar la efectividad de las leyes, reglamentos, políticas, normas o procedimientos.
T0103	Examinar los datos recuperados para obtener información pertinente al problema en cuestión.
T0104	Combinar los análisis de ataques a redes informáticas con las investigaciones y operaciones penales y de contrainteligencia.
T0105	Identificar componentes o elementos, asignar funciones de seguridad a esos elementos y describir las relaciones entre estos.
T0106	Identificar estrategias alternativas de seguridad de la información para cumplir el objetivo de seguridad de la organización.
T0107	Identificar y dirigir soluciones a los problemas técnicos que se descubran durante las pruebas y la implementación de sistemas nuevos (por ejemplo, identificar y buscar soluciones para protocolos de comunicación que no sean interoperables).
T0108	Identificar y priorizar las funciones de negocios críticas en colaboración con las partes interesadas de la organización.
T0109	Identificar y priorizar las funciones o sistemas secundarios esenciales del sistema necesarios y compatibles con las capacidades o las funciones de negocios indispensables para restaurar o recuperar el sistema después de un error o durante un evento de

Id. de la tarea	Descripción de la tarea
	recuperación del sistema en función de los requisitos generales de continuidad y disponibilidad de este.
T0110	Identificar o determinar si un incidente de seguridad indica una infracción de la ley que requiera una acción legal específica.
T0111	Identificar defectos de codificación básicos y comunes en un nivel alto.
T0112	Identificar datos o información de inteligencia de valor probatorio para ayudar a las investigaciones penales y de contrainteligencia.
T0113	Identificar las pruebas digitales que deban ser examinadas y analizadas de manera que se evite una alteración involuntaria.
T0114	Identificar los elementos probatorios del delito.
T0115	Identificar las implicaciones de las nuevas tecnologías o actualizaciones tecnológicas en los programas de seguridad de la tecnología de la información (TI).
T0116	Identificar a las partes interesadas de las políticas organizativas.
T0117	Identificar las implicaciones de seguridad y emplear metodologías dentro de los entornos centralizados y descentralizados de todos los sistemas informáticos de la empresa en la programación de software.
T0118	Identificar los problemas de seguridad relacionados con el funcionamiento y la gestión del software en estado estable e incorporar las medidas de seguridad que se deben tomar cuando un producto llega al final de su vida útil.
T0119	Identificar, evaluar y recomendar productos de ciberseguridad o habilitados para la ciberseguridad a fin de usarlos en un sistema y lograr que los productos recomendados cumplan con los requisitos de evaluación y validación de la organización.
T0120	Identificar, recolectar y obtener pruebas documentales o físicas, incluidos los medios y registros digitales asociados con incidentes, investigaciones y operaciones de ciberintrusiones.
T0121	Implementar nuevos procedimientos de diseño de sistemas, procedimientos de prueba y estándares de calidad.
T0122	Implementar diseños de seguridad para sistemas nuevos o existentes.
T0123	Implementar contramedidas específicas de ciberseguridad para sistemas o aplicaciones.
T0124	Incorporar soluciones para vulnerabilidades de ciberseguridad en los diseños de sistemas (por ejemplo, alertas de vulnerabilidades de ciberseguridad).
T0125	Instalar y mantener el software del sistema operativo del dispositivo de infraestructura de la red (por ejemplo, IOS, firmware).
T0126	Instalar o reemplazar los concentradores, enrutadores y conmutadores de la red.
T0127	Integrar y alinear las políticas de seguridad de la información o de ciberseguridad para facilitar que el análisis del sistema cumpla los requisitos de seguridad.
T0128	Integrar capacidades automatizadas para actualizar o aplicar parches al software del sistema cuando sea factible, y establecer procesos y procedimientos para la actualización manual y la aplicación de parches al software del sistema de acuerdo con los requisitos actuales y proyectados del calendario de parches para el entorno operativo del sistema.
T0129	Integrar sistemas nuevos en la arquitectura de red existente.
T0130	Interactuar con organizaciones externas (por ejemplo, organismos de asuntos públicos, personal del orden público, inspector general de mando o de componentes) para lograr la difusión correcta y exacta de la información sobre incidentes y otra información sobre defensa de redes informáticas.
T0131	Interpretar y aplicar leyes, reglamentos, políticas, normas o procedimientos a temas específicos.

Id. de la tarea	Descripción de la tarea
T0132	Interpretar o aprobar los requisitos de seguridad relativos a las capacidades de las nuevas tecnologías de la información.
T0133	Interpretar las características del incumplimiento para determinar su impacto sobre los niveles de riesgo o la efectividad general del programa de ciberseguridad de la empresa.
T0134	Dirigir las prioridades de seguridad de la tecnología de la información (TI) y alinearlas con la estrategia de seguridad.
T0135	Dirigir y supervisar el presupuesto, la dotación de personal y la contratación para la seguridad de la información.
T0136	Mantener la seguridad de referencia del sistema de acuerdo con las políticas de la organización.
T0137	Mantener el software de los sistemas de gestión de bases de datos.
T0138	Mantener conjunto de herramientas implementables para la auditoría de la ciberdefensa (por ejemplo, software y hardware de ciberdefensa especializados) que sirva de ayuda en las misiones de auditoría de la ciberdefensa.
T0139	Mantener servicios de replicación de directorios para que la información se pueda replicar automáticamente desde los servidores posteriores a las unidades anteriores a través de un enrutamiento optimizado.
T0140	Mantener el intercambio de información por medio de funciones de publicación, suscripción y alerta para que los usuarios puedan enviar y recibir información crítica según sea necesario.
T0141	Mantener los materiales de acreditación y garantía de los sistemas de información.
T0142	Mantener el conocimiento de políticas, reglamentos y documentos aplicables sobre cumplimiento y ciberdefensa que se relacionan específicamente con la auditoría de la ciberdefensa.
T0143	Hacer recomendaciones que se basen en los resultados de pruebas.
T0144	Gestionar cuentas, derechos de red y acceso a sistemas y equipos.
T0145	Gestionar y aprobar los paquetes de acreditación (por ejemplo, ISO/IEC 15026-2).
T0146	Gestionar la compilación, catalogación, almacenamiento en caché, distribución y recuperación de datos.
T0147	Gestionar la vigilancia de las fuentes de datos de seguridad de la información para mantener el conocimiento situacional de la organización.
T0148	Gestionar la publicación de orientación en materia de defensa de las redes informáticas (por ejemplo, órdenes de red con tiempo de cumplimiento [TCNO, por sus siglas en inglés], conceptos de operaciones, informes de analistas de red, modo deslizante de terminal no singular [NTSM, por sus siglas en ingles], órdenes de asignación de tareas de mantenimiento [MTO, por sus siglas en inglés]) de los grupos empresariales representados.
T0149	Gestionar el análisis de amenazas o de objetivos de la información sobre ciberdefensa y la producción de información sobre amenazas dentro de la empresa.
T0150	Vigilar y evaluar el cumplimiento con un sistema de los requisitos de seguridad, resiliencia y confiabilidad de la tecnología de la información (TI).
T0151	Vigilar y evaluar la efectividad de las salvaguardias de ciberseguridad de la empresa para comprobar que proporcionen el nivel de protección previsto.
T0152	Vigilar y mantener bases de datos para garantizar un rendimiento óptimo.
T0153	Vigilar la capacidad y el rendimiento de la red.
T0154	Vigilar e informar del uso de los activos y los recursos de la gestión del conocimiento.

Id. de la tarea	Descripción de la tarea
T0155	Documentar y remitir a una instancia superior los incidentes (incluidos el historial, estado y efecto potencial de los incidentes para llevar a cabo otras acciones) que puedan causar un impacto continuo e inmediato en el entorno.
T0156	Supervisar la gestión de configuraciones y hacer recomendaciones.
T0157	Supervisar el programa de capacitación y concientización sobre la seguridad de la información.
T0158	Participar en una evaluación de riesgos a la seguridad de la información durante el proceso de evaluación y autorización de la seguridad.
T0159	Participar en la formulación o modificación de los planes y requisitos del programa de ciberseguridad del entorno informático.
T0160	Aplicar parches a las vulnerabilidades de la red para lograr que la información esté protegida contra partes externas.
T0161	Hacer un análisis de los archivos de registros de diversas fuentes (por ejemplo, registros individuales de hosts, registros de tráfico de redes, registros de firewalls y registros del sistema de detección de intrusiones [IDS]) para identificar posibles amenazas a la seguridad de la red.
T0162	Hacer copias de seguridad y recuperación de bases de datos para garantizar la integridad de los datos.
T0163	Hacer evaluaciones de incidentes de defensa de la ciberseguridad que incluyan determinación del alcance, urgencia e impacto potencial; identificar la vulnerabilidad específica; y hacer recomendaciones que faciliten su corrección inmediata.
T0164	Hacer análisis y preparar informes de las tendencias de defensa de la ciberseguridad.
T0165	Hacer un análisis dinámico para hacer la “imagen” de arranque de una unidad (sin tener necesariamente la unidad original) y poder ver la intrusión como la haya visto el usuario, en el entorno nativo.
T0166	Hacer la correlación de eventos utilizando información obtenida de una variedad de fuentes dentro de la empresa para lograr el conocimiento situacional y determinar la efectividad de un ataque observado.
T0167	Hacer un análisis de firma de archivo.
T0168	Hacer la comparación hash usando como referencia la base de datos establecida.
T0169	Hacer pruebas de ciberseguridad de las aplicaciones o los sistemas desarrollados.
T0170	Hacer una recolección inicial de imágenes de calidad forense apropiada; examinarlas para determinar la posibilidad de mitigación y corrección en los sistemas empresariales.
T0171	Hacer pruebas de control de calidad integradas de la funcionalidad de la seguridad y los ataques a la resiliencia.
T0172	Hacer análisis forenses en tiempo real (por ejemplo, utilizando Helix junto con LiveView).
T0173	Hacer análisis de calendarios.
T0174	Hacer análisis de necesidades a fin de determinar las oportunidades para soluciones nuevas y mejoradas de los procesos de negocios.
T0175	Dirigir el manejo de incidentes de defensa de la ciberseguridad en tiempo real (por ejemplo, recolecciones forenses, correlación y seguimiento de intrusiones, análisis de amenazas y corrección directa de sistemas) para ayudar a los equipos desplegables de respuesta a incidentes (IRT, por sus siglas en inglés).
T0176	Hacer programaciones seguras e identificar defectos potenciales en los códigos para mitigar vulnerabilidades.
T0177	Hacer revisiones de seguridad, identificar deficiencias en la arquitectura de seguridad y elaborar un plan de gestión de riesgos a la seguridad.

Id. de la tarea	Descripción de la tarea
T0178	Hacer revisiones de seguridad e identificar las deficiencias en la arquitectura de seguridad que den lugar a recomendaciones para su inclusión en la estrategia de mitigación de riesgos.
T0179	Hacer análisis de medios estáticos.
T0180	Hacer la administración de sistemas en las aplicaciones y los sistemas especializados de ciberdefensa (por ejemplo, antivirus, auditoría y corrección) o dispositivos de red privada virtual (VPN, por sus siglas en inglés) que incluyan instalación, configuración, mantenimiento, copias de seguridad y restauración.
T0181	Hacer análisis de riesgos (por ejemplo, amenaza, vulnerabilidad y probabilidad de que ocurran) siempre que una aplicación o un sistema se someta a un cambio importante.
T0182	Hacer análisis de malware de nivel 1, 2 y 3.
T0183	Seguir los pasos de validación, comparar los resultados reales con los resultados previstos y analizar las diferencias para identificar el impacto y los riesgos.
T0184	Planificar y llevar a cabo revisiones de autorizaciones de seguridad y el desarrollo de casos de garantía para la instalación inicial de sistemas y redes.
T0185	Planificar y gestionar la distribución de proyectos de gestión del conocimiento.
T0186	Planificar, ejecutar y verificar la redundancia de datos y los procedimientos de recuperación del sistema.
T0187	Planificar y recomendar modificaciones o ajustes que se basen en los resultados del ejercicio o en el entorno del sistema.
T0188	Preparar informes de auditoría que identifiquen los resultados técnicos y de procedimiento, y proporcionar estrategias y soluciones recomendadas de corrección.
T0189	Preparar flujos de trabajo y diagramas detallados que describan la entrada, la salida y el funcionamiento lógico, y convertirlos en una serie de instrucciones codificadas en un lenguaje informático.
T0190	Preparar medios digitales para la creación de imágenes que aseguren la integridad de los datos (por ejemplo, bloqueadores de escritura de acuerdo con los procedimientos operativos estándar).
T0191	Preparar casos de uso para justificar la necesidad de soluciones específicas de tecnología de la información (TI).
T0192	Preparar, distribuir y mantener planes, instrucciones, orientación y procedimientos operativos estándar relativos a la seguridad de las operaciones de los sistemas de redes.
T0193	Procesar lugares donde se cometieron delitos.
T0194	Documentar correctamente todas las actividades de implementación, operaciones y mantenimiento de la seguridad de los sistemas y actualizarlas según sea necesario.
T0195	Proporcionar un flujo gestionado de información pertinente (a través de portales web u otros medios) en función de los requisitos de la misión.
T0196	Ofrecer asesoramiento sobre los costos de proyectos, conceptos de diseño o cambios de diseño.
T0197	Proporcionar una evaluación técnica precisa de la aplicación del software, el sistema o la red, documentando la postura de seguridad, las capacidades y las vulnerabilidades con respecto al cumplimiento de ciberseguridad pertinente.
T0198	Proporcionar informes resumidos diarios de los eventos y actividades de la red correspondientes a las prácticas de ciberdefensa.
T0199	Impartir orientación sobre la ciberseguridad empresarial y la gestión de riesgos de la cadena de suministro para la elaboración de planes de continuidad de operaciones.
T0200	Proporcionar retroalimentación sobre los requisitos de la red, incluidas su arquitectura e infraestructura.

Id. de la tarea	Descripción de la tarea
T0201	Proporcionar directrices para implementar los sistemas desarrollados para clientes o equipos de instalación.
T0202	Impartir orientación sobre ciberseguridad a la dirección.
T0203	Aportar información sobre los requisitos de seguridad que se incluirán en las declaraciones de trabajo y otros documentos de adquisición necesarios.
T0204	Aportar información para los planes de implementación y los procedimientos operativos estándar.
T0205	Aportar información para las actividades del proceso del Marco de gestión de riesgos y la documentación correspondiente (por ejemplo, planes de soporte del ciclo de vida del sistema, concepto de operaciones, procedimientos operativos y materiales de capacitación para el mantenimiento).
T0206	Proporcionar liderazgo y dirección al personal de tecnología de la información (TI), facilitando que se impartan conocimientos, conceptos básicos, habilidades y capacitación en materia de ciberseguridad al personal de operaciones de acuerdo con sus responsabilidades.
T0207	Proporcionar de manera continua mejoramiento y asistencia para la solución de problemas.
T0208	Hacer recomendaciones para posibles mejoramientos y actualizaciones.
T0209	Hacer recomendaciones sobre estructuras de datos y bases de datos que aseguren la producción correcta y de calidad de informes e información administrativa.
T0210	Hacer recomendaciones sobre nuevas tecnologías y arquitecturas de bases de datos.
T0211	Aportar información relacionada con el sistema sobre los requisitos de ciberseguridad que se incluirán en las declaraciones de trabajo y otros documentos de adquisición apropiados.
T0212	Proporcionar ayuda técnica en asuntos de pruebas digitales al personal correspondiente.
T0213	Proporcionar a la sede superior documentos técnicos, informes de incidentes, resultados de análisis informáticos, resúmenes y demás información sobre el conocimiento situacional.
T0214	Recibir y analizar alertas de red de diversas fuentes dentro de la empresa y determinar las posibles causas de esas alertas.
T0215	Reconocer una posible infracción de seguridad y adoptar las medidas necesarias para informar del incidente, según proceda.
T0216	Reconocer y dar parte con precisión de artefactos forenses que sean indicativos de un sistema operativo en particular.
T0217	Considerar las implicaciones de seguridad en la fase de aceptación del software, incluidos criterios de finalización, aceptación y documentación de riesgos, criterios comunes y métodos de pruebas independientes.
T0218	Recomendar medidas nuevas o modificadas de seguridad, resiliencia y confiabilidad que se basen en los resultados de las revisiones.
T0219	Recomendar las asignaciones de recursos necesarias para operar y mantener de forma segura los requisitos de ciberseguridad de una organización.
T0220	Resolver conflictos en las leyes, reglamentos, políticas, normas o procedimientos.
T0221	Revisar los documentos de autorización y garantía para confirmar que el nivel de riesgo se encuentre dentro de los límites aceptables para cada aplicación de software, sistema y red.
T0222	Revisar las políticas existentes y propuestas con las partes interesadas.
T0223	Revisar o llevar a cabo auditorías de los programas y proyectos de tecnología de la información (TI).
T0224	Revisar la documentación de capacitación (por ejemplo, documentos del contenido del curso [CCD, por sus siglas en inglés], planes de lecciones, textos para los estudiantes,

Id. de la tarea	Descripción de la tarea
	exámenes, calendarios de instrucción [SOI, por sus siglas en inglés] y descripciones de cursos).
T0225	Proteger el dispositivo electrónico o la fuente de información.
T0226	Servir en las juntas de políticas institucionales e interinstitucionales.
T0227	Recomendar políticas y coordinar su revisión y aprobación.
T0228	Almacenar, recuperar y manejar datos para analizar las capacidades y los requisitos del sistema.
T0229	Supervisar o gestionar las medidas de protección o corrección cuando se descubra un incidente o vulnerabilidad de ciberseguridad.
T0230	Ayudar con el diseño y la ejecución de casos hipotéticos para ejercicios.
T0231	Ofrecer ayuda a las actividades de pruebas y evaluaciones de seguridad y certificación.
T0232	Poner a prueba y mantener la infraestructura de la red, incluidos los dispositivos de software y hardware.
T0233	Dar seguimiento y documentar los incidentes de defensa de la ciberseguridad desde el momento en que se detectan hasta su resolución final.
T0234	Dar seguimiento a los resultados y las recomendaciones de auditorías para comprobar que se adopten las medidas de mitigación apropiadas.
T0235	Convertir los requisitos funcionales en soluciones técnicas.
T0236	Convertir los requisitos de seguridad en elementos de diseño de aplicaciones, incluida la documentación de los elementos de las superficies de ataque del software, el modelado de amenazas y la definición de todo criterio de seguridad específico.
T0237	Solucionar problemas del hardware y el software del sistema.
T0238	Extraer datos usando técnicas de recuperación de datos (por ejemplo, Forensic Toolkit [FTK], Foremost).
T0239	Utilizar documentos publicados federales y específicos de la organización para gestionar las operaciones de los sistemas de su entorno informático.
T0240	Capturar y analizar el tráfico de la red asociado con actividades malintencionadas utilizando herramientas para vigilar la red.
T0241	Usar equipos y técnicas especializados para catalogar, documentar, extraer, recolectar, empaquetar y preservar pruebas digitales.
T0242	Usar modelos y simulacros para analizar o predecir el rendimiento del sistema en diferentes condiciones de funcionamiento.
T0243	Verificar y actualizar la documentación de seguridad que refleje las características de diseño de seguridad de la aplicación o el sistema.
T0244	Verificar que las posturas de seguridad del software, la red y el sistema de la aplicación se implementen según lo indicado, documenten las desviaciones y recomienden las medidas necesarias para corregir esas desviaciones.
T0245	Verificar que la documentación de acreditación y de garantía de la aplicación, la red y el sistema del software esté vigente.
T0246	Redactar y publicar técnicas, orientación e informes de defensa de la ciberseguridad sobre los resultados de incidentes para los grupos representados correspondientes.
T0247	Redactar materiales didácticos (por ejemplo, procedimientos operativos estándar, manual de producción) para impartir orientación detallada al personal correspondiente.
T0248	Promover el conocimiento de los problemas de seguridad entre la administración y comprobar que los principios de seguridad acertados se reflejen en la visión y las metas de la organización.
T0249	Investigar la tecnología actual para conocer las capacidades que requiere el sistema o la red.

Id. de la tarea	Descripción de la tarea
T0250	Identificar las estrategias de capacidades cibernéticas para el desarrollo de hardware y software personalizados en función de los requisitos de la misión.
T0251	Elaborar procesos de cumplimiento o auditorías de seguridad para los servicios externos (por ejemplo, proveedores de servicios en la nube, centros de datos).
T0252	Llevar a cabo las revisiones necesarias, según corresponda, dentro del entorno (por ejemplo, vigilancia técnica, revisiones de contramedidas [TSCM, por sus siglas en inglés], revisiones de contramedidas TEMPEST).
T0253	Llevar a cabo análisis binarios casuales.
T0254	Supervisar las políticas y las estrategias de implementación a fin de comprobar que los procedimientos y las directrices cumplan con las políticas de ciberseguridad.
T0255	Participar en el proceso de gobernanza de riesgos para presentar los riesgos de seguridad, mitigaciones y aportaciones de información sobre otros riesgos técnicos.
T0256	Evaluar la efectividad de la función de adquisiciones en la atención de los requisitos de la seguridad de la información y los riesgos de la cadena de suministro que presentan las actividades de adquisición, y recomendar mejoramientos.
T0257	Determinar el alcance, la infraestructura, los recursos y el tamaño de la muestra de datos para garantizar que se demuestren adecuadamente los requisitos del sistema.
T0258	Proporcionar detección, identificación y alerta oportunas de posibles ataques o intrusiones, actividades anómalas y actividades de uso indebido, y distinguir estos incidentes y eventos de las actividades benignas.
T0259	Usar herramientas de ciberdefensa para vigilar y analizar de manera continua la actividad del sistema a fin de detectar actividades malintencionadas.
T0260	Analizar las actividades malintencionadas detectadas para determinar las vulnerabilidades explotadas, los métodos de explotación y los efectos en el sistema y la información.
T0261	Ayudar a identificar, priorizar y coordinar la protección de la infraestructura de ciberdefensa crítica y los recursos clave.
T0262	Emplear los principios y las prácticas de defensa en profundidad aprobados (por ejemplo, defensa en varios lugares, defensas en capas, solidez de la seguridad).
T0263	Identificar los requisitos de seguridad específicos de un sistema de tecnología de la información (TI) en todas las fases del ciclo de vida del sistema.
T0264	Comprobar que se hayan establecido planes de acción e hitos o planes de corrección para las vulnerabilidades identificadas durante las evaluaciones de riesgos, auditorías, inspecciones, etc.
T0265	Comprobar la implementación y la funcionalidad correctas de los requisitos de seguridad y las políticas y los procedimientos de la tecnología de la información (TI) apropiados de acuerdo con la misión y las metas de la organización.
T0266	Efectuar las pruebas de penetración necesarias para las aplicaciones nuevas o actualizadas.
T0267	Diseñar contramedidas y medidas de mitigación contra la explotación potencial de las debilidades y vulnerabilidades del lenguaje de programación en el sistema y los elementos.
T0268	Definir y documentar la manera en que la implementación de un nuevo sistema o las nuevas interfaces entre sistemas afectan la postura de seguridad del entorno actual.
T0269	Diseñar y establecer funciones clave de gestión (relacionadas con la ciberseguridad).
T0270	Analizar las necesidades y los requisitos de los usuarios para planificar y llevar a cabo el desarrollo de la seguridad del sistema.
T0271	Crear diseños de ciberseguridad para satisfacer necesidades operativas y factores ambientales específicos (por ejemplo, controles de acceso, aplicaciones automatizadas, operaciones en red, requisitos de alta integridad y disponibilidad, seguridad y

Id. de la tarea	Descripción de la tarea
	procesamiento de varios niveles de clasificaciones múltiples y procesamiento de información confidencial compartimentada).
T0272	Garantizar que el diseño de la seguridad y las actividades de desarrollo de la ciberseguridad estén debidamente documentados (proporcionando una descripción funcional de la implementación de la seguridad) y actualizados según sea necesario.
T0273	Identificar y documentar los riesgos de la cadena de suministro de los elementos críticos del sistema según corresponda.
T0274	Crear pruebas auditables de las medidas de seguridad.
T0275	Respaldar las actividades de cumplimiento necesarias (por ejemplo, comprobar que se sigan las directrices de configuración de seguridad del sistema, que se vigile el cumplimiento).
T0276	Participar en el proceso de adquisición según sea necesario, siguiendo las prácticas apropiadas de gestión de riesgos de la cadena de suministro.
T0277	Garantizar que todas las adquisiciones, compras y medidas de subcontratación adoptadas satisfagan los requisitos de seguridad de la información, de acuerdo con las metas de la organización.
T0278	Recolectar artefactos de intrusiones (por ejemplo, código fuente, malware, troyanos) y usar los datos descubiertos para facilitar la mitigación de los incidentes potenciales de defensa de la ciberseguridad dentro de la empresa.
T0279	Servir como perito técnico y de enlace con el personal del orden público, y explicar los detalles del incidente según sea necesario.
T0280	Validar continuamente la organización con respecto a las políticas, directrices, procedimientos, reglamentos y leyes para garantizar el cumplimiento.
T0281	Pronosticar las demandas de servicio continuas y comprobar que se revisen las suposiciones de seguridad según sea necesario.
T0282	Definir o implementar políticas y procedimientos para garantizar la protección de la infraestructura crítica según corresponda.
T0283	Colaborar con las partes interesadas para identificar o desarrollar la tecnología de soluciones apropiada.
T0284	Diseñar y desarrollar nuevas herramientas y tecnologías relacionadas con la ciberseguridad.
T0285	Llevar a cabo detecciones de virus en los medios digitales.
T0286	Efectuar análisis forenses de sistemas de archivos.
T0287	Efectuar un análisis estático para montar la “imagen” de una unidad (sin tener necesariamente la unidad original).
T0288	Efectuar análisis estáticos de malware.
T0289	Usar herramientas implementables de análisis forense para ayudar a las operaciones según sea necesario.
T0290	Determinar las tácticas, técnicas y procedimientos (TTP, por sus siglas en inglés) para los conjuntos de intrusiones
T0291	Analizar las topologías de red para entender los flujos de datos a través de la red.
T0292	Recomendar correcciones a las vulnerabilidades del entorno informático.
T0293	Identificar y analizar las anomalías en el tráfico de la red mediante el uso de metadatos.
T0294	Llevar a cabo investigaciones, análisis y correlaciones en una amplia variedad de conjuntos de datos de origen (indicaciones y advertencias).
T0295	Validar las alertas del sistema de detección de intrusiones (IDS) tomando como referencia el tráfico de la red y empleando herramientas de análisis de paquetes.
T0296	Aislar y eliminar malware.

Id. de la tarea	Descripción de la tarea
T0297	Identificar las aplicaciones y sistemas operativos de un dispositivo de red en función del tráfico de la red.
T0298	Reconstruir un ataque o actividad malintencionados en función del tráfico de la red.
T0299	Identificar las actividades de asignación de la red y de creación de huellas digitales del sistema operativo (SO).
T0300	Establecer y documentar los requisitos de la experiencia de usuario (UX), entre los que figuran la arquitectura de la información y los requisitos de la interfaz de usuario.
T0301	Establecer e implementar procesos independientes de auditoría de la ciberseguridad para software, redes y sistemas de aplicaciones. Supervisar las auditorías independientes continuas para comprobar que los procesos y procedimientos operativos y de investigación y desarrollo cumplan con los requisitos de ciberseguridad obligatorios de la organización, y que los administradores de sistemas y demás personal de ciberseguridad los sigan con precisión en el desempeño de sus actividades diarias.
T0302	Establecer un lenguaje contractual para comprobar la seguridad de la cadena de suministro, el sistema, la red y las operaciones.
T0303	Identificar y aprovechar el sistema de control de versiones para toda la empresa mientras se diseñan y desarrollan aplicaciones seguras.
T0304	Implementar e integrar metodologías del ciclo de vida del desarrollo de sistemas (SDLC, por sus siglas en inglés) (por ejemplo, el proceso racional unificado de IBM) en el entorno de desarrollo.
T0305	Llevar a cabo la gestión de configuraciones, la gestión de problemas, la gestión de la capacidad y la gestión financiera de bases de datos y sistemas de gestión de datos.
T0306	Ayudar a la gestión de incidentes, la gestión de nivel de servicio, la gestión de cambios, la gestión de versiones, la gestión de la continuidad y la gestión de disponibilidad de bases de datos y de sistemas de gestión de datos.
T0307	Analizar arquitecturas candidatas, asignar servicios de seguridad y seleccionar mecanismos de seguridad.
T0308	Analizar los datos de incidentes de las tendencias emergentes.
T0309	Evaluar la efectividad de los controles de seguridad.
T0310	Ayudar en la construcción de firmas que puedan implementarse en herramientas de red de ciberdefensa en respuesta a amenazas nuevas u observadas dentro del entorno o el enclave de la red.
T0311	Consultar con los clientes sobre el diseño y el mantenimiento de los sistemas de software.
T0312	Coordinarse con los analistas de inteligencia para correlacionar los datos de las evaluaciones de amenazas.
T0313	Diseñar y documentar estándares de calidad.
T0314	Crear un contexto de seguridad del sistema, un concepto de operaciones preliminar de la seguridad del sistema (CONOPS, por sus siglas en inglés) y definir los requisitos de referencia de la seguridad del sistema según los requisitos de ciberseguridad aplicables.
T0315	Elaborar e impartir capacitación técnica para educar a otros o para satisfacer las necesidades de los clientes.
T0316	Elaborar o ayudar a elaborar módulos o clases de capacitación por computadora.
T0317	Elaborar o ayudar a elaborar las tareas de los cursos.
T0318	Elaborar o ayudar a elaborar las evaluaciones de los cursos.
T0319	Elaborar o ayudar a elaborar los estándares de calificaciones y competencias.
T0320	Ayudar con la elaboración de planes de formación, capacitación o corrección individuales o colectivos.
T0321	Elaborar o ayudar a elaborar los objetivos y las metas de aprendizaje.

Id. de la tarea	Descripción de la tarea
T0322	Elaborar o ayudar a elaborar materiales o programas de capacitación en el trabajo.
T0323	Elaborar o ayudar a elaborar pruebas escritas para medir y evaluar la competencia del estudiante.
T0324	Dirigir la programación de software y la redacción de documentación.
T0325	Documentar el propósito de un sistema y el concepto de operaciones preliminar de la seguridad del sistema.
T0326	Emplear procesos de gestión de configuraciones.
T0327	Evaluar las vulnerabilidades de la infraestructura de la red para mejorar las capacidades que se estén desarrollando.
T0328	Evaluar las arquitecturas y los diseños de seguridad para determinar la idoneidad del diseño y la arquitectura de seguridad propuestos o suministrados en respuesta a los requisitos que figuran en los documentos de adquisición.
T0329	Seguir las normas y los procesos del ciclo de vida de ingeniería del software y los sistemas.
T0330	Mantener seguros los sistemas de entrega de mensajes.
T0331	Mantener el seguimiento de incidentes y la base de datos de soluciones.
T0332	Informar a los administradores designados, coordinadores de la respuesta a incidentes de ciberseguridad y a los miembros del equipo de proveedores de servicios de ciberseguridad de presuntos incidentes de ciberseguridad, y comunicar el historial, el estado y el impacto potencial del evento para adoptar medidas adicionales de acuerdo con el plan de respuesta a los incidentes de ciberseguridad de la organización.
T0334	Comprobar que todos los componentes del sistema se puedan integrar y alinear (por ejemplo, procedimientos, bases de datos, políticas, software y hardware).
T0335	Fabricar, instalar, configurar y poner a prueba el hardware dedicado de ciberdefensa.
T0336	Retirado: se integró en T0228.
T0337	Supervisar y asignar el trabajo a programadores, diseñadores, tecnólogos y técnicos, así como a otro personal científico y de ingeniería.
T0338	Redactar especificaciones funcionales detalladas que documenten el proceso de desarrollo de la arquitectura.
T0339	Dirigir iniciativas que promuevan el uso de la gestión del conocimiento y el intercambio de información de la organización.
T0340	Intervenir como parte interesada principal en los procesos y las funciones operativas subyacentes de la tecnología de la información (TI) que contribuyan al servicio, brinden orientación y vigilen todas las actividades importantes para que el servicio se preste sin problemas.
T0341	Promover la financiación adecuada de recursos de capacitación en cibernética que incluyan cursos internos e impartidos por el sector, instructores y materiales afines.
T0342	Analizar las fuentes de datos para ofrecer recomendaciones procesables.
T0343	Analizar las crisis para cuidar la protección del público, el personal y los recursos.
T0344	Evaluar todos los procesos de gestión de configuraciones (gestión de la configuración de cambios y de versiones).
T0345	Evaluar la efectividad y la eficiencia de la instrucción, de acuerdo con la facilidad de uso de la tecnología de enseñanza y el aprendizaje de los estudiantes, la transferencia de conocimientos y la satisfacción.
T0346	Evaluar el comportamiento de víctimas, testigos o sospechosos individuales en relación con una investigación.
T0347	Evaluar la validez de los datos de origen y los resultados posteriores.

Id. de la tarea	Descripción de la tarea
T0348	Ayudar a evaluar el impacto de la implementación y el mantenimiento de una infraestructura dedicada de ciberdefensa.
T0349	Recolectar métricas y datos de tendencias.
T0350	Llevar a cabo un análisis del mercado para identificar, evaluar y recomendar productos comerciales, productos ya existentes del gobierno y productos de código abierto para su uso en un sistema, y lograr que los productos recomendados cumplan con los requisitos de evaluación y validación de la organización.
T0351	Comprobar hipótesis utilizando procesos estadísticos.
T0352	Llevar a cabo evaluaciones de las necesidades de aprendizaje e identificar requisitos.
T0353	Consultar con analistas, ingenieros, programadores y demás personal de los sistemas para diseñar aplicaciones.
T0354	Coordinar y gestionar el servicio general que se presta a un cliente de extremo a extremo.
T0355	Coordinarse con expertos en el tema internos y externos para procurar que los estándares de cualificación existentes reflejen los requisitos funcionales de la organización y cumplan con los estándares del sector.
T0356	Coordinarse con las partes interesadas del personal de la organización para facilitar que se asignen y distribuyan apropiadamente los recursos del capital humano.
T0357	Elaborar ejercicios de aprendizaje interactivos para crear un ambiente efectivo de aprendizaje.
T0358	Diseñar y desarrollar la funcionalidad de administración y gestión de sistemas para usuarios con acceso privilegiado.
T0359	Diseñar, implementar, poner a prueba y evaluar interfaces seguras entre sistemas de información, sistemas físicos o tecnologías insertadas.
T0360	Determinar el alcance de las amenazas y recomendar medidas o contramedidas para mitigar los riesgos.
T0361	Establecer y facilitar métodos para obtención de datos.
T0362	Redactar e implementar descripciones normalizadas de puestos que se basen en las funciones laborales cibernéticas establecidas.
T0363	Establecer y revisar los procedimientos de captación, contratación y retención de acuerdo con las políticas actuales de RR. HH.
T0364	Organizar una estructura de clasificación del campo profesional cibernético que incluya el establecimiento de requisitos para ingresar al campo profesional y otra nomenclatura, como códigos e identificadores.
T0365	Elaborar o ayudar a elaborar las políticas y los protocolos de capacitación para la capacitación en cibernética.
T0366	Elaborar perspectivas estratégicas a partir de grandes conjuntos de datos.
T0367	Establecer las metas y los objetivos para el plan de estudios en cibernética.
T0368	Comprobar que los campos profesionales cibernéticos se gestionen de acuerdo con las directivas y las políticas de los RR. HH. de la organización.
T0369	Comprobar que las políticas y los procesos de gestión del personal de cibernética cumplan con los requisitos legales y organizativos relacionados con la igualdad de oportunidades, diversidad y prácticas justas de contratación y empleo.
T0370	Comprobar que se definan acuerdos de nivel de servicio (SLA, por sus siglas en inglés) y contratos de soporte fundamentales apropiados que describan claramente para el cliente el servicio y las medidas destinadas a la vigilancia del servicio.
T0371	Establecer límites aceptables para la aplicación del software, la red o el sistema.

Id. de la tarea	Descripción de la tarea
T0372	Establecer y recolectar métricas para vigilar y validar la preparación del personal de cibernética, incluido el análisis de los datos de ese personal a fin de evaluar el estado de los puestos identificados, ocupados y los ocupados con personal cualificado.
T0373	Establecer y supervisar los procesos de exención para el ingreso en el campo profesional cibernético y los requisitos de capacitación para la cualificación.
T0374	Establecer las trayectorias profesionales en cibernética para el avance profesional, el desarrollo deliberado y el crecimiento dentro de los campos profesionales cibernéticos y entre estos.
T0375	Establecer normas de recursos humanos, personal y elementos de datos de cualificación compatibles con la gestión del personal de cibernética y los requisitos de preparación de informes.
T0376	Establecer, implementar y evaluar programas de gestión del personal de cibernética, y aportar recursos a esos programas, de acuerdo con los requisitos de la organización.
T0377	Obtener retroalimentación sobre la satisfacción del cliente y el rendimiento interno del servicio para fomentar el mejoramiento continuo.
T0378	Incorporar un proceso de actualización del mantenimiento de sistemas basado en riesgos para solventar las deficiencias del sistema (de manera periódica y fuera de ciclo).
T0379	Coordinar la relación interna con los propietarios de los procesos de tecnología de la información (TI) que contribuyen al servicio, facilitando la definición y aceptación de los acuerdos de nivel de operación (OLA, por sus siglas en inglés).
T0380	Planificar, junto con educadores y capacitadores, estrategias de instrucción como conferencias, demostraciones, ejercicios interactivos, presentaciones multimedia y cursos en video y en internet para lograr los ambientes más efectivos de aprendizaje.
T0381	Presentar información técnica al público técnico y no técnico.
T0382	Presentar datos en formatos creativos.
T0383	Programar algoritmos personalizados.
T0384	Promover entre la administración el conocimiento de las políticas y estrategias cibernéticas, según corresponda, y comprobar que se reflejen principios sólidos en la misión, la visión y las metas de la organización.
T0385	Hacer recomendaciones procesables a las partes interesadas decisivas en función del análisis de datos y resultados.
T0386	Ofrecer ayuda de investigación penal a los abogados durante el proceso judicial.
T0387	Revisar y aplicar los estándares de cualificación del campo profesional cibernético.
T0388	Revisar y aplicar las políticas organizativas relacionadas con el personal de cibernética o que influyan en este.
T0389	Revisar los informes de rendimiento del servicio, identificando todo problema y variación de importancia, y, cuando sea necesario, iniciar la aplicación de medidas correctivas y verificar que se dé seguimiento a todos los problemas pendientes.
T0390	Revisar o evaluar la efectividad del personal de cibernética para ajustar las habilidades o los estándares de cualificación.
T0391	Ayudar a la integración del personal cualificado de cibernética en los procesos de desarrollo del ciclo de vida de los sistemas de información.
T0392	Utilizar documentación o recursos técnicos para implementar un nuevo método matemático, de ciencia de datos o de informática.
T0393	Validar las especificaciones y los requisitos para la comprobación.
T0394	Colaborar con los demás administradores de servicios y propietarios de productos para equilibrar y priorizar los servicios a fin de cumplir los requisitos, las restricciones y los objetivos generales del cliente.

Id. de la tarea	Descripción de la tarea
T0395	Escribir y publicar análisis posteriores a una acción.
T0396	Procesar imágenes con las herramientas correctas en función de las metas del analista.
T0397	Efectuar análisis del registro de Windows.
T0398	Llevar a cabo la vigilancia de archivos y del registro en el sistema en ejecución después de identificar una intrusión mediante un análisis dinámico.
T0399	Ingresar información de medios en la base de datos de seguimiento (por ejemplo, la herramienta Product Tracker Tool) para los medios digitales que se hayan adquirido.
T0400	Correlacionar los datos de incidentes y preparar informes de ciberdefensa.
T0401	Mantener un conjunto de herramientas implementables de ciberdefensa (por ejemplo, software y hardware de ciberdefensa especializados) para ayudar a la misión del equipo de respuesta a incidentes.
T0402	Asignar con efectividad capacidad de almacenamiento en el diseño de sistemas de gestión de datos.
T0403	Leer, interpretar, escribir, modificar y ejecutar secuencias de comandos simples (por ejemplo, Perl, VBScript) en sistemas Windows y UNIX (por ejemplo, los que ejecutan tareas como análisis de archivos de datos extensos, automatización de tareas manuales y obtención o procesamiento de datos remotos).
T0404	Usar diferentes lenguajes de programación para escribir código, abrir archivos, leer archivos y escribir archivos de salida distintos.
T0405	Usar lenguaje de código abierto, como R, y aplicar técnicas cuantitativas (por ejemplo, estadísticas descriptivas y deductivas, muestreo, diseño experimental, pruebas paramétricas y no paramétricas de diferencia, regresión de mínimos cuadrados ordinarios, línea general).
T0406	Comprobar que se documenten debidamente, y se actualicen según sea necesario, las actividades de diseño y desarrollo (proporcionando una descripción funcional de la implementación).
T0407	Participar en el proceso de adquisición según sea necesario.
T0408	Interpretar y aplicar las leyes, estatutos y documentos regulatorios correspondientes e integrarlos en políticas.
T0409	Solucionar problemas de diseño y procesos de prototipos durante las fases de diseño y desarrollo de un producto y antes de su lanzamiento.
T0410	Identificar las características funcionales y relacionadas con la seguridad en busca de oportunidades de desarrollo de nuevas capacidades para aprovechar o mitigar vulnerabilidades.
T0411	Identificar o diseñar herramientas de ingeniería inversa para mejorar las capacidades y detectar las vulnerabilidades.
T0412	Llevar a cabo revisiones de importaciones o exportaciones para adquirir sistemas y software.
T0413	Desarrollar capacidades de gestión de datos (por ejemplo, gestión centralizada de claves criptográficas basada en la nube) que incluyan asistencia al personal móvil.
T0414	Establecer los requisitos de la cadena de suministro, el sistema, la red, el rendimiento y la ciberseguridad.
T0415	Comprobar que los requisitos de la cadena de suministro, el sistema, la red, el rendimiento y la ciberseguridad se incluyan en el texto del contrato y se cumplan.
T0416	Habilitar las aplicaciones con claves públicas haciendo uso de las bibliotecas existentes de infraestructura de clave pública (PKI, por sus siglas en inglés) e incorporando las funcionalidades de cifrado y la gestión de certificados cuando corresponda.

Id. de la tarea	Descripción de la tarea
T0417	Identificar y hacer uso de los servicios de seguridad de toda la empresa en el diseño y desarrollo de aplicaciones seguras (por ejemplo, infraestructuras de clave pública de la empresa, servidores de identidad federada, antivirus de la empresa) cuando corresponda.
T0418	Instalar, actualizar y solucionar problemas de sistemas o servidores.
T0419	Adquirir y mantener un conocimiento práctico de las cuestiones constitucionales que surgen en las leyes, reglamentos, políticas, acuerdos, estándares, procedimientos y demás publicaciones pertinentes.
T0420	Administrar bancos de prueba y poner a prueba y evaluar las aplicaciones, infraestructuras de hardware, normas o firmas, controles de acceso y configuraciones de plataformas gestionadas por los proveedores de servicios.
T0421	Gestionar la indexación o catalogación, el almacenamiento y el acceso a conocimientos organizativos explícitos (por ejemplo, documentos impresos, archivos digitales).
T0422	Implementar las normas, requisitos y especificaciones de la gestión de datos.
T0423	Analizar las amenazas generadas por computadora en busca de actividades delictivas o de contrainteligencia.
T0424	Analizar y proveer información a las partes interesadas que ayudarán al desarrollo de una aplicación de seguridad o la modificación de una aplicación de seguridad existente.
T0425	Analizar la política sobre cibernética de la organización.
T0426	Analizar los resultados de las pruebas de software, hardware o interoperabilidad.
T0427	Analizar las necesidades y los requisitos del usuario para planificar la arquitectura.
T0428	Analizar las necesidades de seguridad y los requisitos del software para determinar la factibilidad del diseño en vista de las limitaciones de tiempo y costo, y los mandatos de seguridad.
T0429	Evaluar las necesidades de políticas y colaborar con las partes interesadas para formular políticas que rijan las actividades cibernéticas.
T0430	Obtener y preservar las pruebas que se utilicen en los juicios relacionados con delitos informáticos.
T0431	Comprobar la disponibilidad, funcionalidad, integridad y eficacia del hardware del sistema.
T0432	Recolectar y analizar artefactos de intrusiones (por ejemplo, código fuente, malware y configuraciones del sistema) y usar los datos descubiertos para habilitar la mitigación de los incidentes potenciales de defensa de la ciberseguridad dentro de la empresa.
T0433	Analizar archivos de registros, pruebas y demás información a fin de determinar los mejores métodos para identificar a los perpetradores de una intrusión en la red o de otros delitos.
T0434	Estructurar las declaraciones para identificar correctamente las presuntas infracciones de la ley, reglamentos, políticas u orientaciones.
T0435	Llevar a cabo el mantenimiento periódico del sistema, incluida limpieza (tanto física como electrónica), revisiones de discos, reinicios de rutinas, volcados de datos y pruebas.
T0436	Llevar a cabo ejecuciones de prueba de programas y aplicaciones de software para lograr que se genere la información deseada y que las instrucciones y los niveles de seguridad sean los correctos.
T0437	Correlacionar la capacitación y el aprendizaje con los requisitos de negocios o de la misión.
T0438	Crear, editar y gestionar listas de control de acceso a redes en los sistemas especializados de ciberdefensa (por ejemplo, firewalls y sistemas de prevención de intrusiones).
T0439	Detectar y analizar datos cifrados, estenografía, secuencias alternas de datos y demás formas de datos ocultos.

Id. de la tarea	Descripción de la tarea
T0440	Captar e integrar las capacidades esenciales del sistema o las funciones de negocios necesarias para la restauración parcial o total del sistema después de un evento de falla catastrófica.
T0441	Definir e integrar los entornos de la misión actuales y futuros.
T0442	Crear cursos de capacitación adaptados al público y al entorno físico.
T0443	Impartir cursos de capacitación adaptados al público y a los entornos físicos o virtuales.
T0444	Exponer a los estudiantes a conceptos, procedimientos, software, equipos o aplicaciones tecnológicas.
T0445	Diseñar o integrar una estrategia cibernética que describa la visión, la misión y las metas alineadas con el plan estratégico de la organización.
T0446	Diseñar, establecer, integrar y actualizar medidas de seguridad del sistema que proporcionen confidencialidad, integridad, disponibilidad y autenticación, y sin rechazo de estas.
T0447	Diseñar hardware, sistemas operativos y aplicaciones de software para satisfacer adecuadamente los requisitos.
T0448	Diseñar la arquitectura empresarial o los componentes del sistema requeridos para satisfacer las necesidades de los usuarios.
T0449	Diseñar los requisitos de seguridad para comprobar que se cumplan los requisitos de todos los sistemas o las aplicaciones.
T0450	Diseñar el plan de estudios de capacitación y el contenido del curso en función de los requisitos.
T0451	Participar en la elaboración del plan de estudios de capacitación y el contenido del curso.
T0452	Diseñar, desarrollar, implementar y mantener un marco de gestión del conocimiento que dé a los usuarios finales acceso al capital intelectual de la organización.
T0453	Determinar y descubrir pistas y fuentes de información para identificar o enjuiciar a los responsables de una intrusión o de otros delitos.
T0454	Definir los requisitos de referencia de la seguridad de acuerdo con las directrices aplicables.
T0455	Elaborar procedimientos, programación y documentación de pruebas y validación de sistemas de software.
T0456	Elaborar procedimientos seguros de pruebas y validación de software.
T0457	Elaborar procedimientos, programación y documentación de pruebas y validación del sistema.
T0458	Cumplir con los procedimientos operativos estándar de la administración de los sistemas de la organización.
T0459	Implementar las aplicaciones de extracción y almacenamiento de datos.
T0460	Desarrollar e implementar programas de extracción y almacenamiento de datos.
T0461	Implementar y hacer cumplir las políticas y los procedimientos acerca del uso de la red local.
T0462	Establecer procedimientos y poner a prueba la conmutación por error para la transferencia de operaciones del sistema a un sitio alternativo en función de los requisitos de disponibilidad del sistema.
T0463	Elaborar estimaciones de costos para sistemas nuevos o modificados.
T0464	Redactar documentación de diseño detallada para las especificaciones de componentes e interfaces que sea compatible con el diseño y el desarrollo del sistema.
T0465	Elaborar directrices para la implementación.
T0466	Establecer estrategias de mitigación para abordar costos, programas, rendimiento y riesgos a la seguridad.

Id. de la tarea	Descripción de la tarea
T0467	Comprobar que la capacitación cumpla los objetivos y las metas de capacitación, educación o concientización de la ciberseguridad.
T0468	Diagnosticar y resolver los incidentes, problemas y eventos del sistema denunciados por el cliente.
T0469	Analizar las tendencias de la postura de seguridad de la organización e informar de estas.
T0470	Analizar las tendencias de la postura de seguridad del sistema e informar de estas.
T0471	Documentar la condición original de las pruebas digitales o afines (por ejemplo, por medio de fotografías digitales, informes escritos, comprobación de la función hash).
T0472	Redactar y publicar las políticas sobre cibernética, y dotarlas de personal.
T0473	Documentar y actualizar, según sea necesario, todas las actividades de definición y arquitectura.
T0474	Proporcionar análisis y decisiones de índole jurídica a los inspectores generales, funcionarios de privacidad y personal de supervisión y cumplimiento acerca del cumplimiento con las políticas de ciberseguridad y los requisitos legales y normativos pertinentes.
T0475	Evaluar los controles de acceso adecuados según los principios de privilegios mínimos y de la necesidad de saber.
T0476	Evaluar el efecto de los cambios hechos a leyes, reglamentos, políticas, normas o procedimientos.
T0477	Facilitar la ejecución de la recuperación ante desastres y la continuidad de las operaciones.
T0478	Impartir orientación sobre leyes, reglamentos, políticas, normas o procedimientos a la administración, el personal o los clientes.
T0479	Emplear los sistemas de tecnología de la información (TI) y medios de almacenamiento digital para resolver, investigar o enjuiciar a los responsables de ciberdelitos y fraude cometidos contra personas y bienes.
T0480	Identificar componentes o elementos, asignar componentes funcionales completos, incluidas las funciones de seguridad, y describir las relaciones entre elementos.
T0481	Identificar y resolver los problemas de planificación y gestión del personal de cibernética (por ejemplo, captación, retención y capacitación).
T0482	Hacer recomendaciones que se basen en el análisis de tendencias para el mejoramiento de las soluciones de software y hardware con el fin de potenciar la experiencia del cliente.
T0483	Identificar conflictos potenciales con la implementación de cualquier herramienta de ciberdefensa (por ejemplo, pruebas y optimización de herramientas y firmas).
T0484	Determinar las necesidades de protección (es decir, los controles de seguridad) de los sistemas de información y las redes, y documentarlas debidamente.
T0485	Implementar medidas de seguridad para resolver vulnerabilidades, mitigar riesgos y recomendar cambios de seguridad en el sistema o los componentes del sistema, según sea necesario.
T0486	Implementar los requisitos del Marco de gestión de riesgos (RMF, por sus siglas en inglés) y de la evaluación y autorización de seguridad (SA&A, por sus siglas en inglés) para los sistemas dedicados de ciberdefensa dentro de la empresa, y documentar y mantener sus registros.
T0487	Facilitar la implementación de leyes, reglamentos, órdenes ejecutivas, políticas, normas o procedimientos nuevos o modificados.
T0488	Implementar diseños para sistemas nuevos o existentes.
T0489	Implementar medidas de seguridad del sistema de acuerdo con los procedimientos establecidos para comprobar la confidencialidad, integridad, disponibilidad y autenticación, y sin rechazo de estas.

Id. de la tarea	Descripción de la tarea
T0490	Instalar y configurar sistemas y software de gestión de bases de datos.
T0491	Instalar y configurar hardware, software y equipos periféricos para los usuarios de sistemas de acuerdo con los estándares de la organización.
T0492	Comprobar la integración y la implementación de soluciones entre dominios (CDS, por sus siglas en inglés) en un entorno seguro.
T0493	Dirigir y supervisar el presupuesto, la dotación de personal y la contratación.
T0494	Administrar cuentas, derechos de red y acceso a sistemas y equipos.
T0495	Gestionar paquetes de acreditación (por ejemplo, ISO/IEC 15026-2).
T0496	Efectuar la gestión de activos y el inventario de los recursos de tecnología de la información (TI).
T0497	Gestionar el proceso de planificación de tecnología de la información (TI) para comprobar que las soluciones planteadas cumplan los requisitos del cliente.
T0498	Gestionar los recursos del sistema o servidor, incluidos rendimiento, capacidad, disponibilidad, facilidad de mantenimiento y capacidad de recuperación.
T0499	Mitigar o corregir las deficiencias de la seguridad identificadas durante las pruebas de seguridad o de certificación, o recomendar la aceptación de riesgos al dirigente sénior o representante autorizado apropiado.
T0500	Modificar y mantener el software existente para corregir errores, adaptarlo a un hardware nuevo o actualizar las interfaces y mejorar el rendimiento.
T0501	Vigilar y mantener la configuración del sistema o servidor.
T0502	Vigilar el rendimiento del sistema informático a nivel de cliente e informar de este.
T0503	Vigilar las fuentes de datos externas (por ejemplo, sitios de proveedores de defensa de la ciberseguridad, equipos de respuesta a emergencias informáticas, grupos de discusión de seguridad) para estar al día de la condición de las amenazas a la defensa de la ciberseguridad y determinar los problemas de seguridad que podrían tener un impacto sobre la empresa.
T0504	Evaluar y vigilar la ciberseguridad relacionada con la implementación de sistemas y las prácticas de pruebas.
T0505	Vigilar la aplicación rigurosa de políticas, principios y prácticas de cibernética en la prestación de servicios de planificación y gestión.
T0506	Buscar el consenso de los interesados sobre los cambios de políticas propuestos.
T0507	Supervisar la instalación, implementación, configuración y soporte de los componentes del sistema.
T0508	Verificar que se hayan establecido los requisitos mínimos de seguridad para todas las aplicaciones.
T0509	Hacer una evaluación de los riesgos a la seguridad de la información.
T0510	Coordinar las funciones de respuesta a incidentes.
T0511	Efectuar pruebas de desarrollo en los sistemas en desarrollo.
T0512	Efectuar pruebas de interoperabilidad en los sistemas que intercambian información electrónica con otros sistemas.
T0513	Efectuar pruebas de funcionamiento.
T0514	Diagnosticar el hardware defectuoso del sistema o servidor.
T0515	Reparar el hardware defectuoso del sistema o servidor.
T0516	Efectuar pruebas, revisiones o evaluaciones de programas seguros para identificar defectos potenciales en los códigos y mitigar vulnerabilidades.
T0517	Integrar los resultados de la identificación de deficiencias en la arquitectura de seguridad.
T0518	Hacer revisiones de seguridad e identificar las deficiencias de seguridad en la arquitectura.

Id. de la tarea	Descripción de la tarea
T0519	Planificar y coordinar la impartición de técnicas y formatos en el aula (por ejemplo, conferencias, demostraciones, ejercicios interactivos, presentaciones multimedia) para lograr el ambiente más efectivo de aprendizaje.
T0520	Planificar técnicas y formatos educativos que se impartan fuera del aula (por ejemplo, cursos en video, mentores, cursos en internet).
T0521	Planificar la estrategia de implementación para comprobar que los componentes de la empresa se puedan integrar y alinear.
T0522	Preparar documentos jurídicos y otros documentos pertinentes (por ejemplo, exposiciones, informes, declaraciones juradas, declaraciones, apelaciones, alegatos, descubrimientos de pruebas).
T0523	Preparar informes para documentar una investigación siguiendo normas y requisitos legales.
T0524	Promover el intercambio de conocimientos entre propietarios y usuarios de la información mediante los sistemas y procesos operativos de una organización.
T0525	Impartir orientación a la cadena de suministro sobre la ciberseguridad empresarial y la gestión de riesgos.
T0526	Hacer recomendaciones de ciberseguridad a la dirección en función de las amenazas y vulnerabilidades importantes.
T0527	Aportar información para los planes de implementación y los procedimientos operativos estándar en relación con la seguridad de los sistemas de información.
T0528	Aportar información para los planes de implementación, los procedimientos operativos estándar, la documentación de mantenimiento y los materiales de capacitación sobre mantenimiento.
T0529	Impartir orientación en materia de políticas a los administradores, el personal y los usuarios de la cibernética.
T0530	Elaborar un análisis de tendencias y un informe de impactos.
T0531	Solucionar problemas de interfaz y de interoperabilidad del hardware o el software.
T0532	Revisar imágenes forenses y otras fuentes de datos (por ejemplo, datos volátiles) para recuperar información potencialmente pertinente.
T0533	Revisar, llevar a cabo o participar en auditorías de programas y proyectos cibernéticos.
T0534	Llevar a cabo revisiones o modificaciones periódicas del contenido de los cursos para determinar la precisión, integridad, correspondencia y vigencia (por ejemplo, documentos del contenido del curso, planes de lecciones, textos para los estudiantes, exámenes, calendarios de instrucción y descripciones de cursos).
T0535	Recomendar modificaciones de los planes de estudio y el contenido del curso de acuerdo con la retroalimentación obtenida de sesiones de capacitación previas.
T0536	Servir como consultor y asesor interno en su propio ámbito de experiencia (por ejemplo, tecnología, derechos de autor, medios impresos, medios electrónicos).
T0537	Ayudar al director de sistemas de información (CIO) en la formulación de políticas relacionadas con la cibernética.
T0538	Ofrecer ayuda a las actividades de prueba y evaluación.
T0539	Poner a prueba, evaluar y verificar el hardware o el software para determinar que cumpla con las especificaciones y requisitos definidos.
T0540	Registrar y gestionar los datos de las pruebas.
T0541	Rastrear los requisitos del sistema para diseñar componentes y hacer análisis de deficiencias.
T0542	Convertir las capacidades propuestas en requisitos técnicos.
T0544	Verificar la estabilidad, interoperabilidad, portabilidad o escalabilidad de la arquitectura de un sistema.

Id. de la tarea	Descripción de la tarea
T0545	Colaborar con las partes interesadas para resolver los incidentes de seguridad informática y el cumplimiento en materia de vulnerabilidades.
T0546	Redactar y publicar recomendaciones, informes y notas de productos de defensa de la ciberseguridad sobre los resultados de incidentes para los grupos representados correspondientes.
T0547	Investigar y evaluar las tecnologías y normas disponibles para satisfacer los requisitos de los clientes.
T0548	Ofrecer asesoramiento y aportar información para los planes de recuperación ante desastres, contingencia y continuidad de las operaciones.
T0549	Hacer evaluaciones técnicas (evaluación de la tecnología) y no técnicas (evaluación de personas y operaciones), de riesgos y vulnerabilidades de las áreas tecnológicas de enfoque pertinentes (por ejemplo, entorno informático local, redes e infraestructura, límites del enclave, infraestructura y aplicaciones compatibles).
T0550	Hacer recomendaciones sobre la selección de controles de seguridad rentables para mitigar los riesgos (por ejemplo, protección de la información, los sistemas y los procesos).
T0551	Redactar y publicar documentos acerca de la seguridad de la cadena de suministro y la gestión de riesgos.
T0552	Revisar y aprobar una política de gestión de riesgos o de seguridad de la cadena de suministro.
T0553	Aplicar las funciones de ciberseguridad (por ejemplo, cifrado, control del acceso y gestión de identidades) para reducir las oportunidades de explotación.
T0554	Determinar y documentar los parches de software o el alcance de las versiones que harían que el software quedara vulnerable.
T0555	Documentar la manera en que la implementación de un sistema o interfaz nuevos entre sistemas afectaría el entorno actual y de destino, lo que incluiría, entre otros aspectos, la postura de seguridad.
T0556	Evaluar y diseñar funciones de gestión de seguridad en relación con el ciberespacio.
T0557	Integrar funciones de gestión clave en relación con el ciberespacio.
T0558	Analizar las necesidades y los requisitos del usuario para planificar y llevar a cabo el desarrollo de sistemas.
T0559	Crear diseños para satisfacer necesidades operativas y factores del entorno específicos (por ejemplo, controles de acceso, aplicaciones automatizadas, operaciones en red).
T0560	Colaborar en los diseños de ciberseguridad para satisfacer necesidades operativas y factores del entorno específicos (por ejemplo, controles de acceso, aplicaciones automatizadas, operaciones en red, requisitos de alta integridad y disponibilidad, seguridad y procesamiento de varios niveles de clasificaciones múltiples y procesamiento de información confidencial compartimentada).
T0561	Describir con precisión los objetivos.
T0562	Ajustar las operaciones de recolección o el plan de recolección para considerar los problemas u obstáculos identificados, y sincronizar las recolecciones con los requisitos operativos generales.
T0563	Aportar información para el análisis, diseño, desarrollo o adquisición de las capacidades que se emplean para cumplir los objetivos.
T0564	Analizar la retroalimentación para determinar el alcance del cumplimiento de los productos y servicios de recolección con los requisitos.
T0565	Analizar las solicitudes de recolección entrantes.

Id. de la tarea	Descripción de la tarea
T0566	Analizar la arquitectura, las herramientas y los procedimientos operativos internos para mejorar el rendimiento.
T0567	Analizar la arquitectura operativa del objetivo en busca de maneras de obtener acceso.
T0568	Analizar planes, directivas, orientación y políticas en busca de factores que influirían en la estructura y los requisitos operativos de la gestión de la recolección (por ejemplo, duración, alcance, requisitos de comunicación, acuerdos interinstitucionales o internacionales).
T0569	Responder a las solicitudes de información.
T0570	Aplicar y usar las capacidades cibernéticas autorizadas para poder acceder a las redes seleccionadas como objetivo.
T0571	Aplicar la experiencia en políticas y procesos para facilitar la elaboración y negociación de planes o memorandos de acuerdo y la dotación de personal interno para estos.
T0572	Aplicar la experiencia en recolección, preparación de entornos y colaboración en el ámbito cibernético a fin de habilitar explotaciones nuevas o continuar las operaciones de recolección, o satisfacer los requisitos del cliente.
T0573	Evaluar y aplicar los factores y riesgos del entorno operativo al proceso de gestión de la recolección.
T0574	Aplicar y obedecer los estatutos, leyes, reglamentos y políticas correspondientes.
T0575	Coordinar la ayuda de inteligencia en las actividades de planificación operativa.
T0576	Evaluar inteligencia de todas las fuentes y recomendar objetivos compatibles con las metas de las ciberoperaciones.
T0577	Evaluar la eficacia de los sistemas de intercambio y gestión de la información existentes.
T0578	Evaluar el rendimiento de los recursos de recolección con respecto a las especificaciones prescritas.
T0579	Evaluar las vulnerabilidades del objetivo o las capacidades operativas para determinar el plan de acción.
T0580	Evaluar la efectividad de las recolecciones para solucionar las deficiencias de información prioritarias, utilizando las capacidades y los métodos disponibles, y ajustar las estrategias y los requisitos de recolección según corresponda.
T0581	Ayudar y asesorar a los socios interinstitucionales en la identificación y la elaboración de las mejores prácticas, para facilitar la asistencia operativa y lograr los objetivos de la organización.
T0582	Aportar experiencia a la preparación del plan de acción.
T0583	Aportar experiencia en el tema al establecimiento de una imagen operativa común.
T0584	Mantener una imagen de inteligencia común.
T0585	Aportar experiencia en el tema a la creación de indicadores específicos de ciberoperaciones.
T0586	Ayudar con la coordinación, validación y gestión de los requisitos, planes o actividades de recolección de todas las fuentes.
T0587	Ayudar con la elaboración y el refinamiento de los requisitos de información prioritarios.
T0588	Aportar experiencia a la elaboración de medidas de efectividad y de rendimiento.
T0589	Ayudar con la identificación de insuficiencias en la recolección de inteligencia.
T0590	Permitir la sincronización de los planes de soporte de inteligencia entre las organizaciones de socios según sea necesario.
T0591	Hacer análisis de las actividades de explotación de la infraestructura del objetivo.
T0592	Aportar información para identificar los criterios satisfactorios en materia cibernética.
T0593	Informar de las situaciones actuales de la amenaza o del objetivo.
T0594	Organizar y mantener carpetas electrónicas del objetivo.

Id. de la tarea	Descripción de la tarea
T0595	Clasificar los documentos de acuerdo con las directrices de clasificación.
T0596	Cerrar las solicitudes de información una vez que se hayan atendido.
T0597	Colaborar con las organizaciones de analistas de inteligencia y selección de objetivos que participan en áreas afines.
T0598	Colaborar con las organizaciones de desarrollo para crear e implementar las herramientas necesarias y lograr los objetivos.
T0599	Colaborar con otras organizaciones de clientes, inteligencia y selección de objetivos que participan en áreas cibernéticas afines.
T0600	Colaborar con otras organizaciones de socios internos y externos en los problemas operativos y de acceso a objetivos.
T0601	Colaborar con otros miembros del equipo u organizaciones de socios para preparar un programa diverso de materiales informativos (por ejemplo, páginas web, sesiones informativas, materiales impresos).
T0602	Colaborar con el cliente para definir los requisitos de información.
T0603	Comunicar a la dirección y a los clientes internos y externos los acontecimientos recientes, avances, problemas y lecciones aprendidas.
T0604	Comparar los recursos asignados y disponibles con la demanda de recolección expresada por medio de los requisitos.
T0605	Compilar las lecciones aprendidas al llevar a la práctica los objetivos de recolección organizativos de la actividad de gestión de recolección.
T0606	Compilar, integrar o interpretar los datos de todas las fuentes en busca de inteligencia o vulnerabilidades valiosas con respecto a objetivos específicos.
T0607	Identificar y llevar a cabo un análisis de las comunicaciones del objetivo para identificar la información esencial para las operaciones de soporte.
T0608	Llevar a cabo un análisis de tecnologías digitales, físicas y lógicas (por ejemplo, inalámbricas, sistemas de control de supervisión y adquisición de datos [SCADA, por sus siglas en inglés], telecomunicaciones) para identificar posibles vías de acceso.
T0609	Habilitar el acceso de computadores inalámbricas y redes digitales.
T0610	Recolectar y procesar redes informáticas inalámbricas y digitales.
T0611	Llevar a cabo evaluaciones al terminar las operaciones.
T0612	Llevar a cabo la explotación de redes informáticas inalámbricas y digitales.
T0613	Llevar a cabo la coordinación formal e informal de los requisitos de recolección de conformidad con las directrices y los procedimientos establecidos.
T0614	Llevar a cabo análisis independientes y detallados técnicos y del objetivo, que incluyan información específica acerca del objetivo (por ejemplo, cultural, organizativa, política) que dé lugar al acceso.
T0615	Llevar a cabo investigaciones y análisis detallados.
T0616	Llevar a cabo análisis de vulnerabilidades de sistemas y de rastreo de redes dentro de una red.
T0617	Llevar a cabo análisis nodales.
T0618	Llevar a cabo actividades en red para controlar y filtrar datos de las tecnologías implementadas.
T0619	Llevar a cabo actividades en red y fuera de la red para controlar y filtrar datos de las tecnologías automatizadas implementadas.
T0620	Recolectar datos de código abierto utilizando diversas herramientas en línea.
T0621	Llevar a cabo controles de calidad para determinar la validez y relevancia de la información obtenida acerca de redes.

Id. de la tarea	Descripción de la tarea
T0622	Elaborar, revisar e implementar todos los niveles de orientación sobre planificación compatibles con las ciberoperaciones.
T0623	Llevar a cabo un estudio de las redes informáticas y digitales.
T0624	Llevar a cabo investigaciones y análisis de objetivos.
T0625	Considerar la eficiencia y efectividad de los activos y los recursos de recolección cuando se aplican, o si se aplican, con respecto a los requisitos de información prioritarios.
T0626	Elaborar planes y matrices de recolección empleando la orientación y los procedimientos establecidos.
T0627	Contribuir a la planificación de acciones en casos de crisis para las ciberoperaciones.
T0628	Contribuir a la elaboración de las herramientas de ayuda para decisiones de la organización, de ser necesario.
T0629	Contribuir, junto con los responsables de la toma de decisiones internos o externos, a la elaboración y coordinación de políticas, normas de desempeño, planes y paquetes de aprobación de las ciberoperaciones, y a la dotación de personal.
T0630	Incorporar los recursos de inteligencia en el diseño general de los planes de ciberoperaciones.
T0631	Coordinar, con los encargados de la disciplina de recolección, la asignación de los recursos de los activos de recolección con respecto a los requisitos de recolección priorizados.
T0632	Coordinar la inclusión del plan de recolección en la documentación correspondiente.
T0633	Coordinar la investigación del objetivo con los socios apropiados.
T0634	Reasignar o redireccionar los activos y los recursos de recolección.
T0635	Coordinarse con los socios en materia de inteligencia y ciberdefensa para obtener información esencial pertinente.
T0636	Coordinarse con los planificadores de inteligencia para comprobar que los administradores de recolección reciban los requisitos de información.
T0637	Coordinarse con el equipo de planificación de inteligencia a fin de evaluar la capacidad para cumplir las tareas de inteligencia asignadas.
T0638	Coordinar, generar y dar seguimiento a los requisitos de inteligencia.
T0639	Coordinar, sincronizar y redactar secciones de inteligencia aplicables de los planes de ciberoperaciones.
T0640	Usar las evaluaciones de inteligencia para afrontar las acciones potenciales del objetivo.
T0641	Crear estrategias de explotación integrales que identifiquen las vulnerabilidades técnicas u operativas que puedan ser explotadas.
T0642	Mantener el conocimiento de las estructuras internas y externas de la organización cibernética, sus fortalezas y su empleo de personal y tecnología.
T0643	Aplicar herramientas a un objetivo y utilizarlas en este (por ejemplo, puertas traseras, analizadores de protocolos).
T0644	Detectar ataques contra redes y hosts seleccionados como objetivos y reaccionar en consecuencia.
T0645	Determinar el plan de acción para considerar los cambios en los objetivos, la orientación y el entorno operativo.
T0646	Determinar las bases de datos, bibliotecas y almacenes existentes de la página web para la gestión de recolección.
T0647	Determinar la manera en que los factores identificados afectan la asignación de tareas, la recolección, el procesamiento, la explotación y la difusión de la forma y la función de la arquitectura.

Id. de la tarea	Descripción de la tarea
T0648	Determinar los indicadores (por ejemplo, las medidas de la efectividad) que mejor se adapten a los objetivos específicos de una ciberoperación.
T0649	Determinar las organizaciones o los niveles que cuenten con autoridad sobre todos los recursos de recolección accesibles.
T0650	Determinar las tecnologías que utiliza un determinado objetivo.
T0651	Establecer un método para comparar los informes de recolección con los requisitos pendientes a fin de identificar las deficiencias de información.
T0652	Preparar materiales de inteligencia de todas las fuentes para la selección de objetivos.
T0653	Aplicar técnicas analíticas para obtener más información sobre los objetivos.
T0654	Formular y mantener planes deliberados o de crisis.
T0655	Elaborar y revisar la orientación específica de ciberoperaciones para integrarla en actividades de planificación más amplias.
T0656	Elaborar y revisar la orientación de inteligencia para integrarla en la ayuda a la planificación y ejecución de las ciberoperaciones.
T0657	Elaborar instrucciones de coordinación por disciplina de recolección para cada fase de una operación.
T0658	Elaborar planes y orientación de ciberoperaciones para comprobar que las decisiones de ejecución y asignación de recursos se ajusten a los objetivos de la organización.
T0659	Establecer ayuda detallada de inteligencia para los requisitos de las ciberoperaciones.
T0660	Formular los requisitos de información necesarios para responder a las solicitudes de información prioritarias.
T0661	Elaborar medidas de efectividad y de rendimiento.
T0662	Asignar los recursos de recolección en función de la orientación, las prioridades o el énfasis operativo de la dirección.
T0663	Hacer evaluaciones de la efectividad de la munición o materiales para evaluaciones operativas.
T0664	Formular técnicas nuevas para lograr y mantener el acceso a los sistemas del objetivo.
T0665	Elaborar o participar en la elaboración de normas para proporcionar, solicitar u obtener el apoyo de los socios externos a fin de sincronizar las ciberoperaciones.
T0666	Formular o conformar las estrategias, políticas y actividades internacionales de trabajo cibernético para cumplir los objetivos de la organización.
T0667	Elaborar posibles planes de acción.
T0668	Formular procedimientos para proporcionar retroalimentación a los administradores de la recolección y de los recursos y a los centros de procesamiento, explotación y difusión.
T0669	Establecer estrategias y procesos para el desarrollo de la planificación, las operaciones y las capacidades de los socios.
T0670	Formular, implementar y recomendar cambios a los procedimientos y las políticas de planificación apropiados.
T0671	Establecer, mantener y evaluar acuerdos de seguridad de cooperación cibernética con socios externos.
T0672	Diseñar, documentar y validar los documentos de estrategia y planificación de ciberoperaciones.
T0673	Difundir informes para comunicar a los responsables de la toma de decisiones los problemas de recolección.
T0674	Difundir mensajes sobre la asignación de tareas y los planes de recolección.
T0675	Llevar a cabo y documentar una evaluación de los resultados de la recolección usando los procedimientos establecidos.
T0676	Redactar los requisitos de recolección y producción de ciberinteligencia.

Id. de la tarea	Descripción de la tarea
T0677	Editar o ejecutar secuencias de comandos simples (por ejemplo, Perl, VBScript) en sistemas Windows y UNIX.
T0678	Dialogar con los clientes para entender sus necesidades y deseos de información de inteligencia.
T0679	Comprobar que las iniciativas de planificación de operaciones se conviertan efectivamente en operaciones en curso.
T0680	Comprobar que las actividades de planificación de inteligencia se integren y sincronicen con el calendario de planificación de operaciones.
T0681	Establecer vías alternativas de procesamiento, explotación y difusión para resolver las cuestiones o los problemas identificados.
T0682	Validar el vínculo entre solicitudes de recolección y requisitos de información crítica, y los requisitos de inteligencia prioritarios de la dirección.
T0683	Establecer una actividad de gestión del procesamiento, la explotación y la difusión usando la orientación o los procedimientos aprobados.
T0684	Calcular los efectos operativos que generan las actividades cibernéticas.
T0685	Evaluar los procesos de toma de decisiones sobre amenazas.
T0686	Identificar las vulnerabilidades de las amenazas.
T0687	Identificar las amenazas a las vulnerabilidades de Blue Force.
T0688	Evaluar las capacidades disponibles con respecto a los efectos deseados para recomendar soluciones eficientes.
T0689	Evaluar hasta qué punto la información recolectada o la información de inteligencia producida satisface las solicitudes de información.
T0690	Evaluar los cálculos de inteligencia para ayudar al ciclo de planificación.
T0691	Evaluar las condiciones que afectan el uso de las capacidades de ciberinteligencia disponibles.
T0692	Generar y evaluar la efectividad de las estrategias de análisis de redes.
T0693	Evaluar hasta qué punto las operaciones de recolección están sincronizadas con los requisitos operativos.
T0694	Evaluar la efectividad de las operaciones de recolección con respecto al plan de recolección.
T0695	Examinar los metadatos y el contenido relacionados con las interceptaciones considerando la importancia de la selección del objetivo.
T0696	Explotar las vulnerabilidades de dispositivos de red, dispositivos de seguridad o terminales o entornos utilizando diversos métodos o herramientas.
T0697	Facilitar el acceso habilitando medios físicos o inalámbricos.
T0698	Facilitar información actualizada continuamente sobre inteligencia, vigilancia y visualización a los administradores de imágenes operativas comunes.
T0699	Facilitar las interacciones entre los responsables de la toma de decisiones de los socios internos y externos para sincronizar e integrar los planes de acción compatibles con los objetivos.
T0700	Facilitar el intercambio de “mejores prácticas” y de “lecciones aprendidas” en toda la comunidad de ciberoperaciones.
T0701	Colaborar con los diseñadores, transmitiendo conocimientos técnicos y acerca de los objetivos en las presentaciones de requisitos de herramientas para mejorar el desarrollo de herramientas.
T0702	Formular estrategias de recolección en función del conocimiento de las capacidades disponibles de la disciplina de inteligencia y los métodos de obtención que alinean las

Id. de la tarea	Descripción de la tarea
	capacidades y los accesos de recolección multidisciplinaria con los objetivos y sus propiedades observables.
T0703	Obtener y analizar datos (por ejemplo, medidas de efectividad) para determinar la eficacia, y presentar informes para actividades posteriores.
T0704	Incorporar los planes de soporte de ciberoperaciones y seguridad de las comunicaciones en los objetivos de la organización.
T0705	Incorporar inteligencia y contrainteligencia para ayudar a la elaboración de planes.
T0706	Obtener información sobre redes por medio de técnicas tradicionales y alternativas (por ejemplo, análisis de redes sociales, encadenamiento de llamadas, análisis de tráfico).
T0707	Generar solicitudes de información.
T0708	Identificar tácticas y metodologías de amenazas.
T0709	Identificar todas las capacidades y limitaciones de inteligencia disponibles de los socios para soporte de las ciberoperaciones.
T0710	Identificar y evaluar las capacidades, requisitos y vulnerabilidades críticas de las amenazas.
T0711	Identificar, redactar, evaluar y priorizar los requisitos de información o de inteligencia pertinentes.
T0712	Identificar y gestionar las prioridades de la cooperación en materia de seguridad con los socios externos.
T0713	Identificar y presentar requisitos de inteligencia para designar los requisitos de información prioritarios.
T0714	Identificar los foros de colaboración que puedan servir como mecanismos para coordinar procesos, funciones y resultados con las organizaciones y los grupos funcionales especificados.
T0715	Identificar deficiencias de recolección y estrategias potenciales de recolección contra objetivos.
T0716	Identificar los requisitos y procedimientos de coordinación con las autoridades de recolección designadas.
T0717	Identificar los elementos de los objetivos críticos.
T0718	Identificar las deficiencias e insuficiencias de inteligencia.
T0719	Identificar las deficiencias e insuficiencias de ciberinteligencia en la planificación ciberoperativa.
T0720	Identificar las deficiencias de conocimientos acerca de la tecnología del objetivo y del desarrollo de métodos innovadores de recolección.
T0721	Identificar asuntos o problemas que puedan interrumpir o degradar la efectividad de la arquitectura de procesamiento, explotación y difusión.
T0722	Identificar los componentes de la red y su funcionalidad para habilitar el análisis y establecimiento de objetivos.
T0723	Identificar las posibles disciplinas de recolección para aplicarlas a los requisitos de información prioritarios.
T0724	Identificar los puntos fuertes y las vulnerabilidades potenciales dentro de una red.
T0725	Identificar y mitigar los riesgos de la capacidad para gestionar la recolección y apoyar el plan, las operaciones y el ciclo del objetivo.
T0726	Identificar la necesidad, el alcance y el plazo para la producción derivada de la preparación del entorno de inteligencia aplicable.
T0727	Identificar, localizar y dar seguimiento a objetivos por medio de técnicas de análisis geoespacial.

Id. de la tarea	Descripción de la tarea
T0728	Aportar información para los planes de acción o elaborar estos planes en función de los factores de amenaza.
T0729	Informar a los socios externos de los efectos potenciales de las políticas y la orientación nuevas o modificadas sobre las actividades de ciberoperaciones en asociación.
T0730	Informar a las partes interesadas (por ejemplo, administradores de la recolección y de los recursos, centros de procesamiento, explotación y difusión) de los resultados de evaluaciones utilizando los procedimientos establecidos.
T0731	Iniciar solicitudes para guiar la asignación de tareas y ayudar con la gestión de recolección.
T0732	Integrar las iniciativas de planificación cibernética y selección de objetivos con otras organizaciones.
T0733	Interpretar las evaluaciones de las preparaciones del entorno para determinar el plan de acción.
T0734	Expedir solicitudes de información.
T0735	Dirigir y coordinar la ayuda de inteligencia con la planificación operativa.
T0736	Dirigir o habilitar las operaciones de explotación compatibles con las metas de la organización y los requisitos de objetivos.
T0737	Vincular los requisitos de recolección prioritarios con activos y recursos óptimos.
T0738	Mantener el conocimiento de los avances en las tecnologías de hardware y software (por ejemplo, asistir a sesiones de capacitación o conferencias, leer) y de sus implicaciones potenciales.
T0739	Mantener relaciones con los socios internos y externos que se dedican a la planificación cibernética o áreas afines.
T0740	Mantener el conocimiento situacional y la funcionalidad de la infraestructura operativa orgánica.
T0741	Mantener el conocimiento situacional de los requisitos de inteligencia y la asignación de tareas correspondientes relacionados con la cibernética.
T0742	Mantener el conocimiento situacional de las capacidades y actividades de los socios.
T0743	Mantener el conocimiento situacional para determinar si los cambios en el entorno operativo requieren la revisión del plan.
T0744	Mantener listas de objetivos (es decir, listas de objetivos restringidos [RTL, por sus siglas en inglés], listas de objetivos conjuntos [JTL, por sus siglas en inglés], listas de objetivos candidatos [CTL, por sus siglas en inglés], etc.).
T0745	Hacer recomendaciones para guiar la recolección y satisfacer los requisitos del cliente.
T0746	Modificar los requisitos de recolección según sea necesario.
T0747	Vigilar y evaluar las ciberoperaciones integradas para identificar las oportunidades de cumplir los objetivos de la organización.
T0748	Vigilar y comunicar los cambios en las disposiciones, actividades, tácticas, capacidades, objetivos, etc., de la amenaza en relación con los conjuntos de problemas de advertencias de las ciberoperaciones designadas.
T0749	Vigilar y comunicar las actividades de amenazas validadas.
T0750	Vigilar que terminen las labores de recolección reasignadas.
T0751	Vigilar los sitios web de código abierto en busca de contenido hostil dirigido contra los intereses de la organización o sus socios.
T0752	Vigilar el entorno operativo e informar de las actividades de adversarios, en cumplimiento de los requisitos de información prioritarios de la dirección.
T0753	Vigilar el estado operativo y la efectividad de la arquitectura de procesamiento, explotación y difusión.

Id. de la tarea	Descripción de la tarea
T0754	Vigilar las redes del objetivo para proporcionar indicaciones y advertencias de cambios en las comunicaciones del objetivo o errores en el procesamiento.
T0755	Vigilar el entorno operativo en busca de factores y riesgos potenciales del proceso de gestión de la operación de recolección.
T0756	Operar y mantener sistemas automatizados para lograr y mantener el acceso a los sistemas del objetivo.
T0757	Optimizar la combinación de activos y recursos de recolección para aumentar la efectividad y la eficiencia con respecto a la información esencial asociada con los requisitos de inteligencia prioritarios.
T0758	Producir inteligencia puntual y combinada de ciberoperaciones o productos de inteligencia de indicaciones y advertencias de todas las fuentes (por ejemplo, evaluaciones de amenazas, sesiones informativas, estudios de inteligencia, estudios de países).
T0759	Contribuir a la revisión y el refinamiento de las políticas, incluidas las evaluaciones de las consecuencias de aprobar o no aprobar esas políticas.
T0760	Aportar experiencia en el tema a los equipos de planificación, grupos de coordinación y grupos de trabajo según sea necesario.
T0761	Aportar experiencia en el tema y apoyo a foros y grupos de trabajo de planificación y desarrollo según corresponda.
T0763	Llevar a cabo iniciativas de planificación estratégica a largo plazo con socios internos y externos en las actividades cibernéticas.
T0764	Aportar experiencia en el tema a las iniciativas de planificación con socios internos y externos de ciberoperaciones.
T0765	Aportar experiencia en el tema a la elaboración de ejercicios.
T0766	Proponer políticas que rijan las interacciones con los grupos de coordinación externos.
T0767	Hacer análisis de contenido o de metadatos para cumplir los objetivos de la organización.
T0768	Llevar a cabo actividades cibernéticas para degradar o eliminar la información que resida en las computadoras y redes informáticas.
T0769	Llevar a cabo actividades de automatización de la selección de objetivos.
T0770	Caracterizar los sitios web.
T0771	Aportar experiencia en el tema a las caracterizaciones de sitios web.
T0772	Prepararse para los ejercicios y aportar a estos experiencia en el tema.
T0773	Priorizar los requisitos de recolección para las plataformas de recolección en función de las capacidades de la plataforma.
T0774	Procesar datos filtrados para analizarlos o difundirlos a los clientes.
T0775	Producir reconstrucciones de red.
T0776	Elaborar productos de análisis de sistemas del objetivo.
T0777	Generar perfiles de los administradores de redes o sistemas y sus actividades.
T0778	Generar perfiles de los objetivos y sus actividades.
T0779	Ofrecer asesoramiento o ayuda a los encargados de la toma de decisiones sobre operaciones e inteligencia con la reasignación de los recursos y los activos de recolección en respuesta a situaciones operativas dinámicas.
T0780	Ofrecer ayuda de asesoramiento y promoción para la planificación de la recolección como un componente integrado de los planes estratégicos de campaña y otros planes adaptativos.
T0781	Hacer recomendaciones sobre el punto de mira y la reactivación.
T0782	Proporcionar análisis y ayuda para la evaluación de la efectividad.
T0783	Proporcionar ayuda de inteligencia reciente a las partes interesadas esenciales, internas y externas según corresponda.

Id. de la tarea	Descripción de la tarea
T0784	Proporcionar orientación sobre cibernética y asesoramiento sobre las aportaciones de información al plan de soporte de inteligencia.
T0785	Proporcionar las evaluaciones y la retroalimentación necesarias para mejorar la producción de inteligencia, los informes de inteligencia, los requisitos de recolección y las operaciones.
T0786	Proporcionar información y evaluaciones a fin de informar a la dirección y los clientes; desarrollar y refinar los objetivos; ayudar a la planificación y ejecución de operaciones; y evaluar los efectos de las operaciones.
T0787	Aportar información para el desarrollo y refinamiento de los objetivos, prioridades, estrategias, planes y programas de las ciberoperaciones.
T0788	Aportar información y ayudar en las evaluaciones de efectividad posteriores a una acción.
T0789	Aportar información y ayudar en la elaboración de planes y orientación.
T0790	Aportar información para las evaluaciones de efectividad de la selección de objetivos para que sean aceptados por la dirección.
T0791	Aportar información para los elementos administrativos y logísticos de un plan de soporte operativo.
T0792	Proporcionar análisis y ayuda de inteligencia a los ejercicios designados, las actividades de planificación y las operaciones urgentes.
T0793	Proporcionar soporte de efectividad a los ejercicios designados o a las operaciones urgentes.
T0794	Hacer recomendaciones sobre operaciones y reactivación.
T0795	Proporcionar ayuda de planificación entre socios internos y externos.
T0796	Proporcionar información procesable de geolocalización en tiempo real.
T0797	Hacer recomendaciones sobre objetivos que cumplan los objetivos de la dirección.
T0798	Proporcionar productos y ayuda para la selección de objetivos según se haya designado.
T0799	Proporcionar ayuda urgente para la selección de objetivos.
T0800	Dar aviso oportuno de intenciones o actividades inminentes u hostiles que podrían afectar los objetivos, recursos o capacidades de la organización.
T0801	Recomendar refinamiento, adaptación, conclusión y ejecución de los planes operativos según corresponda.
T0802	Revisar las fuentes de información apropiadas para determinar la validez y la pertinencia de la información obtenida.
T0803	Reconstruir redes en formato de diagrama o de informe.
T0804	Registrar la recolección de información o de las actividades de preparación del entorno contra los objetivos durante las operaciones diseñadas para lograr efectos cibernéticos.
T0805	Informar de las intrusiones y los eventos de la red importantes derivados de información de inteligencia.
T0806	Solicitar el procesamiento y la explotación de una disciplina, y difundir la información recolectada usando los activos y recursos de recolección de esa disciplina de acuerdo con la orientación o los procedimientos aprobados.
T0807	Investigar las tendencias de las comunicaciones en las tecnologías emergentes (en las redes informáticas y de telefonía, por satélite, por cable e inalámbricas) tanto en fuentes de código abierto como clasificadas.
T0808	Revisar y entender la orientación y los objetivos de la dirección de la organización para tenerlos en cuenta durante la planificación.
T0809	Revisar las capacidades de los recursos de recolección asignados.
T0810	Revisar la orientación de la recolección de inteligencia para determinar su precisión y aplicabilidad.

Id. de la tarea	Descripción de la tarea
T0811	Revisar la lista de requisitos de recolección priorizados y la información esencial.
T0812	Revisar y actualizar el plan de recolección completo, según sea necesario.
T0813	Revisar, aprobar, priorizar y presentar los requisitos operativos para la investigación, desarrollo o adquisición de las capacidades cibernéticas.
T0814	Revisar la matriz de recolección en función de la disponibilidad de los activos y los recursos óptimos.
T0815	Corregir y minimizar la información para proteger las fuentes y los métodos.
T0816	Investigar la iniciativa de planificación de ciberinteligencia.
T0817	Servir como conducto de información de los equipos de socios mediante la identificación de los expertos en el tema que puedan ayudar con la investigación de situaciones complejas o inusuales.
T0818	Servir de enlace con los socios externos.
T0819	Solicitar y gestionar la retroalimentación de los solicitantes sobre la calidad, puntualidad y efectividad de la recolección con respecto a los requisitos de esta.
T0820	Especificar los cambios al plan de recolección o al entorno operativo que requieran la reasignación de tareas o la redirección de los activos y los recursos de recolección.
T0821	Especificar las recolecciones o las asignaciones de tareas propias de una disciplina que se deben hacer a corto plazo.
T0822	Presentar solicitudes de información a la sección de gestión de requisitos de recolección para procesarlas como solicitudes de recolección.
T0823	Presentar o responder a las solicitudes de eliminación de conflictos de las ciberoperaciones.
T0824	Ayudar a la identificación y documentación de los efectos colaterales.
T0825	Sincronizar las actividades de interacción internacional cibernética y los requisitos de recursos afines según corresponda.
T0826	Sincronizar las secciones cibernéticas de los planes de cooperación para la seguridad.
T0827	Sincronizar el empleo integrado de todos los recursos disponibles de recolección de inteligencia orgánica y de socios usando las capacidades y las técnicas de colaboración a disposición.
T0828	Poner a prueba y evaluar las herramientas creadas localmente para uso operativo.
T0829	Poner a prueba las herramientas y técnicas elaboradas internamente con respecto a las herramientas del objetivo.
T0830	Hacer el seguimiento del estado de las solicitudes de información, incluidas las procesadas como solicitudes de recolección y requisitos de producción, usando los procedimientos establecidos.
T0831	Convertir las solicitudes de recolección en requisitos de recolección específicos de la disciplina aplicable.
T0832	Usar los resultados de la retroalimentación (por ejemplo, las lecciones aprendidas) para identificar oportunidades para mejorar la efectividad y la eficiencia de la gestión de recolección.
T0833	Validar las solicitudes de información de acuerdo con los criterios establecidos.
T0834	Colaborar estrechamente con los planificadores, analistas de inteligencia y administradores de recolección para comprobar que los requisitos de inteligencia y los planes de recolección sean precisos y estén actualizados.
T0835	Colaborar estrechamente con los planificadores, analistas y administradores de recolección para identificar las deficiencias de inteligencia y comprobar que los requisitos de inteligencia sean precisos y estén actualizados.

Id. de la tarea	Descripción de la tarea
T0836	Documentar las lecciones aprendidas que transmitan los resultados de los eventos o los ejercicios.
T0837	Asesorar a los administradores y operadores sobre los problemas lingüísticos y culturales que influyen en los objetivos de la organización.
T0838	Analizar y procesar la información usando experiencia lingüística o cultural.
T0839	Evaluar, documentar y aplicar la motivación o el marco de referencia de un objetivo para facilitar el análisis, la selección de objetivos y las oportunidades de recolección.
T0840	Colaborar en todas de líneas organizativas internas o externas para mejorar la recolección, el análisis y la difusión.
T0841	Llevar a cabo investigaciones de todas las fuentes del objetivo, incluido el uso de materiales de código abierto en el idioma del objetivo.
T0842	Llevar a cabo un análisis de las comunicaciones del objetivo para identificar información esencial compatible con las metas de la organización.
T0843	Hacer una revisión de la calidad y proporcionar retroalimentación sobre los materiales transcritos o traducidos.
T0844	Evaluar e interpretar metadatos en busca de tendencias, anomalías o eventos, optimizando con ello la selección de objetivos, el análisis y el procesamiento.
T0845	Identificar tácticas y metodologías de las amenazas cibernéticas.
T0846	Identificar las comunicaciones del objetivo dentro de la red global.
T0847	Mantener el conocimiento de las herramientas y las técnicas de comunicación del objetivo, y las características de sus redes de comunicación (por ejemplo, capacidad, funcionalidad, rutas, nodos críticos) y sus implicaciones potenciales en la selección de objetivos, recolección y análisis.
T0848	Proporcionar retroalimentación a los administradores de recolección para mejorar la recolección y el análisis futuros.
T0849	Identificar idiomas y dialectos extranjeros en los datos de origen iniciales.
T0850	Hacer o respaldar el análisis técnico y la asignación de redes.
T0851	Proporcionar requisitos y retroalimentación para optimizar la elaboración de herramientas de procesamiento lingüístico.
T0852	Hacer y documentar el análisis de redes sociales según corresponda.
T0853	Escanear, identificar y priorizar materiales lingüísticos gráficos (incluidas las comunicaciones de máquina a máquina) o de voz del objetivo.
T0854	Dar información crítica o urgente a los clientes apropiados.
T0855	Transcribir materiales de voz del objetivo al idioma del objetivo.
T0856	Traducir el material gráfico del objetivo (por ejemplo, de manera textual o resumida, o lo esencial).
T0857	Traducir el material de voz del objetivo (por ejemplo, de manera textual o resumida, o lo esencial).
T0858	Identificar terminología en idiomas extranjeros en los programas informáticos (por ejemplo, comentarios, nombres de variables).
T0859	Dar ayuda de análisis lingüístico en tiempo casi real (por ejemplo, operaciones en vivo).
T0860	Identificar terminología relacionada con la tecnología y la cibernética en el idioma del objetivo.
T0861	Colaborar con el asesor general, la oficina de asuntos externos y las empresas para procurar que tanto los servicios existentes como los nuevos cumplan con las obligaciones de privacidad y seguridad de datos.
T0862	Colaborar con el asesor legal, la administración y los departamentos y comités clave, para facilitar que la organización tenga y mantenga los debidos formularios de consentimiento

Id. de la tarea	Descripción de la tarea
	de privacidad y confidencialidad, formularios de autorización y avisos y materiales de información conforme a las prácticas y los requisitos legales y organizativos vigentes.
T0863	Coordinarse con los órganos normativos apropiados para procurar que los programas, políticas y procedimientos relacionados con los derechos civiles, las libertades civiles y las consideraciones de privacidad se tengan en cuenta de manera integrada y completa.
T0864	Colaborar con los organismos normativos y acreditativos.
T0865	Colaborar con la oficina de asuntos externos para entablar relaciones con las autoridades normativas y demás funcionarios gubernamentales responsables de las cuestiones de privacidad y seguridad de datos.
T0866	Mantener el conocimiento actual de las leyes de privacidad federales y estatales y las normas de acreditación aplicables, y vigilar los avances en las tecnologías de la privacidad de la información para facilitar la adaptación y el cumplimiento organizativos.
T0867	Comprobar que todos los procesamientos o las bases de datos estén registrados ante las autoridades locales de protección de datos y privacidad donde sea necesario.
T0868	Colaborar con los equipos empresariales y la alta dirección para facilitar el conocimiento de las “mejores prácticas” en cuestiones de privacidad y seguridad de datos.
T0869	Colaborar con la alta dirección de la organización para establecer un comité de supervisión de la privacidad en toda la organización.
T0870	Asumir la función de liderazgo en las actividades del comité de supervisión de la privacidad.
T0871	Colaborar en las políticas y los procedimientos de seguridad y privacidad en materia cibernética.
T0872	Colaborar con el personal de ciberseguridad en el proceso de evaluación de riesgos a la seguridad para lograr el cumplimiento de la privacidad y la mitigación de riesgos.
T0873	Interactuar con la alta dirección a fin de elaborar planes estratégicos para la recolección, el uso y el intercambio de la información de manera que se maximice su valor y se cumpla con los reglamentos de privacidad aplicables.
T0874	Impartir orientación estratégica a los funcionarios corporativos acerca de los recursos y la tecnología de la información.
T0875	Ayudar al funcionario de seguridad con el establecimiento y la implementación de una infraestructura de información.
T0876	Coordinar con el funcionario de cumplimiento corporativo los procedimientos para que cada persona documente y dé parte de todo indicio de infracciones de la privacidad.
T0877	Colaborar con las unidades de la organización correspondientes para supervisar los derechos del consumidor de acceso a la información.
T0878	Servir como el enlace de privacidad de la información para los usuarios de sistemas tecnológicos.
T0879	Servir como enlace del departamento de sistemas de información.
T0880	Elaborar materiales de capacitación sobre privacidad y otras comunicaciones para aumentar el conocimiento de los empleados sobre las políticas de privacidad de la empresa, las prácticas y los procedimientos del manejo de datos y las obligaciones legales.
T0881	Supervisar, dirigir, impartir o comprobar la impartición de capacitación y orientación iniciales en materia de privacidad a todos los empleados, voluntarios, contratistas, alianzas, socios comerciales y otros terceros apropiados.
T0882	Llevar a cabo actividades de concientización y capacitación continuas sobre privacidad.
T0883	Colaborar con la oficina de asuntos externos para entablar relaciones con las organizaciones de consumidores y demás ONG que tengan un interés en las cuestiones de

Id. de la tarea	Descripción de la tarea
	privacidad y seguridad de datos, y para gestionar la participación de la empresa en eventos públicos relacionados con la privacidad y la seguridad de datos.
T0884	Colaborar con la administración de la organización, el asesor jurídico y otras partes afines para representar los intereses de la organización en materia de privacidad de la información con partes externas, incluidos los organismos gubernamentales, que asumen la adopción o enmienda de la legislación, reglamentación o normativa sobre privacidad.
T0885	Comunicar periódicamente el estado del programa de privacidad a la junta, director ejecutivo u otra persona o comité responsable.
T0886	Colaborar con la oficina de asuntos externos para responder las preguntas de la prensa y otras consultas sobre inquietudes relativas a los datos de consumidores y empleados.
T0887	Proporcionar liderazgo al programa de privacidad de la organización.
T0888	Dirigir y supervisar a los especialistas en privacidad y coordinar los programas de privacidad y seguridad de datos con los ejecutivos sénior a nivel mundial para garantizar la uniformidad en toda la organización.
T0889	Lograr el cumplimiento de las prácticas de privacidad y la aplicación uniforme de sanciones por incumplimiento con las políticas de privacidad de todos los empleados del personal de la organización, personal adicional y todos los socios comerciales, en cooperación con los RR. HH., el funcionario de seguridad de sistemas de información, la administración y el asesor jurídico, según corresponda.
T0890	Formular sanciones apropiadas por incumplimiento con las políticas y los procedimientos corporativos en materia de privacidad.
T0891	Resolver alegaciones de incumplimiento con las políticas corporativas en materia de privacidad o de avisos de prácticas de información.
T0892	Establecer y coordinar un marco de gestión de riesgos y cumplimiento en materia de privacidad.
T0893	Hacer una revisión completa de los proyectos de privacidad y datos de la empresa, y comprobar que concuerden con las metas y las políticas corporativas en materia de privacidad y seguridad de datos.
T0894	Formular y gestionar procedimientos en toda la empresa para comprobar que el diseño de productos y servicios nuevos concuerde con las políticas de privacidad de la empresa y sus obligaciones legales.
T0895	Establecer un proceso para recibir, documentar, dar seguimiento, investigar y atender toda queja relacionada con las políticas y los procedimientos de privacidad de la organización.
T0896	Establecer junto con los sectores de gestión y operaciones un mecanismo de seguimiento del acceso a la información protegida sobre salud, dentro de la esfera de la organización y según lo requiera la ley, para permitir que las personas cualificadas revisen o reciban un informe sobre dicha actividad.
T0897	Proporcionar liderazgo a la planificación, diseño y evaluación de proyectos relacionados con la privacidad y la seguridad.
T0898	Establecer un programa interno de auditoría de la privacidad.
T0899	Revisar periódicamente el programa de privacidad tomando en cuenta los cambios en las leyes, reglamentos o políticas de la compañía.
T0900	Impartir orientación de elaboración y ayudar con la identificación, implementación y mantenimiento de las políticas y los procedimientos organizativos para la privacidad de la información en coordinación con la dirección y la administración de la organización, y el asesor jurídico.

Id. de la tarea	Descripción de la tarea
T0901	Comprobar que el uso de tecnologías mantenga y no reduzca las protecciones de privacidad en el uso, la recolección y la divulgación de información personal.
T0902	Vigilar el establecimiento de sistemas y las operaciones para el cumplimiento de la seguridad y la privacidad.
T0903	Llevar a cabo evaluaciones del impacto en la privacidad de las normas propuestas sobre la privacidad de la información personal, incluidos el tipo de información personal recolectada y el número de personas afectadas.
T0904	Llevar a cabo evaluaciones periódicas del impacto en la privacidad de la información y actividades continuas de vigilancia del cumplimiento en coordinación con otras funciones de cumplimiento y evaluación operativa de la organización.
T0905	Revisar todos los planes de seguridad de la información relacionados con el sistema para comprobar la correspondencia entre las prácticas de seguridad y privacidad.
T0906	Colaborar con todo el personal de la organización que participa en cualquier aspecto de la divulgación de información protegida para comprobar la coordinación con las políticas, procedimientos y requisitos legales de la organización.
T0907	Considerar y administrar las solicitudes individuales de publicación o divulgación de información personal o protegida.
T0908	Formular y gestionar procedimientos para la investigación y auditoría de proveedores a fin de comprobar el cumplimiento con las políticas de privacidad y seguridad de datos y los requisitos legales.
T0909	Participar en la implementación y la vigilancia continua del cumplimiento de todo acuerdo con colaboradores y socios comerciales para procurar que se tengan en cuenta todas las inquietudes, requisitos y responsabilidades en materia de privacidad.
T0910	Servir como asesor y colaborar en lo relacionado con los contratos de los socios comerciales.
T0911	Mitigar los efectos del uso o la divulgación de información personal que hagan los empleados o socios comerciales.
T0912	Establecer y aplicar procedimientos de medidas correctivas.
T0913	Administrar medidas ante toda queja relativa a las políticas y los procedimientos de privacidad de la organización en coordinación y colaboración con otras funciones similares y, de ser necesario, con el asesor jurídico.
T0914	Ayudar al programa de cumplimiento de privacidad de la organización, colaborando estrechamente con el funcionario de privacidad, el director de seguridad de sistemas de información y demás líderes empresariales para lograr el cumplimiento con las leyes y los reglamentos federales y estatales sobre privacidad.
T0915	Identificar y corregir posibles incumplimientos de la empresa o áreas de riesgo para garantizar que se cumpla plenamente con los reglamentos de privacidad.
T0916	Gestionar los incidentes y las vulneraciones de privacidad junto con el funcionario de privacidad, el director de seguridad de sistemas de información, el asesor jurídico y las unidades de negocios.
T0917	Coordinarse con el director de seguridad de sistemas de información para lograr la correspondencia entre las prácticas de seguridad y privacidad.
T0918	Establecer, implementar y mantener las políticas y los procedimientos en toda la organización para cumplir con los reglamentos de privacidad.
T0919	Comprobar que la empresa mantenga avisos, formularios de consentimiento y autorización y materiales apropiados sobre la privacidad y la confidencialidad.
T0920	Establecer y mantener comunicaciones y capacitación apropiadas para promover y educar a todo el personal y a los miembros de la junta en lo que se refiere a los problemas y

Id. de la tarea	Descripción de la tarea
	requisitos del cumplimiento de la privacidad, y las consecuencias que acarrea el incumplimiento.
T0921	Determinar los requisitos de los socios comerciales relacionados con el programa de privacidad de la organización.
T0922	Establecer y administrar un proceso para recibir, documentar, dar seguimiento e investigar las quejas relacionadas con las políticas y los procedimientos de privacidad de la empresa, y tomar medidas correctivas según corresponda.
T0923	Cooperar con los organismos normativos pertinentes y otras entidades jurídicas, así como con los funcionarios de la organización, en toda revisión o investigación del cumplimiento.
T0924	Llevar a cabo actividades continuas de vigilancia del cumplimiento de la privacidad.
T0925	Vigilar los avances en las tecnologías de la privacidad de la información para comprobar que la organización las adopte y logre el cumplimiento.
T0926	Elaborar o ayudar a elaborar materiales de capacitación sobre privacidad y otras comunicaciones para aumentar el conocimiento de los empleados sobre las políticas de privacidad de la empresa, las prácticas y procedimientos del manejo de datos y las obligaciones legales.
T0927	Nombrar y orientar a un equipo de expertos en seguridad de la TI.
T0928	Colaborar con las partes interesadas clave para establecer un programa de gestión de riesgos a la ciberseguridad.
T0929	Identificar y asignar personal a las funciones específicas asociadas con la ejecución del Marco de gestión de riesgos.
T0930	Establecer una estrategia de gestión de riesgos para la organización que incluya la determinación de la tolerancia al riesgo.
T0931	Identificar las misiones, funciones de negocios y procesos de la misión y de negocios que incluirá el sistema.
T0932	Identificar a las partes interesadas que tengan un interés relacionado con la seguridad en el desarrollo, implementación, operación o mantenimiento de un sistema.
T0933	Identificar a las partes interesadas que tengan un interés relacionado con la seguridad en el desarrollo, implementación, operación o mantenimiento de un sistema.
T0934	Identificar los activos de las partes interesadas que requieran protección.
T0935	Llevar a cabo una evaluación inicial del riesgo de los activos de las partes interesadas y actualizar la evaluación del riesgo de forma continua.
T0936	Definir las necesidades de protección de las partes interesadas y sus requisitos de seguridad.
T0937	Determinar la colocación de un sistema dentro de la arquitectura de la empresa.
T0938	Identificar los controles comunes de toda la organización que estén disponibles para ser heredados por los sistemas organizativos.
T0939	Llevar a cabo una categorización de segundo nivel de la seguridad de los sistemas organizativos que tengan el mismo nivel de impacto.
T0940	Determinar el límite de un sistema.
T0941	Identificar los requisitos de seguridad asignados a un sistema y a la organización.
T0942	Identificar los tipos de información que debe procesar, almacenar o transmitir un sistema.
T0943	Categorizar el sistema y documentar los resultados de la categorización de la seguridad como parte de los requisitos del sistema.
T0944	Describir las características de un sistema.
T0945	Registrar el sistema en las oficinas correspondientes de gestión o del programa organizativo.

Id. de la tarea	Descripción de la tarea
T0946	Seleccionar los controles de seguridad de un sistema y documentar la descripción funcional de las implementaciones de control planificadas en un plan de seguridad.
T0947	Elaborar una estrategia para vigilar la efectividad del control de la seguridad; coordinar con la organización la estrategia a nivel de sistemas y la estrategia de vigilancia a nivel de procesos de la misión o de negocios.
T0948	Revisar y aprobar los planes de seguridad.
T0949	Implementar los controles de seguridad especificados en un plan de seguridad o en otra documentación del sistema.
T0950	Documentar los cambios en la implementación planificada del control de seguridad y establecer la configuración de referencia para un sistema.
T0951	Formular, revisar y aprobar un plan para evaluar los controles de seguridad en un sistema y en la organización.
T0952	Evaluar los controles de seguridad de conformidad con los procedimientos de evaluación definidos en un plan de evaluación de la seguridad.
T0953	Preparar un informe de la evaluación de la seguridad que documente los problemas, resultados y recomendaciones de la evaluación del control de seguridad.
T0954	Aplicar medidas iniciales de corrección a los controles de seguridad, en función de los resultados y las recomendaciones de un informe de evaluación de la seguridad; volver a evaluar los controles corregidos.
T0955	Preparar un plan de acción y establecer hitos en función de los resultados y las recomendaciones de un informe de evaluación de la seguridad, que excluya las medidas correctivas adoptadas.
T0956	Reunir un paquete de autorizaciones y presentarlo al funcionario que autoriza para que lo adjudique.
T0957	Determinar el riesgo de la operación o el uso de un sistema, o del suministro o el uso de controles comunes.
T0958	Identificar e implementar un plan de acción preferido en respuesta al riesgo determinado.
T0959	Determinar si el riesgo derivado de la operación o el uso del sistema, o del suministro o el uso de controles comunes, es aceptable.
T0960	Vigilar los cambios en un sistema y su entorno de funcionamiento.
T0961	Evaluar los controles de seguridad empleados en el sistema, y heredados por este, de acuerdo con una estrategia de vigilancia definida por la organización.
T0962	Responder a los riesgos en función de los resultados de actividades de vigilancia continua, la evaluación del riesgo y los elementos pendientes de un plan de acción y los hitos.
T0963	Actualizar un plan de seguridad, un informe de evaluación de la seguridad y un plan de acción y los hitos en función de los resultados de un proceso de vigilancia continua.
T0964	Informar al funcionario que autoriza del estado de seguridad de un sistema (incluida la efectividad de los controles de seguridad) de forma continua y de acuerdo con la estrategia de vigilancia.
T0965	Revisar el estado de la seguridad de un sistema (incluida la efectividad de los controles de seguridad) de forma continua para determinar si el riesgo sigue siendo aceptable.
T0966	Implementar una estrategia de eliminación del sistema que ejecute las acciones necesarias cuando se elimine un sistema del servicio.
T0967	Patrocinar y promover la vigilancia continua dentro de la organización.
T0968	Asignar personal, según sea necesario, a los grupos de trabajo de vigilancia continua correspondientes.
T0969	Identificar los requisitos de la preparación de informes compatibles con las actividades de vigilancia continua.

Id. de la tarea	Descripción de la tarea
T0970	Establecer métricas de puntuación y calificación para medir la efectividad del programa de vigilancia continua.
T0971	Determinar la manera en que se integra un programa de vigilancia continua en las estructuras y las políticas más amplias de gobernanza en materia de seguridad de la información de la organización.
T0972	Usar las métricas de puntuación y calificación de la vigilancia continua a fin de tomar decisiones sobre la inversión en la seguridad de la información para resolver problemas persistentes.
T0973	Comprobar que el personal de vigilancia continua disponga de la capacitación y los recursos necesarios (por ejemplo, personal y presupuesto) para desempeñar las obligaciones asignadas.
T0974	Colaborar con los analistas de riesgos de la organización para que se incluyan los niveles apropiados de la organización en la preparación de los informes de vigilancia continua.
T0975	Colaborar con los analistas de riesgos de la organización para garantizar que las métricas del riesgo se definan de forma realista y compatible con la vigilancia continua.
T0976	Colaborar con los funcionarios de la organización para facilitar que los datos de las herramientas de la vigilancia continua proporcionen un conocimiento situacional de los niveles de riesgo.
T0977	Establecer los desencadenadores de los umbrales de riesgo inaceptables para los datos de vigilancia continua.
T0978	Colaborar con los funcionarios de la organización para establecer categorías de informes a nivel de sistema que puedan ser usadas por el programa de vigilancia continua de la organización.
T0980	Designar a una persona cualificada como responsable de la gestión y la implementación del programa de vigilancia continua.
T0981	Identificar a las partes interesadas en la vigilancia continua y establecer un proceso para mantenerlas informadas del programa.
T0982	Identificar los requisitos de preparación de informes de la organización orientados a la seguridad que satisfaga el programa de vigilancia continua.
T0983	Usar los datos de la vigilancia continua a fin de tomar decisiones sobre la inversión en la seguridad de la información para resolver problemas persistentes.
T0984	Definir los desencadenadores dentro del programa de vigilancia continua que puedan usarse para definir el riesgo inaceptable y que den lugar a la adopción de medidas para resolverlo.
T0985	Establecer métricas de puntuación y calificación para medir la efectividad del programa de vigilancia continua.
T0986	Colaborar con los administradores de seguridad a fin de establecer los requisitos apropiados para la preparación de informes de la vigilancia continua a nivel de sistema.
T0987	Usar las herramientas y tecnologías de vigilancia continua para la evaluación en curso del riesgo.
T0988	Establecer los requisitos apropiados para la preparación de informes que cumplan los criterios identificados en el programa de vigilancia continua para su uso en la evaluación automatizada del control.
T0989	Emplear métodos de evaluación no automatizados cuando los datos de las herramientas y tecnologías para la vigilancia continua no cuenten aún con la suficiencia o la calidad adecuadas.

Id. de la tarea	Descripción de la tarea
T0990	Formular procesos con el grupo de auditoría externa acerca de la manera de intercambiar información del programa de vigilancia continua y su efecto en la evaluación del control de la seguridad.
T0991	Identificar los requisitos de la preparación de informes para su uso en la evaluación automatizada del control compatible con la vigilancia continua.
T0992	Determinar la manera en que se utilizarán los resultados de la vigilancia continua en la autorización en curso.
T0993	Establecer procesos y procedimientos para el control del acceso a las herramientas y tecnologías de vigilancia continua.
T0994	Comprobar que el control del acceso a las herramientas y tecnologías de vigilancia continua se gestione adecuadamente.
T0995	Establecer un proceso para proporcionar ayuda técnica a los mitigadores de la vigilancia continua.
T0996	Coordinar los requisitos de la preparación de informes de vigilancia continua entre los diversos usuarios.
T0997	Establecer las responsabilidades de ayuda para la implementación de cada herramienta o tecnología de vigilancia continua.
T0998	Establecer un enlace con el grupo de trabajo de calificación y métricas de ayuda para la vigilancia continua.
T0999	Establecer y poner en marcha un proceso para gestionar la introducción de nuevos riesgos y ayudar a la vigilancia continua.
T1000	Establecer un subgrupo encargado de la coordinación y los problemas de configuración de la vigilancia continua.
T1001	Establecer requisitos de gestión y medición del rendimiento de las herramientas y las tecnologías de la vigilancia continua.
T1002	Usar las puntuaciones y calificaciones para motivar y evaluar el desempeño, y tener en cuenta las inquietudes de ayuda de la vigilancia continua.
T1003	Colaborar con los administradores de seguridad (es decir, propietarios de sistemas, administradores de seguridad de sistemas de información, funcionarios de seguridad de sistemas de información, etc.) a fin de establecer los requisitos adecuados para la preparación de informes de vigilancia continua a nivel del sistema.
T1004	Emplear herramientas de vigilancia continua para evaluar el riesgo en todo momento.
T1005	Usar los datos de la vigilancia continua a fin de tomar decisiones sobre la inversión en la seguridad de la información para resolver problemas persistentes.
T1006	Responder a los problemas señalados durante la vigilancia continua, remitirlos a una instancia superior y coordinar una respuesta.
T1007	Revisar los resultados del programa de vigilancia continua y mitigar los riesgos de manera oportuna.

A.5 Descripciones de los conocimientos del Marco de la NICE

La Tabla 5 proporciona una lista de los diversos tipos de información que se aplican directamente al desempeño de una función. En la Lista detallada de funciones laborales del Apéndice B, se incluyen las identificaciones y descripciones de los conocimientos seleccionados de esta lista para cada función laboral. Las seis primeras son comunes a todas las funciones laborales de ciberseguridad. Esta lista se actualizará periódicamente [1]. Véase la fuente definitiva de la versión más reciente de este material en la Hoja de cálculo de referencia para la Publicación especial 800-181 del NIST [4].

Tabla 5: Descripciones de los conocimientos del Marco de la NICE

Id. de los CHC	Descripción
K0001	Conocimiento de conceptos y protocolos de redes informáticas, y de metodologías de seguridad de redes
K0002	Conocimiento de procesos de gestión de riesgos (por ejemplo, métodos para evaluar y mitigar riesgos)
K0003	Conocimiento de leyes, reglamentos, políticas y ética en relación con la ciberseguridad y la privacidad
K0004	Conocimiento de principios de ciberseguridad y privacidad
K0005	Conocimiento de amenazas y vulnerabilidades cibernéticas
K0006	Conocimiento de impactos operativos específicos de fallas de la ciberseguridad
K0007	Conocimiento de métodos de autenticación, autorización y control del acceso
K0008	Conocimiento de operaciones y procesos de negocios aplicables de las organizaciones de clientes
K0009	Conocimiento de vulnerabilidades de aplicaciones
K0010	Conocimiento de métodos, principios y conceptos de comunicación compatibles con la infraestructura de la red
K0011	Conocimiento de capacidades y aplicaciones de equipos de redes, incluidos enrutadores, conmutadores, puentes, servidores, medios de transmisión y el hardware correspondiente
K0012	Conocimiento de análisis de capacidades y requisitos
K0013	Conocimiento de herramientas, y sus capacidades, para la evaluación de la ciberdefensa y vulnerabilidades
K0014	Conocimiento de estructuras complejas de datos
K0015	Conocimiento de algoritmos informáticos
K0016	Conocimiento de principios de programación informática
K0017	Conocimiento de conceptos y prácticas del procesamiento de datos forenses digitales
K0018	Conocimiento de algoritmos de cifrado
K0019	Conocimiento de conceptos de criptografía y de gestión de claves criptográficas
K0020	Conocimiento de políticas sobre administración y normalización de datos
K0021	Conocimiento de copias de seguridad y recuperación de datos
K0022	Conocimiento de los principios de extracción y almacenamiento de datos
K0023	Conocimiento de sistemas, lenguajes de consulta, relaciones de tablas y vistas de la gestión de bases de datos
K0024	Conocimiento de sistemas de bases de datos
K0025	Conocimiento de gestión de derechos digitales
K0026	Conocimiento de planes de continuidad de operaciones, de continuidad de negocios y de recuperación ante desastres

Id. de los CHC	Descripción
K0027	Conocimiento de arquitectura de seguridad de la información empresarial de la organización
K0028	Conocimiento de requisitos de evaluación y validación de la organización
K0029	Conocimiento de conexiones de la red de área extensa y la red de área local de la organización
K0030	Conocimiento de ingeniería eléctrica que se aplica a la arquitectura informática (por ejemplo, tarjetas de circuitos, procesadores, chips y hardware informático)
K0031	Conocimiento de sistemas de mensajería empresarial y el software correspondiente
K0032	Conocimiento de resiliencia y redundancia
K0033	Conocimiento de mecanismos de control del acceso a la red o los host (por ejemplo, lista de control de acceso, listas de capacidades)
K0034	Conocimiento de interacciones entre los servicios y protocolos de redes que proporcionan comunicaciones de red
K0035	Conocimiento de instalación, integración y optimización de los componentes del sistema
K0036	Conocimiento de los principios de la interacción persona-computadora
K0037	Conocimiento del proceso de evaluación y autorización de la seguridad
K0038	Conocimiento de los principios de ciberseguridad y privacidad que se emplean en la gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos
K0039	Conocimiento de los principios y métodos de ciberseguridad y privacidad que se aplican al desarrollo de software
K0040	Conocimiento de fuentes de difusión de información sobre vulnerabilidades (por ejemplo, alertas, avisos, erratas y boletines)
K0041	Conocimiento de categorías de incidentes, respuestas a incidentes y plazos para respuestas
K0042	Conocimiento de metodologías de respuesta y manejo de incidentes
K0043	Conocimiento de los principios y métodos de análisis comunes y aceptados por la organización
K0044	Conocimiento de los principios de ciberseguridad y privacidad y requisitos organizativos (pertinentes a la confidencialidad, integridad, disponibilidad y autenticación, y sin rechazo de estas)
K0045	Conocimiento de los principios de ingeniería de los sistemas de seguridad de la información (Publicación especial 800-160 del NIST)
K0046	Conocimiento de metodologías y técnicas de detección de intrusiones para detectar intrusiones basadas en el host y la red
K0047	Conocimiento de conceptos y marcos arquitectónicos de tecnología de la información (TI)
K0048	Conocimiento de los requisitos del Marco de gestión de riesgos (RMF)
K0049	Conocimiento de los principios y métodos de seguridad de la tecnología de la información (TI) (por ejemplo, firewalls, zonas desmilitarizadas, cifrado)
K0050	Conocimiento de los principios y conceptos de redes de área local y área extensa, incluida la gestión del ancho de banda
K0051	Conocimiento de lenguajes informáticos de bajo nivel (por ejemplo, lenguajes ensambladores)
K0052	Conocimiento de matemáticas (por ejemplo, logaritmos, trigonometría, álgebra lineal, cálculo, estadística y análisis de operaciones)
K0053	Conocimiento de medidas o indicadores del rendimiento y la disponibilidad del sistema

Id. de los CHC	Descripción
K0054	Conocimiento de los métodos actuales del sector para evaluar, implementar y difundir herramientas y procedimientos de evaluación, vigilancia, detección y corrección de la seguridad de la tecnología de la información (TI) utilizando conceptos y capacidades que se basan en normas
K0055	Conocimiento de microprocesadores
K0056	Conocimiento de acceso a redes, identidad y gestión del acceso (por ejemplo, infraestructura de clave pública, protocolos Oauth y OpenID, lenguajes de marcado SAML y SPML)
K0057	Conocimiento de dispositivos de hardware y funciones de red
K0058	Conocimiento de métodos de análisis del tráfico de red
K0059	Conocimiento de tecnologías de la información (TI) y de tecnologías de ciberseguridad nuevas y emergentes
K0060	Conocimiento de sistemas operativos
K0061	Conocimiento de la manera en que fluye el tráfico a través de la red (por ejemplo, protocolo de control de transmisión [TCP, por sus siglas en inglés] y protocolo de internet [IP, por sus siglas en inglés], modelo de interconexión de sistemas abiertos [OSI, por sus siglas en inglés], biblioteca de infraestructura de tecnología de la información [ITIL, por sus siglas en inglés], versión vigente)
K0062	Conocimiento de análisis a nivel de paquete
K0063	Conocimiento de conceptos de informática en paralelo y distribuida
K0064	Conocimiento de herramientas y técnicas de ajuste del rendimiento
K0065	Conocimiento de controles de acceso basados en políticas y adaptados al riesgo
K0066	Conocimiento de evaluaciones del impacto de la privacidad
K0067	Conocimiento de conceptos de la ingeniería de procesos
K0068	Conocimiento de estructuras y lógica del lenguaje de programación
K0069	Conocimiento de lenguajes de consulta como SQL (lenguaje de consulta estructurado)
K0070	Conocimiento de amenazas y vulnerabilidades de la seguridad de sistemas y aplicaciones (por ejemplo, desbordamiento de búfer, código móvil, secuencias de comandos entre sitios, lenguaje de procedimiento/lenguaje de consulta estructurado [PL/SQL, por sus siglas en inglés] e inyecciones, condiciones de carrera, canal caché, reproducción, ataques orientados a la devolución de valores, código malintencionado)
K0071	Conocimiento de conceptos de la tecnología de acceso remoto
K0072	Conocimiento de principios y técnicas de la gestión de recursos
K0073	Conocimiento de técnicas seguras de gestión de configuraciones (por ejemplo, guías de implementación técnica de seguridad [STIG, por sus siglas en inglés], mejores prácticas de ciberseguridad en cisecurity.org)
K0074	Conocimiento de conceptos clave en la gestión de seguridad (por ejemplo, gestión de entregas, gestión de parches)
K0075	Conocimiento de herramientas, métodos y técnicas de diseño de sistemas de seguridad
K0076	Conocimiento de teorías, conceptos y métodos de administración de servidores e ingeniería de sistemas
K0077	Conocimiento de sistemas operativos de servidor y cliente
K0078	Conocimiento de herramientas de diagnóstico de servidores y de técnicas de identificación de errores
K0079	Conocimiento de los principios de depuración de software
K0080	Conocimiento de herramientas, métodos y técnicas del diseño de software
K0081	Conocimiento de modelos de desarrollo de software (por ejemplo, modelo de cascada, modelo de espiral)

Id. de los CHC	Descripción
K0082	Conocimiento de ingeniería de software
K0083	Conocimiento de fuentes, características y usos de los recursos de datos de la organización
K0084	Conocimiento de principios y métodos del análisis estructurado
K0086	Conocimiento de herramientas, métodos y técnicas del diseño de sistemas, incluidas las herramientas automatizadas de análisis y diseño de sistemas
K0087	Conocimiento de software de sistemas, y de normas, políticas y métodos autorizados del diseño organizativo (por ejemplo, directrices de la Organización Internacional de Normalización [ISO]) relacionado con el diseño de sistemas
K0088	Conocimiento de conceptos de administración de sistemas
K0089	Conocimiento de herramientas de diagnóstico de sistemas y de técnicas de identificación de errores
K0090	Conocimiento de los principios de gestión del ciclo de vida de sistemas, incluidas la seguridad y utilidad del software
K0091	Conocimiento de métodos de prueba y evaluación de sistemas
K0092	Conocimiento de procesos de integración de la tecnología
K0093	Conocimiento de conceptos de telecomunicaciones (por ejemplo, canal de comunicaciones, presupuesto de vínculos de sistemas, eficiencia espectral, multiplexación)
K0094	Conocimiento de las capacidades y la funcionalidad asociadas con las tecnologías de creación de contenido (por ejemplo, wiki, redes sociales, sistemas de gestión de contenido, blogs)
K0095	Conocimiento de las capacidades y la funcionalidad asociadas con las diversas tecnologías para organizar y gestionar la información (por ejemplo, bases de datos, motores de marcadores)
K0096	Conocimiento de las capacidades y la funcionalidad de diversas tecnologías de colaboración (por ejemplo, groupware, SharePoint)
K0097	Conocimiento de las características de los medios de almacenamiento de datos físicos y virtuales
K0098	Conocimiento de la estructura y los procesos para la preparación de informes del proveedor de servicios de ciberdefensa dentro de la propia organización
K0100	Conocimiento de la arquitectura de la tecnología de la información (TI) empresarial
K0101	Conocimiento de las metas y objetivos de la organización en materia de tecnología de la información (TI) empresarial
K0102	Conocimiento del proceso de ingeniería de sistemas
K0103	Conocimiento del tipo y la frecuencia del mantenimiento de rutina del hardware
K0104	Conocimiento de seguridad de la red privada virtual (VPN)
K0105	Conocimiento de servicios web (por ejemplo, arquitectura orientada a servicios, protocolo simple de acceso a objetos y lenguaje de descripción de servicios web)
K0106	Conocimiento de lo que constituye un ataque a la red y la relación de un ataque a la red con las amenazas y las vulnerabilidades
K0107	Conocimiento de investigaciones, preparación de informes, herramientas de investigación y leyes o reglamentos sobre las amenazas internas
K0108	Conocimiento de conceptos, terminología y operaciones de una amplia gama de medios de comunicación (redes informáticas y de telefonía, satélite, fibra, inalámbricos)
K0109	Conocimiento de arquitecturas y componentes informáticos físicos, incluidas las funciones de diversos componentes y periféricos (por ejemplo, unidades centrales de procesamiento [CPU, por sus siglas en inglés], tarjetas de interfaz de red, almacenamiento de datos)
K0110	Conocimiento de tácticas, técnicas y procedimientos de adversarios
K0111	Conocimiento de herramientas de red (por ejemplo, ping, traceroute, nslookup)

Id. de los CHC	Descripción
K0112	Conocimiento de principios de defensa en profundidad y arquitectura de seguridad de red
K0113	Conocimiento de diferentes tipos de comunicación de red (por ejemplo, red de área local [LAN, por sus siglas en inglés], red de área extensa [WAN, por sus siglas en inglés], red de área metropolitana [MAN, por sus siglas en inglés], red de área local inalámbrica [WLAN, por sus siglas en inglés], red de área extensa inalámbrica [WWAN, por sus siglas en inglés])
K0114	Conocimiento de dispositivos electrónicos (por ejemplo, sistemas y componentes informáticos, dispositivos de control de acceso, cámaras digitales, escáneres digitales, agendas electrónicas, discos duros, tarjetas de memoria, módems, componentes de red, dispositivos en red, dispositivos en red de control domótico, impresoras, dispositivos de almacenamiento extraíbles, teléfonos, copiadoras, máquinas de fax, etc.)
K0115	Conocimiento de que la tecnología puede ser explotada
K0116	Conocimiento de extensiones de archivo (por ejemplo, .dll, .bat, .zip, .pcap, .gzip)
K0117	Conocimiento de implementaciones de sistemas de archivos (por ejemplo, sistema de archivos de nueva tecnología [NTFS, por sus siglas en inglés], tabla de asignación de archivos [FAT, por sus siglas en inglés], extensión de archivo [EXT, por sus siglas en inglés])
K0118	Conocimiento de procesos para la incautación y conservación de pruebas digitales
K0119	Conocimiento de metodologías de piratería
K0120	Conocimiento de la manera en que se interpretan, siguen y priorizan las necesidades de información y los requisitos de recolección en toda la empresa
K0121	Conocimiento de gestión de programas de seguridad de la información, y de principios y técnicas de gestión de proyectos
K0122	Conocimiento de implicaciones investigativas del hardware, sistemas operativos y tecnologías de red
K0123	Conocimiento de gobernanza legal relacionada con la admisibilidad (por ejemplo, reglas de pruebas)
K0124	Conocimiento de dominios cognitivos múltiples y herramientas y métodos aplicables para el aprendizaje en cada dominio
K0125	Conocimiento de procesos de recolección, empaquetado, transporte y almacenamiento de pruebas electrónicas para mantener la cadena de custodia
K0126	Conocimiento de prácticas de gestión de riesgos de la cadena de suministro (Publicación especial 800-161 del NIST)
K0127	Conocimiento de la naturaleza y la función de la estructura de información pertinente (por ejemplo, Infraestructura nacional de información)
K0128	Conocimiento de tipos y recolección de datos persistentes
K0129	Conocimiento de herramientas de línea de comandos (por ejemplo, mkdir, mv, ls, passwd, grep)
K0130	Conocimiento de tecnologías de virtualización y de desarrollo y mantenimiento de máquinas virtuales
K0131	Conocimiento de recolección de correo web, técnicas de búsqueda y análisis, herramientas y cookies
K0132	Conocimiento de archivos de sistema (por ejemplo, archivos de registros, archivos del registro, archivos de configuración) que contengan información pertinente y del lugar donde se encuentran esos archivos de sistema
K0133	Conocimiento de tipos de datos forenses digitales y de cómo reconocerlos
K0134	Conocimiento de técnicas forenses implementables
K0135	Conocimiento de tecnologías de filtrado web

Id. de los CHC	Descripción
K0136	Conocimiento de las capacidades de los diferentes sistemas y métodos de comunicación electrónica (por ejemplo, correo electrónico, voz sobre protocolo de internet [VoIP, por sus siglas en inglés], mensajería instantánea, foros web, difusiones de video en directo)
K0137	Conocimiento de la gama de redes existentes (por ejemplo, PBX, LAN, WAN, WIFI, SCADA)
K0138	Conocimiento de wifi
K0139	Conocimiento de lenguajes informáticos interpretados y compilados
K0140	Conocimiento de técnicas de codificación segura
K0141	Retirado: se integró en K0420.
K0142	Conocimiento de procesos, capacidades y limitaciones de gestión de la recolección
K0143	Conocimiento de sistemas de recolección front-end, incluida recolección, filtrado y selección del tráfico
K0144	Conocimiento de dinámica social de los atacantes informáticos en un contexto global
K0145	Conocimiento de herramientas de correlación de eventos de seguridad
K0146	Conocimiento de los principales procesos de negocios y de la misión de la organización
K0147	Conocimiento de problemas, riesgos y vulnerabilidades de seguridad emergentes
K0148	Conocimiento de reglamentos de control de importaciones y exportaciones y los organismos responsables, a fin de reducir el riesgo de la cadena de suministro
K0149	Conocimiento de la tolerancia al riesgo o del método de gestión de riesgos de la organización
K0150	Conocimiento del programa, funciones y responsabilidades de la respuesta a incidentes de la empresa
K0151	Conocimiento de amenazas y vectores de amenazas actuales y emergentes
K0152	Conocimiento de principios y métodos de seguridad de tecnología de la información (TI) relacionados con el software (por ejemplo, modularidad, disposición en capas, abstracción, ocultación de datos, simplicidad y minimización)
K0153	Conocimiento de procesos de control de calidad del software
K0154	Conocimiento de normas, procesos y prácticas de la gestión de riesgos de la cadena de suministro
K0155	Conocimiento de leyes de pruebas electrónicas
K0156	Conocimiento de las normas legales sobre pruebas y procedimientos judiciales
K0157	Conocimiento de políticas, procedimientos y reglamentos de ciberdefensa y seguridad de la información
K0158	Conocimiento de políticas organizativas de tecnología de la información (TI) sobre la seguridad del usuario (por ejemplo, creación de cuentas, normas de contraseñas, control del acceso)
K0159	Conocimiento de transmisión de voz sobre protocolo de internet (VoIP)
K0160	Conocimiento de los vectores de ataque comunes en la capa de la red
K0161	Conocimiento de diferentes clases de ataques (por ejemplo, ataques pasivos, activos, internos, cercanos, de distribución)
K0162	Conocimiento de ciberatacantes (por ejemplo, script kiddies, amenazas internas, patrocinados por un grupo sin un país reconocido y patrocinados por un país)
K0163	Conocimiento de requisitos esenciales de adquisición de tecnología de la información (TI)
K0164	Conocimiento de requisitos de funcionalidad, calidad y seguridad, y la manera en que estos se aplican a elementos específicos del suministro (es decir, elementos y procesos)
K0165	Conocimiento de evaluación de riesgos y amenazas

Id. de los CHC	Descripción
K0167	Conocimiento de técnicas de administración de sistemas y técnicas de protección de redes y sistemas operativos
K0168	Conocimiento de leyes, estatutos (por ejemplo, los títulos 10, 18, 32, 50 del Código de los Estados Unidos), directivas presidenciales, directrices del poder ejecutivo o directrices y procedimientos legales administrativos o penales aplicables
K0169	Conocimiento de seguridad de la cadena de suministro de tecnología de la información (TI) y políticas, requisitos y procedimientos de gestión de riesgos de la cadena de suministro
K0170	Conocimiento de sistemas de infraestructura crítica con tecnología de comunicación de la información que fueron diseñados sin ninguna consideración de seguridad del sistema
K0171	Conocimiento de técnicas de ingeniería inversa de hardware
K0172	Conocimiento de middleware (por ejemplo, bus de servicio empresarial y colas de mensajes)
K0174	Conocimiento de protocolos de red
K0175	Conocimiento de técnicas de ingeniería inversa de software
K0176	Conocimiento de esquemas de lenguaje de marcado extensible (XML)
K0177	Conocimiento de etapas de los ciberataques (por ejemplo, reconocimiento, exploración, enumeración, logro del acceso, aumento de privilegios, mantenimiento del acceso, explotación de la red, ocultación de pistas)
K0178	Conocimiento de metodologías, herramientas y prácticas seguras de implementación de software
K0179	Conocimiento de conceptos de arquitectura de la seguridad de la red, incluidos topología, protocolos, componentes y principios (por ejemplo, aplicación de la defensa en profundidad)
K0180	Conocimiento de principios, modelos, métodos (por ejemplo, vigilancia del rendimiento de sistemas de extremo a extremo) y herramientas de gestión de sistemas de redes
K0182	Conocimiento de herramientas y técnicas de recuperación de datos (por ejemplo, Foremost)
K0183	Conocimiento de conceptos de ingeniería inversa
K0184	Conocimiento de tácticas, técnicas y procedimientos antiforenses
K0185	Conocimiento de aplicaciones de configuración y soporte de diseño de laboratorios forenses (por ejemplo, VMware, Wireshark)
K0186	Conocimiento de procedimientos y herramientas de depuración
K0187	Conocimiento del abuso de adversarios de los tipos de archivos en busca de comportamiento anómalo
K0188	Conocimiento de herramientas de análisis de malware (por ejemplo, OllyDbg, IDA Pro)
K0189	Conocimiento de malware con detección de máquinas virtuales (por ejemplo, malware que detectan recursos virtuales, malware que detecta depuradores y malware desempaquetado que busca cadenas relacionadas con máquinas virtuales en la pantalla de una computadora)
K0190	Conocimiento de metodologías de cifrado
K0191	Impacto de la implementación de firmas para virus, malware y ataques
K0192	Conocimiento de puertos y servicios de Windows y Unix
K0193	Conocimiento de funciones avanzadas de seguridad para la corrección de datos en bases de datos
K0194	Conocimiento de tecnologías de gestión del conocimiento basadas en la nube y conceptos relacionados con seguridad, gobernanza, adquisiciones y administración
K0195	Conocimiento de normas y metodologías de clasificación de datos que se basan en la confidencialidad y otros factores de riesgo

Id. de los CHC	Descripción
K0196	Conocimiento de reglamentos de importación y exportación relacionados con la criptografía y otras tecnologías de seguridad
K0197	Conocimiento de interfaces de programación de aplicaciones de acceso a bases de datos (por ejemplo, Java Database Connectivity [JDBC, por sus siglas en inglés])
K0198	Conocimiento de conceptos de mejoramiento de procesos organizativos y modelos de madurez de procesos (por ejemplo, Integración de modelos de madurez de capacidades [CMMI, por sus siglas en inglés] para el desarrollo, CMMI para servicios y CMMI para adquisiciones)
K0199	Conocimiento de conceptos de arquitectura de seguridad y modelos de referencia de arquitecturas empresariales (por ejemplo, Zachman, arquitectura empresarial federal [FEA, por sus siglas en inglés])
K0200	Conocimiento de conceptos de gestión de servicios para redes y estándares afines (por ejemplo, biblioteca de infraestructura de tecnología de la información [ITIL], versión vigente)
K0201	Conocimiento de técnicas y conceptos de rotación de claves simétricas
K0202	Conocimiento de conceptos y funciones de firewalls de aplicaciones (por ejemplo, punto único de autenticación, auditoría y aplicación de políticas, exploración de mensajes en busca de contenido malintencionado, anonimización de datos para cumplir con las normas de la industria de tarjetas de pago [PCI, por sus siglas en inglés] y de la información de identificación personal [PII], exploración de protección contra la pérdida de datos, operaciones criptográficas aceleradas, seguridad de capa de puertos seguros [SSL, por sus siglas en inglés], procesamiento REST/JSON)
K0203	Conocimiento de modelos de seguridad (por ejemplo, modelo Bell-LaPadula, modelo de integridad Biba, modelo de integridad Clark-Wilson)
K0204	Conocimiento de técnicas de evaluación del aprendizaje (rúbricas, planes de evaluación, exámenes, pruebas cortas)
K0205	Conocimiento de técnicas básicas de endurecimiento de sistemas, redes y sistemas operativos
K0206	Conocimiento de principios y técnicas de piratería ética
K0207	Conocimiento de análisis de circuitos
K0208	Conocimiento de capacitación por computadora y de servicios de aprendizaje en línea
K0209	Conocimiento de técnicas de comunicación encubierta
K0210	Conocimiento de conceptos sobre copias de seguridad y restauración de datos
K0211	Conocimiento de requisitos de confidencialidad, integridad y disponibilidad
K0212	Conocimiento de productos de software habilitados para la ciberseguridad
K0213	Conocimiento de modelos didácticos de diseño y evaluación (por ejemplo, modelo ADDIE, modelo de Smith y Ragan, eventos de instrucción de Gagné, modelo de evaluación de Kirkpatrick)
K0214	Conocimiento de la metodología de evaluación del Marco de gestión de riesgos
K0215	Conocimiento de políticas de capacitación organizativa
K0216	Conocimiento de niveles de aprendizaje (es decir, la taxonomía de aprendizaje de Bloom)
K0217	Conocimiento de sistemas de gestión del aprendizaje y su uso en la gestión del aprendizaje
K0218	Conocimiento de estilos de aprendizaje (por ejemplo, asimilador, auditivo, cenestésico)
K0220	Conocimiento de modos de aprendizaje (por ejemplo, aprendizaje por repetición, observación)
K0221	Conocimiento del modelo de interconexión de sistemas abiertos (OSI) y los protocolos de red subyacentes (por ejemplo, TCP/IP)

Id. de los CHC	Descripción
K0222	Conocimiento de leyes, autoridades legales, restricciones y reglamentos pertinentes que conciernen a las actividades de ciberdefensa
K0223	Retirado: se integró en K0073.
K0224	Conocimiento de conceptos de administración de sistemas para sistemas operativos como Unix/Linux, IOS, Android y Windows, entre otros
K0226	Conocimiento de sistemas de capacitación organizativa
K0227	Conocimiento de diversos tipos de arquitecturas informáticas
K0228	Conocimiento de teoría de taxonomía y ontología semántica
K0229	Conocimiento de aplicaciones que pueden registrar errores, excepciones y errores y registros de aplicaciones
K0230	Conocimiento de modelos de servicios en la nube y la manera en que esos modelos pueden limitar la respuesta a incidentes
K0231	Conocimiento de protocolos, procesos y técnicas de gestión de crisis
K0233	Conocimiento del Marco nacional para el personal de ciberseguridad, funciones laborales y tareas, conocimientos, habilidades y capacidades afines
K0234	Conocimiento de capacidades cibernéticas de todo el espectro (por ejemplo, defensa, ataque, explotación)
K0235	Conocimiento de la manera de hacer uso de los centros de investigación y desarrollo, grupos de expertos, investigación académica y sistemas industriales
K0236	Conocimiento de la manera de utilizar Hadoop, Java, Python, SQL, Hive y Pig para explorar datos
K0237	Conocimiento de mejores prácticas del sector para el servicio de atención al cliente
K0238	Conocimiento de teoría y principios del aprendizaje automático
K0239	Conocimiento de técnicas y métodos de producción, comunicación y difusión de los medios de comunicación, incluidas maneras alternativas de informar a través de medios escritos, orales y visuales
K0240	Conocimiento de sistemas de seguridad de varios niveles y de soluciones entre dominios
K0241	Conocimiento de políticas, procesos y procedimientos de recursos humanos de la organización
K0242	Conocimiento de políticas de seguridad de la organización
K0243	Conocimiento de políticas, procesos y procedimientos de capacitación y educación de la organización
K0244	Conocimiento de comportamientos físicos y fisiológicos que puedan indicar actividad sospechosa o anormal
K0245	Conocimiento de principios y procesos para llevar a cabo la evaluación de necesidades de capacitación y educación
K0246	Conocimiento de conceptos, procedimientos, software, equipos y aplicaciones tecnológicas pertinentes
K0247	Conocimiento de procesos, herramientas y capacidades de acceso remoto relacionados con la asistencia al cliente
K0248	Conocimiento de teoría y práctica estratégicas
K0249	Conocimiento de tecnologías, procesos y estrategias de sostenimiento
K0250	Conocimiento de procesos de prueba y evaluación de estudiantes
K0251	Conocimiento del proceso judicial, incluida la presentación de hechos y pruebas
K0252	Conocimiento de principios y métodos de capacitación y educación para diseño, enseñanza e impartición de planes de estudios para personas y grupos, y la medición de los efectos de la capacitación y la educación

Id. de los CHC	Descripción
K0253	Retirado: se integró en K0227.
K0254	Conocimiento de análisis binario
K0255	Conocimiento de conceptos de arquitectura de red, y de topología, protocolos y componentes
K0257	Conocimiento de requisitos de adquisición y compras de tecnología de la información (TI)
K0258	Conocimiento de procedimientos, principios y metodologías de prueba (por ejemplo, Integración de modelos de madurez de capacidades [CMMI])
K0259	Conocimiento de conceptos y metodologías de análisis de malware
K0260	Conocimiento de normas de seguridad de los datos de información de identificación personal (PII)
K0261	Conocimiento de normas de seguridad de los datos de la industria de tarjetas de pago (PCI)
K0262	Conocimiento de normas de seguridad de los datos de información personal de salud (PHI, por sus siglas en inglés)
K0263	Conocimiento de políticas, requisitos y procedimientos de gestión de riesgos de la tecnología de la información (TI)
K0264	Conocimiento de planificación de protección de programas (por ejemplo, políticas de gestión de seguridad y riesgos de la cadena de suministro de tecnología de la información (TI), técnicas contra la manipulación indebida y requisitos)
K0265	Conocimiento de tecnología de la información (TI) compatible con la infraestructura para seguridad, rendimiento y confiabilidad
K0266	Conocimiento de la manera de evaluar la confiabilidad del proveedor o el producto
K0267	Conocimiento de leyes, políticas, procedimientos o gobernanza pertinentes a la ciberseguridad de infraestructuras críticas
K0268	Conocimiento de identificación de huellas forenses
K0269	Conocimiento de arquitectura de comunicaciones móviles
K0270	Conocimiento del proceso de ciclos de vida de adquisiciones y compras
K0271	Conocimiento de estructuras y datos internos del sistema operativo (por ejemplo, gestión de procesos, estructura de directorios, aplicaciones instaladas)
K0272	Conocimiento de herramientas de análisis de redes utilizadas para identificar vulnerabilidades de las comunicaciones del software
K0274	Conocimiento de registros de transmisión (por ejemplo, Bluetooth, identificación por radiofrecuencia [RFID, por sus siglas en inglés], redes por infrarrojos [IR], fidelidad inalámbrica [wifi], buscapersonas, teléfonos celulares, antenas satelitales, voz sobre protocolo de internet [VoIP]) y técnicas de interferencia que permiten la transmisión de información no deseada o impiden que los sistemas instalados funcionen correctamente
K0275	Conocimiento de técnicas de gestión de configuraciones
K0276	Conocimiento de gestión de la seguridad
K0277	Conocimiento de funciones de seguridad actuales y emergentes del cifrado de datos (por ejemplo, cifrado de columnas y espacio de tablas, cifrado de archivos y discos) en bases de datos (por ejemplo, funciones de gestión de claves criptográficas integradas)
K0278	Conocimiento de funciones de seguridad actuales y emergentes para la corrección de datos en bases de datos
K0280	Conocimiento de teorías, conceptos y métodos de ingeniería de sistemas
K0281	Conocimiento de catálogos de servicios de tecnología de la información (TI)
K0282	Retirado: se integró en K0200.
K0283	Conocimiento de casos de uso relacionados con la colaboración y la sincronización de contenido entre plataformas (por ejemplo, móviles, computadoras personales, nube)

Id. de los CHC	Descripción
K0284	Conocimiento de desarrollo y aplicación de un sistema de gestión de credenciales de usuario
K0285	Conocimiento de implementación de sistemas empresariales de custodia de claves compatibles con el cifrado de datos en reposo
K0286	Conocimiento de tipologías de N niveles (por ejemplo, sistemas operativos de servidor y cliente)
K0287	Conocimiento del programa de clasificación de la información de una organización y procedimientos para información comprometida
K0288	Conocimiento de modelos de seguridad de los estándares del sector
K0289	Conocimiento de herramientas de diagnóstico de sistema y servidores, y técnicas de identificación de errores
K0290	Conocimiento de métodos de prueba y evaluación de la seguridad de los sistemas
K0291	Conocimiento de las tendencias y los conceptos arquitectónicos de tecnología de la información (TI) empresariales (por ejemplo, referencia, diseño validado y arquitecturas de destino)
K0292	Conocimiento de las operaciones y los procesos para la gestión de incidentes, problemas y eventos
K0293	Conocimiento de integración de las metas y los objetivos de la organización en la arquitectura
K0294	Conocimiento de funcionamiento, mantenimiento y seguridad de los sistemas de TI necesarios para mantener el equipo funcionando correctamente
K0295	Conocimiento de principios de confidencialidad, integridad y disponibilidad
K0296	Conocimiento de capacidades, aplicaciones y vulnerabilidades potenciales de equipos de redes, incluidos concentradores, enrutadores, conmutadores, puentes, servidores, medios de transmisión y el hardware correspondiente
K0297	Conocimiento de diseño de contramedidas para los riesgos de seguridad identificados
K0298	Conocimiento de contramedidas para los riesgos de seguridad identificados
K0299	Conocimiento para determinar la manera en que debe funcionar un sistema de seguridad (incluidas sus capacidades de resiliencia y confiabilidad) y los efectos que los cambios en las condiciones, operaciones o el entorno tendrán en estos resultados
K0300	Conocimiento de asignación de redes y recreación de topologías de redes
K0301	Conocimiento de análisis a nivel de paquetes usando herramientas apropiadas (por ejemplo, Wireshark, tcpdump)
K0302	Conocimiento del funcionamiento básico de las computadoras
K0303	Conocimiento del uso de herramientas de subredes
K0304	Conocimiento de conceptos y prácticas del procesamiento de datos forenses digitales
K0305	Conocimiento de ocultación de datos (por ejemplo, algoritmos de cifrado y estenografía)
K0308	Conocimiento de criptología
K0309	Conocimiento de tecnologías emergentes con potencial de explotación
K0310	Conocimiento de metodologías de piratería
K0311	Conocimiento de indicadores del sector útiles para identificar las tendencias tecnológicas
K0312	Conocimiento de principios, políticas y procedimientos de obtención de inteligencia, incluidas las restricciones y autoridades legales
K0313	Conocimiento de organizaciones externas e instituciones académicas dirigidas a la cibernética (por ejemplo, plan de estudios y capacitación, e investigación y desarrollo en el campo de la cibernética)
K0314	Conocimiento de vulnerabilidades potenciales de ciberseguridad de las tecnologías del sector

Id. de los CHC	Descripción
K0315	Conocimiento de los métodos, procedimientos y técnicas principales de obtención de información, y la producción, preparación de informes e intercambio de información
K0316	Conocimiento de planes de operación, planes conceptuales de operación, órdenes, políticas y normas de combate fijas empresariales o militares
K0317	Conocimiento de procedimientos utilizados para documentar y consultar incidentes, problemas y eventos comunicados
K0318	Conocimiento de herramientas de línea de comandos del sistema operativo
K0319	Conocimiento de capacidades de entrega técnica y sus limitaciones
K0320	Conocimiento de criterios de evaluación y validación de la organización
K0321	Conocimiento de conceptos de ingeniería según su aplicación a la arquitectura informática y al hardware y el software correspondientes
K0322	Conocimiento de sistemas insertados
K0323	Conocimiento de metodologías de tolerancia a errores del sistema
K0324	Conocimiento de herramientas y aplicaciones del sistema de detección de intrusiones (IDS) y del sistema de prevención de intrusiones (IPS, por sus siglas en inglés)
K0325	Conocimiento de teoría de la información (por ejemplo, codificación de fuentes, codificación de canales, teoría de la complejidad de algoritmos y compresión de datos)
K0326	Conocimiento de zonas desmilitarizadas
K0330	Conocimiento de las capacidades correctas para identificar soluciones a problemas menos comunes y más complejos de sistemas
K0332	Conocimiento de protocolos de red, como TCP/ IP, protocolo de configuración dinámica del host, sistema de nombres de dominio (DNS, por sus siglas en inglés) y servicios de directorio
K0333	Conocimiento de procesos de diseño de red, incluidos objetivos de seguridad, objetivos operativos y compensaciones
K0334	Conocimiento de análisis del tráfico de redes (herramientas, metodologías, procesos)
K0335	Conocimiento de tecnologías cibernéticas actuales y emergentes
K0336	Conocimiento de métodos de autenticación del acceso
K0337	Retirado: se integró en K0007.
K0338	Conocimiento de técnicas de extracción de datos
K0339	Conocimiento de la manera de usar las herramientas de análisis de redes para identificar vulnerabilidades
K0341	Conocimiento de políticas extranjeras de divulgación y reglamentos de control de importaciones y exportaciones en relación con la ciberseguridad
K0342	Conocimiento de principios, herramientas y técnicas de pruebas de penetración
K0343	Conocimiento de técnicas de análisis de las causas principales
K0344	Conocimiento del entorno de amenazas de una organización
K0346	Conocimiento de principios y métodos de integración de los componentes de un sistema
K0347	Conocimiento y comprensión del diseño operativo
K0349	Conocimiento de tipos, administración y funciones de sitios web y del sistema de gestión de contenidos (CMS, por sus siglas en inglés)
K0350	Conocimiento de sistemas aceptados de planificación de la organización
K0351	Conocimiento de estatutos, leyes, reglamentos y políticas aplicables que rigen la selección y explotación de objetivos cibernéticos
K0352	Conocimiento de necesidades de soporte, temas y áreas de enfoque de las formas de inteligencia

Id. de los CHC	Descripción
K0353	Conocimiento de posibles circunstancias que darían lugar a cambios en las autoridades de gestión de la recolección
K0354	Conocimiento de procedimientos pertinentes de preparación de informes y difusión
K0355	Conocimiento de procedimientos de preparación de informes y difusión de todas las fuentes
K0356	Conocimiento de herramientas y técnicas analíticas para material lingüístico, de voz o gráfico
K0357	Conocimiento de constructos analíticos y su uso en la evaluación del entorno operativo
K0358	Conocimiento de normas analíticas y el propósito de los niveles de confianza de la información de inteligencia
K0359	Conocimiento de procesos aprobados de difusión de inteligencia
K0361	Conocimiento de disponibilidad, capacidades y limitaciones de recursos
K0362	Conocimiento de métodos y técnicas de ataque (ataque de denegación de servicio distribuido [DDoS, por sus siglas en inglés], fuerza bruta, suplantación de identidad, etc.)
K0363	Conocimiento de procedimientos de auditoría y registro (incluidos registros basados en servidores)
K0364	Conocimiento de bases de datos disponibles y herramientas necesarias para evaluar la asignación correcta de tareas de recolección
K0367	Conocimiento de pruebas de penetración
K0368	Conocimiento de implantes que habilitan la recolección o las actividades de preparación en materia de cibernética
K0371	Conocimiento de principios de los procesos de desarrollo de la recolección (por ejemplo, reconocimiento de números marcados, análisis de redes sociales)
K0372	Conocimiento de conceptos de programación (por ejemplo, niveles, estructuras, lenguajes compilados y lenguajes interpretados)
K0373	Conocimiento de aplicaciones de software básicas (por ejemplo, almacenamiento y copias de seguridad de datos, aplicaciones de bases de datos) y los tipos de vulnerabilidades que se han encontrado en esas aplicaciones
K0375	Conocimiento de vulnerabilidades de las aplicaciones inalámbricas
K0376	Conocimiento de clientes y organizaciones de socios internos y externos, incluidas necesidades de información, objetivos, estructura, capacidades, etc.
K0377	Conocimiento de normas, políticas y procedimientos para marcado de clasificaciones y controles
K0379	Conocimiento de organizaciones de clientes, incluidas necesidades de información, objetivos, estructura, capacidades, etc.
K0380	Conocimiento de herramientas y entornos de colaboración
K0381	Conocimiento de daños colaterales y cálculo de impactos
K0382	Conocimiento de capacidades y limitaciones de la recolección
K0383	Conocimiento de capacidades, accesos, especificaciones del rendimiento y limitaciones de la recolección utilizados para cumplir el plan de recolección
K0384	Conocimiento de funcionalidades de gestión de la recolección (por ejemplo, puestos, funciones, responsabilidades, productos, requisitos de preparación de informes)
K0385	Retirado: se integró en K0142.
K0386	Conocimiento de herramientas de gestión de la recolección
K0387	Conocimiento del proceso de planificación de la recolección y del plan de recolección

Id. de los CHC	Descripción
K0388	Conocimiento de técnicas y herramientas de búsqueda y análisis de la recolección para listas de chat y listas de amigos, tecnologías emergentes, VoIP, medios sobre IP, VPN, terminal de apertura muy pequeña (VSAT, por sus siglas en inglés) e inalámbricos, correo web y cookies
K0389	Conocimiento de fuentes de recolección, incluidas fuentes convencionales y no convencionales
K0390	Conocimiento de estrategias de recolección
K0391	Conocimiento de sistemas, capacidades y procesos de recolección
K0392	Conocimiento de infecciones comunes de computadoras y redes (virus, troyanos, etc.) y métodos de infección (puertos, archivos adjuntos, etc.)
K0393	Conocimiento de dispositivos de red comunes y sus configuraciones
K0394	Conocimiento de bases de datos y herramientas comunes para la preparación de informes
K0395	Conocimiento de fundamentos de las redes informáticas (es decir, componentes informáticos básicos de una red, tipos de redes, etc.)
K0396	Conocimiento de conceptos de programación informática, incluidos lenguajes de computación, programación, pruebas, depuración y tipos de archivos
K0397	Conocimiento de conceptos de seguridad en sistemas operativos (por ejemplo, Linux, Unix)
K0398	Conocimiento de conceptos relacionados con sitios web (por ejemplo, servidores y páginas web, hospedaje, DNS, registro, lenguajes web como HTML)
K0399	Conocimiento de procedimientos para la planificación de acciones en casos de crisis y la planificación urgente
K0400	Conocimiento de planificación de acciones en casos de crisis para las ciberoperaciones
K0401	Conocimiento de criterios para evaluar productos de recolección
K0402	Conocimiento de factores de criticidad y vulnerabilidad (por ejemplo, valor, recuperación, atenuación, contramedidas) para la selección de objetivos y la aplicabilidad al dominio cibernético
K0403	Conocimiento de capacidades y limitaciones criptológicas y sus contribuciones a las ciberoperaciones
K0404	Conocimiento de requisitos de recolección actuales
K0405	Conocimiento de conjuntos informáticos de intrusión actuales
K0406	Conocimiento de software y metodologías actuales para la defensa activa y el endurecimiento de sistemas
K0407	Conocimiento de necesidades de información del cliente
K0408	Conocimiento de principios, capacidades, limitaciones y efectos de las acciones cibernéticas (es decir, ciberdefensa, obtención de información, preparación del entorno, ciberataques)
K0409	Conocimiento de capacidades y repositorios de recolección de ciberinteligencia y ciberinformación
K0410	Conocimiento de derecho informático y su efecto en la planificación cibernética
K0411	Conocimiento de derecho informático y consideraciones jurídicas y su efecto en la planificación cibernética
K0412	Conocimiento de léxico o terminología del ámbito cibernético
K0413	Conocimiento de objetivos, políticas y cuestiones legales de las ciberoperaciones
K0414	Conocimiento de soporte o procesos habilitantes de las ciberoperaciones
K0415	Conocimiento de léxico o terminología del ámbito de las ciberoperaciones
K0416	Conocimiento de ciberoperaciones

Id. de los CHC	Descripción
K0417	Conocimiento de terminología de las comunicaciones de datos (por ejemplo, protocolos de redes, Ethernet, IP, cifrado, dispositivos ópticos, medios extraíbles)
K0418	Conocimiento de procesos de flujos de datos para la recolección de terminales o entornos
K0419	Conocimiento de administración y mantenimiento de bases de datos
K0420	Conocimiento de teoría de bases de datos
K0421	Conocimiento de bases de datos, portales y vehículos de difusión afines
K0422	Conocimiento de procesos y procedimientos de eliminación de conflictos
K0423	Conocimiento de preparación de informes sobre eliminación de conflictos, incluida la interacción externa de la organización
K0424	Conocimiento de técnicas de negación y engaño
K0425	Conocimiento de diferentes objetivos de la organización en todos niveles, incluidos los subordinados, laterales y superiores
K0426	Conocimiento de selección dinámica y deliberada de los objetivos
K0427	Conocimiento de algoritmos de cifrado y capacidades y herramientas cibernéticas (por ejemplo, SSL, PGP)
K0428	Conocimiento de algoritmos de cifrado y herramientas para redes de área local inalámbricas (WLAN)
K0429	Conocimiento de gestión de la información en toda la empresa
K0430	Conocimiento de estrategias y técnicas de evasión
K0431	Conocimiento de tecnologías de comunicación en evolución y emergentes
K0432	Conocimiento de problemas existentes, emergentes y de largo alcance relacionados con la estrategia, las políticas y la organización de las ciberoperaciones
K0433	Conocimiento de implicaciones forenses de la estructura y las operaciones del sistema operativo
K0435	Conocimiento de conceptos, principios, limitaciones y efectos fundamentales de la cibernética
K0436	Conocimiento de conceptos, terminología o léxico (es decir, preparación de entornos, ciberataques, ciberdefensa), principios, capacidades, limitaciones y efectos fundamentales de las ciberoperaciones
K0437	Conocimiento de componentes generales de sistemas de control de supervisión y adquisición de datos (SCADA)
K0438	Conocimiento de arquitectura de comunicaciones celulares móviles (por ejemplo, evolución a largo plazo [LTE, por sus siglas en inglés], acceso múltiple por división de código [CDMA, por sus siglas en inglés], sistema global de comunicaciones móviles/velocidad de datos mejorada para la evolución del GSM [GSM/EDGE, por sus siglas en inglés] y sistema de telecomunicaciones móviles universales/acceso de paquetes a alta velocidad [UMTS/HSPA, por sus siglas en inglés])
K0439	Conocimiento de autoridades gubernamentales a cargo de la selección de objetivos
K0440	Conocimiento de productos de seguridad basados en hosts y el efecto de estos productos en la explotación y la reducción de la vulnerabilidad
K0442	Conocimiento de la manera en que las tecnologías convergentes afectan las ciberoperaciones (por ejemplo, digitales, de telefonía, inalámbricas)
K0443	Conocimiento de la manera en que los concentradores, conmutadores y enrutadores funcionan en conjunto en el diseño de una red
K0444	Conocimiento del funcionamiento de las aplicaciones de internet (correo electrónico de protocolo simple de transferencia [SMTP, por sus siglas en inglés], correo electrónico basado en la web, clientes de chat, VoIP)

Id. de los CHC	Descripción
K0445	Conocimiento del efecto de las redes digitales y la telefonía modernas en las ciberoperaciones
K0446	Conocimiento del efecto de los sistemas de comunicaciones inalámbricas modernos en las ciberoperaciones
K0447	Conocimiento de la manera de recolectar, ver e identificar la información esencial sobre objetivos de interés de los metadatos (por ejemplo, correo electrónico, protocolo de transferencia de hipertexto [http, por sus siglas en inglés])
K0448	Conocimiento de la manera de establecer prioridades para los recursos
K0449	Conocimiento de la manera de extraer, analizar y utilizar metadatos
K0450	Retirado: se integró en K0036.
K0451	Conocimiento de procesos de identificación y preparación de informes
K0452	Conocimiento de implementación de los sistemas Unix y Windows que proporcionan autenticación y registro con protocolo RADIUS, DNS, correo, servicio web, servidor con protocolo de transferencia de archivos [FTP, por sus siglas en inglés], protocolo de configuración dinámica del anfitrión [DHCP, por sus siglas en inglés], firewall y protocolo simple de gestión de red [SNMP, por sus siglas en inglés]
K0453	Conocimiento de indicaciones y advertencias
K0454	Conocimiento de necesidades de información
K0455	Conocimiento de conceptos, métodos y tecnologías de facilitación de seguridad de la información
K0456	Conocimiento de capacidades y limitaciones de inteligencia
K0457	Conocimiento de niveles de confianza de inteligencia
K0458	Conocimiento de disciplinas de inteligencia
K0459	Conocimiento de requisitos del empleo de inteligencia (es decir, logística, soporte de comunicaciones, maniobrabilidad, restricciones legales, etc.)
K0460	Conocimiento de preparación de entornos de inteligencia y procesos similares
K0461	Conocimiento de procesos de producción de inteligencia
K0462	Conocimiento de principios, políticas, procedimientos y vehículos de preparación de informes de inteligencia, incluidos formatos de informes, criterios de capacidad de informes (requisitos y prioridades), prácticas de difusión y autoridades y restricciones legales
K0463	Conocimiento de sistemas de asignación de tareas para los requisitos de inteligencia
K0464	Conocimiento de la ayuda de inteligencia para la planificación, ejecución y evaluación
K0465	Conocimiento de capacidades y herramientas de las ciberoperaciones de socios internos y externos
K0466	Conocimiento de procesos de inteligencia de los socios internos y externos y la preparación de requisitos de información y de información esencial
K0467	Conocimiento de capacidades y limitaciones de las organizaciones de socios internos y externos (aquellas con responsabilidades de asignación de tareas, recolección, procesamiento, explotación y difusión)
K0468	Conocimiento de preparación de informes de socios internos y externos
K0469	Conocimiento de tácticas internas para prever o emular las capacidades y acciones de amenazas
K0470	Conocimiento de internet y de protocolos de enrutamiento
K0471	Conocimiento de direccionamiento de la red de internet (direcciones IP, enrutamiento entre dominios sin clase, numeración de puertos con protocolo de control de transmisión/protocolo de datagramas de usuario [TCP/UDP, por sus siglas en inglés])
K0472	Conocimiento de sistemas de detección de intrusiones y creación de firmas

Id. de los CHC	Descripción
K0473	Conocimiento de conjuntos de intrusión
K0474	Conocimiento de actores clave de ciberamenazas y sus recursos
K0475	Conocimiento de factores clave del entorno operativo y la amenaza
K0476	Conocimiento de herramientas y técnicas de procesamiento de lenguajes
K0477	Conocimiento de intenciones y objetivos de la dirección
K0478	Conocimiento de consideraciones legales en la selección de objetivos
K0479	Conocimiento de análisis y características del malware
K0480	Conocimiento de malware
K0481	Conocimiento de métodos y técnicas utilizados para detectar diversas actividades de explotación
K0482	Conocimiento de métodos para confirmar la postura y disponibilidad de los recursos de recolección
K0483	Conocimiento de métodos para integrar y resumir la información de fuentes potenciales
K0484	Conocimiento de recolección de punto medio (proceso, metas, organización, objetivos, etc.)
K0485	Conocimiento de administración de redes
K0486	Conocimiento de construcción y topología de redes
K0487	Conocimiento de seguridad de redes (por ejemplo, cifrado, firewalls, autenticación, señuelos, protección perimetral)
K0488	Conocimiento de implementaciones de seguridad de redes (por ejemplo, IDS basado en hosts, IPS, listas de control de accesos), incluidas su función y colocación en una red
K0489	Conocimiento de topología de redes
K0490	Retirado: se integró en K0058.
K0491	Conocimiento de fundamentos de redes y comunicaciones por internet (es decir, dispositivos, configuración de dispositivos, hardware, software, aplicaciones, puertos y protocolos, direccionamiento, arquitectura e infraestructura de redes, enrutamiento, sistemas operativos, etc.)
K0492	Conocimiento de metodologías de recolección no tradicionales
K0493	Conocimiento de técnicas de ofuscación (por ejemplo, TOR/Onion/anonimizadores, red privada virtual/servidor privado virtual [VPN/VPS, por sus siglas en inglés], cifrado)
K0494	Conocimiento de objetivos, situación, entorno operativo y estado y disposición de las capacidades de recolección de los socios internos y externos disponibles para el soporte de la planificación
K0495	Conocimiento de operaciones en curso y futuras
K0496	Conocimiento de limitaciones de los recursos operativos
K0497	Conocimiento de evaluación de la efectividad operativa
K0498	Conocimiento de procesos de planificación operativa
K0499	Conocimiento de seguridad de las operaciones
K0500	Conocimiento de sistemas, capacidades y procesos de recolección de las organizaciones o socios (por ejemplo, procesadores de recolección y protocolos)
K0501	Conocimiento de programas, estrategias y recursos de ciberoperaciones de la organización
K0502	Conocimiento de herramientas o métodos de ayuda para la toma de decisiones de la organización
K0503	Conocimiento de formatos de la organización para la preparación de informes acerca de la disponibilidad de recursos y activos, su pertinencia operativa e impacto en la recolección de inteligencia

Id. de los CHC	Descripción
K0504	Conocimiento de problemas, objetivos y operaciones de la organización en el ámbito cibernético, así como de reglamentos y directivas de las políticas que rigen las ciberoperaciones
K0505	Conocimiento de objetivos de la organización y la exigencia correspondiente en la gestión de recolección
K0506	Conocimiento de objetivos, prioridades de la dirección y riesgos para la toma de decisiones de la organización
K0507	Conocimiento de explotación de redes digitales perpetrada por las organizaciones o los socios
K0508	Conocimiento de políticas de organización y conceptos de planificación para asociarse con organizaciones internas o externas
K0509	Conocimiento de autoridades, responsabilidades y contribuciones de la organización y los socios para alcanzar los objetivos
K0510	Conocimiento de políticas, herramientas, capacidades y procedimientos de la organización y los socios
K0511	Conocimiento de jerarquías y procesos organizativos para la toma de decisiones en materia cibernética
K0512	Conocimiento de conceptos de planificación organizativa
K0513	Conocimiento de prioridades, autoridades jurídicas y procesos organizativos para la presentación de requisitos
K0514	Conocimiento de estructuras organizativas y capacidades de inteligencia afines
K0516	Conocimiento de dispositivos de red físicos y lógicos e infraestructura, incluidos concentradores, conmutadores, enrutadores, firewalls, etc.
K0517	Conocimiento del proceso de aprobación de la revisión posterior a la implementación (PIR, por sus siglas en inglés)
K0518	Conocimiento del inicio de la actividad de planificación
K0519	Conocimiento de planificación de calendarios adaptativos y acciones en casos de crisis, y de planificación urgente
K0520	Conocimiento de principios y prácticas relacionados con el establecimiento de objetivos, como conocimiento, asociaciones, sistemas de comunicación e infraestructura de objetivos
K0521	Conocimiento de información prioritaria, manera de obtenerla, sitios donde publicarla, modo de acceso a esta, etc.
K0522	Conocimiento de necesidades y arquitecturas de la explotación y la difusión de la producción
K0523	Conocimiento de productos y nomenclatura de los principales proveedores (por ejemplo, conjuntos de aplicaciones de seguridad, como Trend Micro, Symantec, McAfee, Outpost y Panda) y la manera en que estos productos afectan la explotación y reducen las vulnerabilidades
K0524	Conocimiento de leyes, reglamentos y políticas pertinentes
K0525	Conocimiento de productos necesarios para la planificación de inteligencia asociados con la planificación operativa cibernética
K0526	Conocimiento de estrategias de investigación y gestión del conocimiento
K0527	Conocimiento de gestión de riesgos y estrategias de mitigación
K0528	Conocimiento de sistemas de comunicación por satélite
K0529	Conocimiento de secuencias de comandos
K0530	Conocimiento de opciones de hardware y software de seguridad, incluidos los artefactos de las redes que inducen y sus efectos en la explotación
K0531	Conocimiento de implicaciones de seguridad de las configuraciones de software

Id. de los CHC	Descripción
K0532	Conocimiento de lenguaje especializado del objetivo (por ejemplo, siglas, jerga, terminología técnica, palabras clave)
K0533	Conocimiento de identificadores de objetivos específicos y su uso
K0534	Conocimiento de procesos de administración, asignación y distribución del personal
K0535	Conocimiento de estrategias y herramientas para investigar al objetivo
K0536	Conocimiento de estructura, método, estrategia de las herramientas de explotación (por ejemplo, analizadores de protocolo, registradores de pulsaciones de teclas) y técnicas (por ejemplo, logro de acceso a la puerta trasera, recolección y filtro de datos, análisis de vulnerabilidades de otros sistemas en la red)
K0538	Conocimiento de estructuras de objetivos y amenazas de la organización, capacidades y vulnerabilidades críticas
K0539	Conocimiento de perfiles de comunicación de los objetivos y sus elementos clave (por ejemplo, asociaciones, actividades, infraestructura de comunicación de los objetivos)
K0540	Conocimiento de herramientas y técnicas de comunicación de los objetivos
K0541	Conocimiento de referencias culturales, dialectos, expresiones, modismos y abreviaturas de los objetivos
K0542	Conocimiento de establecimiento de objetivos (es decir, conceptos, funciones, responsabilidades, productos, etc.)
K0543	Conocimiento de tiempos estimados de reparación y recuperación de los objetivos
K0544	Conocimiento de técnicas de obtención de inteligencia y de preparación operativa y ciclos de vida de los objetivos
K0545	Conocimiento de idiomas de los objetivos
K0546	Conocimiento de preparación de listas de objetivos (es decir restringida, conjunta, candidatos, etc.)
K0547	Conocimiento de métodos y procedimientos de objetivos
K0548	Conocimiento de objetivos o de actores y procedimientos de las ciberamenazas
K0549	Conocimiento de procedimientos de investigación y validación de objetivos
K0550	Conocimiento de objetivos, incluidos eventos actuales, perfil de comunicaciones, actores e historia (idioma, cultura) o marco de referencia que se relacionen con estos
K0551	Conocimiento de ciclos de selección de objetivos
K0552	Conocimiento de mecanismos de asignación de tareas
K0553	Conocimiento de procesos de asignación de tareas para los recursos orgánicos y subordinados de recolección
K0554	Conocimiento de asignación de tareas, recolección, procesamiento, explotación y difusión
K0555	Conocimiento de protocolos TCP/IP de redes
K0556	Conocimiento de fundamentos de las telecomunicaciones
K0557	Conocimiento de recolección de terminales o entornos (proceso, metas, organización, objetivos, etc.)
K0558	Conocimiento de las herramientas y aplicaciones disponibles asociadas con los requisitos de recolección y la gestión de recolección
K0559	Conocimiento de la estructura, arquitectura y diseño básicos de aplicaciones convergidas
K0560	Conocimiento de la estructura, arquitectura y diseño básicos de redes de comunicaciones modernas
K0561	Conocimiento de los fundamentos de seguridad de red (por ejemplo, cifrado, firewalls, autenticación, señuelos, protección perimetral)
K0562	Conocimiento de las capacidades y limitaciones de las capacidades, accesos o procesos de recolección nuevos y emergentes

Id. de los CHC	Descripción
K0563	Conocimiento de las capacidades, limitaciones y metodologías de asignación de tareas para las recolecciones internas y externas como se aplican a las actividades cibernéticas planificadas
K0564	Conocimiento de las características de las redes de comunicación seleccionadas como objetivo (por ejemplo, capacidad, funcionalidad, rutas, nodos críticos)
K0565	Conocimiento de los protocolos comunes de red y enrutamiento (por ejemplo, TCP/IP), servicios (por ejemplo, web, correo, DNS) y la manera en que interactúan para proporcionar comunicaciones de red
K0566	Conocimiento de los requisitos de información críticos y la manera en que se usan en la planificación
K0567	Conocimiento del flujo de datos desde el origen de la recolección hasta los repositorios y las herramientas
K0568	Conocimiento de la definición de gestión de recolección y autoridad de la gestión de recolección
K0569	Conocimiento de la arquitectura existente de asignación de tareas, recolección, procesamiento, explotación y difusión
K0570	Conocimiento de los factores de amenaza que podrían afectar las operaciones de recolección
K0571	Conocimiento del ciclo de retroalimentación en los procesos de recolección
K0572	Conocimiento de las funciones y capacidades de los equipos internos que emulan las actividades de amenaza en beneficio de la organización
K0573	Conocimiento de fundamentos del análisis forense digital para extraer inteligencia procesable
K0574	Conocimiento del impacto del análisis lingüístico en las funciones del operador en red
K0575	Conocimiento del impacto de las estimaciones del personal de socios internos y externos
K0576	Conocimiento del entorno de la información
K0577	Conocimiento de los marcos, procesos y sistemas de inteligencia afines
K0578	Conocimiento del desarrollo de los requisitos de inteligencia y los procesos de solicitud de información
K0579	Conocimiento de la organización, funciones y responsabilidades de los subelementos superiores, inferiores y adyacentes
K0580	Conocimiento del formato establecido por la organización para el plan de recolección
K0581	Conocimiento de los ciclos de planificación, operaciones y selección de objetivos de la organización
K0582	Conocimiento del proceso organizativo de planificación y dotación de personal
K0583	Conocimiento de los planes, directivas y orientación de la organización que describen los objetivos
K0584	Conocimiento de las políticas y procedimientos organizativos para la transferencia temporal de la autoridad de recolección
K0585	Conocimiento de la estructura organizativa en lo que atañe a las ciberoperaciones de espectro completo, incluidas las funciones, responsabilidades e interrelaciones entre los distintos elementos internos
K0586	Conocimiento de los resultados del plan de acción y el análisis del ejercicio
K0587	Conocimiento de los puntos de contacto, bases de datos, herramientas y aplicaciones necesarios para establecer productos de preparación del entorno y vigilancia
K0588	Conocimiento de los requisitos de información prioritarios de los niveles subordinado, lateral y superior de la organización

Id. de los CHC	Descripción
K0589	Conocimiento del proceso usado para evaluar el rendimiento y el impacto de las operaciones
K0590	Conocimiento de los procesos para sincronizar los procedimientos de evaluación operativa con el proceso de requisitos de información esencial
K0591	Conocimiento de las responsabilidades de producción, y las capacidades orgánicas de análisis y producción
K0592	Conocimiento de la finalidad y contribución de las plantillas de objetivos
K0593	Conocimiento de la gama de ciberoperaciones y sus necesidades, temas y áreas de enfoque subyacentes de ayuda de inteligencia
K0594	Conocimiento de las relaciones entre estados finales, objetivos, efectos, líneas de operación, etc.
K0595	Conocimiento de las relaciones de los objetivos operativos, requisitos de inteligencia y tareas de producción de inteligencia
K0596	Conocimiento del proceso de solicitud de información
K0597	Conocimiento de la función de las operaciones de redes en la ayuda y facilitación de otras operaciones de la organización
K0598	Conocimiento de la estructura e intención de los planes, orientación y autorizaciones específicos de la organización
K0599	Conocimiento de la estructura, arquitectura y diseño de redes digitales y de telefonía modernas
K0600	Conocimiento de la estructura, arquitectura y diseño de los sistemas modernos de comunicaciones inalámbricas
K0601	Conocimiento de los sistemas, arquitectura y comunicaciones usados para la coordinación
K0602	Conocimiento de disciplinas y capacidades de recolección
K0603	Conocimiento de las formas en que los objetivos o las amenazas usan la internet
K0604	Conocimiento de sistemas de amenazas u objetivos
K0605	Conocimiento de los métodos de señalamiento, secuenciación, mezcla y redundancia
K0606	Conocimiento de procesos y técnicas para transcribir (por ejemplo, de manera textual o resumida, o lo esencial)
K0607	Conocimiento de procesos y técnicas de traducción
K0608	Conocimiento de estructuras y datos internos de los sistemas operativos Unix/Linux y Windows (por ejemplo, gestión de procesos, estructura de directorios, aplicaciones instaladas)
K0609	Conocimiento de tecnologías de máquinas virtuales
K0610	Conocimiento de productos de virtualización (VMware, Virtual PC)
K0611	Retirado: se integró en K0131.
K0612	Conocimiento de lo que constituye una “amenaza” para una red
K0613	Conocimiento de quiénes son los planificadores operativos de la organización, cómo y dónde pueden ser contactados y cuáles son sus expectativas
K0614	Conocimiento de tecnologías inalámbricas (por ejemplo, celulares, satelitales, GSM) que incluyen estructura, arquitectura y diseño básicos de sistemas modernos de comunicaciones inalámbricas
K0615	Conocimiento de declaraciones de divulgación de privacidad basadas en la legislación vigente
K0616	Conocimiento de vigilancia continua y sus procesos, y actividades del programa de diagnóstico y mitigación continuos (CDM, por sus siglas en inglés)
K0617	Conocimiento de evaluaciones automatizadas del control de la seguridad

Id. de los CHC	Descripción
K0618	Conocimiento de gestión de recursos de hardware y el valor del seguimiento de la ubicación y configuración de dispositivos y software en red en todos los departamentos, ubicaciones e instalaciones, y potencialmente, funciones de negocios compatibles
K0619	Conocimiento de gestión de recursos de software y el valor del seguimiento de la ubicación y configuración de dispositivos y software en red, en todos los departamentos, ubicaciones e instalaciones, y potencialmente, funciones de negocios compatibles
K0620	Conocimiento de tecnologías y herramientas de vigilancia continua
K0621	Conocimiento de calificación de riesgos
K0622	Conocimiento de controles relacionados con el uso, procesamiento, almacenamiento y transmisión de datos
K0623	Conocimiento de metodologías de evaluación de riesgos
K0624	Conocimiento de riesgos a la seguridad de las aplicaciones (por ejemplo, lista de los diez riesgos más altos del Proyecto abierto de seguridad de aplicaciones web)
K0625	Conocimiento de que no es práctico hacer aplicación de parches y actualizaciones de software para algunos dispositivos en red
K0626	Conocimiento de mecanismos seguros de actualización
K0627	Conocimiento de la importancia del filtrado de entrada para proteger contra amenazas automatizadas que dependen de direcciones de red con identidad suplantada
K0628	Conocimiento de competencias cibernéticas como una forma para desarrollar habilidades por medio de experiencias prácticas en situaciones simuladas del mundo real
K0629	Conocimiento de listas blancas y negras
K0630	Conocimiento de las técnicas y métodos de intrusión más recientes y de las intrusiones documentadas externas a la organización

A.6 Descripciones de las habilidades del Marco de la NICE

La Tabla 6 proporciona una lista de las habilidades necesarias en el ámbito de la ciberseguridad. Una habilidad es la competencia observable para desempeñar un acto psicomotor aprendido. En la Lista detallada de funciones laborales del Apéndice B, se incluyen las descripciones de las habilidades seleccionadas de esta lista para cada función laboral. Esta lista se actualizará periódicamente [1]. Véase la fuente definitiva de la versión más reciente de este material en la Hoja de cálculo de referencia para la Publicación especial 800-181 del NIST [4].

Tabla 6: Descripciones de las habilidades del Marco de la NICE

Id. de la habilidad	Descripción
S0001	Habilidad para llevar a cabo detecciones de vulnerabilidades y reconocer vulnerabilidades en los sistemas de seguridad
S0002	Habilidad para asignar capacidad de almacenamiento en el diseño de sistemas de gestión de datos
S0003	Habilidad para identificar, capturar, contener y generar informes del malware
S0004	Habilidad para analizar la capacidad de tráfico de la red y las características de rendimiento
S0005	Habilidad para aplicar e incorporar tecnologías de la información en las soluciones propuestas
S0006	Habilidad para aplicar principios de confidencialidad, integridad y disponibilidad
S0007	Habilidad para aplicar controles de acceso a redes o hosts (por ejemplo, lista de control de acceso)
S0008	Habilidad para aplicar principios y técnicas de análisis de los sistemas específicos de la organización
S0009	Habilidad para evaluar la solidez de sistemas y diseños de seguridad
S0010	Habilidad para llevar a cabo análisis de capacidades y requisitos
S0011	Habilidad para llevar a cabo búsquedas de información
S0012	Habilidad para llevar a cabo la asignación de conocimientos (por ejemplo, asignación de repositorios de conocimientos)
S0013	Habilidad para llevar a cabo consultas y diseñar algoritmos a fin de analizar estructuras de datos
S0014	Habilidad para depurar software
S0015	Habilidad para llevar a cabo eventos de prueba
S0016	Habilidad para configurar y optimizar software
S0017	Habilidad para diseñar y usar modelos matemáticos o estadísticos
S0018	Habilidad para formular políticas que reflejen los objetivos de seguridad del sistema
S0019	Habilidad para diseñar programas que validen y procesen entradas múltiples, incluidos argumentos de línea de comandos, variables ambientales y secuencias de entrada
S0020	Habilidad para diseñar e implementar firmas
S0021	Habilidad para diseñar una estructura de análisis de datos (es decir, los tipos de datos que debe generar una prueba y la manera de analizar esos datos)
S0022	Habilidad para diseñar contramedidas para los riesgos de seguridad identificados
S0023	Habilidad para diseñar controles de seguridad en función de los principios y las normas fundamentales de ciberseguridad
S0024	Habilidad para diseñar la integración de soluciones de hardware y software

Id. de la habilidad	Descripción
S0025	Habilidad para detectar intrusiones basadas en hosts y redes mediante tecnologías de detección de intrusiones (por ejemplo, Snort)
S0026	Habilidad para determinar un nivel apropiado de rigurosidad de prueba para un sistema dado
S0027	Habilidad para determinar la manera en que debe funcionar un sistema de seguridad (incluidas sus capacidades de resiliencia y confiabilidad) y los efectos que los cambios en las condiciones, las operaciones o el entorno tendrán en estos resultados
S0028	Habilidad para elaborar diccionarios de datos
S0029	Habilidad para diseñar modelos de datos
S0030	Habilidad para diseñar casos hipotéticos de pruebas basados en operaciones
S0031	Habilidad para diseñar y aplicar controles de acceso al sistema de seguridad
S0032	Habilidad para formular, poner a prueba e implementar planes de contingencia y recuperación de infraestructuras de redes
S0033	Habilidad para diagnosticar problemas de conectividad
S0034	Habilidad para discernir las necesidades de protección (es decir, controles de seguridad) de los sistemas y las redes de información
S0035	Habilidad para establecer un esquema de enrutamiento
S0036	Habilidad para evaluar la idoneidad de los diseños de seguridad
S0037	Habilidad para generar consultas e informes
S0038	Habilidad para identificar medidas o indicadores de rendimiento de sistemas y las acciones necesarias para mejorar o corregir el rendimiento, en relación con las metas del sistema
S0039	Habilidad para identificar las posibles causas de degradación del rendimiento o la disponibilidad de los sistemas e iniciar las acciones necesarias para mitigar esta degradación
S0040	Habilidad para implementar, mantener y mejorar las prácticas establecidas de seguridad de las redes
S0041	Habilidad para instalar, configurar y solucionar problemas de los componentes de la LAN y la WAN, como enrutadores, concentradores y conmutadores
S0042	Habilidad para mantener bases de datos (es decir, hacer copias de seguridad, restaurar, eliminar datos, archivos de registros de transacciones, etc.)
S0043	Habilidad para mantener servicios de directorio (por ejemplo, Microsoft Active Directory, LDAP, etc.)
S0044	Habilidad para imitar los comportamientos de amenazas
S0045	Habilidad para optimizar el rendimiento de las bases de datos
S0046	Habilidad para hacer análisis a nivel de paquetes usando herramientas apropiadas (por ejemplo, Wireshark, tcpdump)
S0047	Habilidad para conservar la integridad de pruebas de acuerdo con los procedimientos operativos estándar o las normas nacionales
S0048	Habilidad para poner a prueba la integración de sistemas
S0049	Habilidad para medir el capital intelectual y generar informes de este
S0050	Habilidad para el modelado de diseños y la creación de casos de uso (por ejemplo, lenguaje unificado de modelado)
S0051	Habilidad para usar herramientas y técnicas de pruebas de penetración
S0052	Habilidad para usar técnicas de ingeniería social (por ejemplo, *phishing*, *baiting*, *tailgating*, etc.)
S0053	Habilidad para ajustar sensores

Id. de la habilidad	Descripción
S0054	Habilidad para usar metodologías de manejo de incidentes
S0055	Habilidad para usar tecnologías de gestión del conocimiento
S0056	Habilidad para usar las herramientas de gestión de redes para analizar tendencias del tráfico de redes (por ejemplo, protocolo simple de gestión de redes)
S0057	Habilidad para usar analizadores de protocolos
S0058	Habilidad para usar herramientas apropiadas para reparar software, hardware y equipos periféricos de un sistema
S0059	Habilidad para usar dispositivos y cifrado de red privada virtual (VPN)
S0060	Habilidad para escribir código en un lenguaje de programación que sea compatible actualmente (por ejemplo, Java, C++)
S0061	Habilidad para redactar planes de prueba
S0062	Habilidad para analizar volcados de memoria con objeto de extraer información
S0063	Habilidad para recolectar datos de una variedad de recursos de ciberdefensa
S0064	Habilidad para diseñar e implementar programas y planes de estudio de capacitación técnica
S0065	Habilidad para identificar y extraer datos de interés forense de diversos medios (es decir, análisis forense de medios)
S0066	Habilidad para identificar deficiencias en las capacidades técnicas
S0067	Habilidad para identificar, modificar y manipular los componentes del sistema aplicables dentro de Windows, Unix o Linux (por ejemplo, contraseñas, cuentas de usuario, archivos)
S0068	Habilidad para recolectar, procesar, empaquetar, transportar y almacenar pruebas electrónicas a fin de evitar la modificación, pérdida, daño físico o destrucción de datos
S0069	Habilidad para configurar una estación de trabajo forense
S0070	Habilidad para hablar con otras personas y transmitir información con efectividad
S0071	Habilidad para usar conjuntos de herramientas forenses (por ejemplo, EnCase, Sleuthkit, FTK)
S0072	Habilidad para emplear normas y métodos científicos para resolver problemas
S0073	Habilidad para usar máquinas virtuales (por ejemplo, Microsoft Hyper-V, VMware vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.)
S0074	Habilidad para desmontar físicamente computadoras personales
S0075	Habilidad para llevar a cabo análisis forenses en entornos de sistemas operativos múltiples (por ejemplo, sistemas de dispositivos móviles)
S0076	Habilidad para configurar y utilizar herramientas de protección informática basadas en software (por ejemplo, firewalls de software, software de antivirus, antispyware)
S0077	Habilidad para proteger las comunicaciones de redes
S0078	Habilidad para reconocer y categorizar tipos de vulnerabilidades y los ataques asociados con estas
S0079	Habilidad para proteger una red contra malware. (por ejemplo, sistemas de detección de intrusiones en redes [NIPS, por sus siglas en inglés], antimalware, dispositivos externos de restricción y prevención, filtros de correo no deseado)
S0080	Habilidad para efectuar evaluaciones de daños
S0081	Habilidad para usar las herramientas de análisis de redes con objeto de identificar vulnerabilidades (por ejemplo, pruebas de vulnerabilidad ante datos aleatorios o inesperados [*fuzzing*], nmap, etc.)
S0082	Habilidad para evaluar planes de prueba con el fin de determinar su aplicabilidad e integridad

Id. de la habilidad	Descripción
S0083	Habilidad para integrar herramientas de prueba de seguridad de caja negra en el proceso de control de calidad de las versiones de software
S0084	Habilidad para configurar y usar componentes de protección de redes (por ejemplo, firewalls, VPN, sistemas de detección de intrusiones en redes)
S0085	Habilidad para llevar a cabo auditorías o revisiones de sistemas técnicos
S0086	Habilidad para evaluar la confiabilidad del proveedor o el producto
S0087	Habilidad para analizar a fondo códigos malintencionados capturados (por ejemplo, análisis forense de malware)
S0088	Habilidad para usar herramientas de análisis binario (por ejemplo, Hexedit, código de comando xxd, hexdump)
S0089	Habilidad para las funciones hash unidireccionales (por ejemplo, algoritmo de hash seguro [SHA, por sus siglas en inglés], algoritmo de resumen de mensaje [MD5, por sus siglas en inglés])
S0090	Habilidad para analizar código anómalo y determinar si es malintencionado o benigno
S0091	Habilidad para analizar datos volátiles
S0092	Habilidad para identificar técnicas de ofuscación
S0093	Habilidad para interpretar los resultados del depurador con objeto de determinar tácticas, técnicas y procedimientos
S0094	Habilidad para leer datos hexadecimales
S0095	Habilidad para identificar técnicas de codificación comunes (por ejemplo, disyunción exclusiva [XOR], Código estándar estadounidense para el intercambio de información [ASCII, por sus siglas en inglés], Unicode, Base64, Uuencode, código de localizador uniforme de recursos [URL, por sus siglas en inglés])
S0096	Habilidad para leer e interpretar firmas (por ejemplo, Snort)
S0097	Habilidad para aplicar controles de seguridad
S0100	Habilidad para organizar o usar actividades de aprendizaje (por ejemplo, casos hipotéticos, juegos instructivos, ejercicios interactivos)
S0101	Habilidad para usar tecnologías (por ejemplo, SmartBoards, sitios web, computadoras, proyectores) con fines educativos
S0102	Habilidad para aplicar capacidades de entrega técnica
S0103	Habilidad para evaluar el poder predictivo de un modelo y su capacidad posterior para generalizar
S0104	Habilidad para llevar a cabo revisiones de preparación para pruebas
S0106	Habilidad para el proceso preliminar de datos (por ejemplo, imputación, reducción de dimensiones, normalización, transformación, extracción, filtrado, atenuación)
S0107	Habilidad para diseñar y documentar estrategias generales de prueba y evaluación de programas
S0108	Habilidad para establecer estándares de cualificación de personal y puestos
S0109	Habilidad para identificar tendencias o relaciones ocultas
S0110	Habilidad para identificar requisitos de la infraestructura de prueba y evaluación (personas, intervalos, herramientas, instrumentación)
S0111	Habilidad para interactuar con los clientes
S0112	Habilidad para gestionar activos de prueba, recursos de prueba y personal de prueba con objeto de lograr la conclusión efectiva de los eventos de prueba
S0113	Habilidad para hacer las conversiones de formatos y crear una representación estándar de los datos
S0114	Habilidad para efectuar análisis de confidencialidad

Id. de la habilidad	Descripción
S0115	Habilidad para preparar informes de prueba y evaluación
S0116	Habilidad para diseñar soluciones de varios niveles de seguridad y entre dominios
S0117	Habilidad para proporcionar cálculos de recursos de prueba y evaluación
S0118	Habilidad para diseñar ontologías semánticas que puedan ser interpretadas por máquinas
S0119	Habilidad para el análisis de regresión (por ejemplo, jerárquica escalonada, modelo lineal generalizada, mínimos cuadrados ordinarios, métodos basados en árboles, logística)
S0120	Habilidad para revisar registros a fin de identificar indicios de intrusiones anteriores
S0121	Habilidad para técnicas de endurecimiento de sistemas, redes y sistemas operativos (por ejemplo, eliminar servicios innecesarios, políticas de contraseñas, segmentación de red, registros de habilitación, privilegio mínimo, etc.)
S0122	Habilidad para usar métodos de diseño
S0123	Habilidad para el análisis de transformación (por ejemplo, agregación, enriquecimiento, procesamiento)
S0124	Habilidad para solucionar problemas, diagnosticar anomalías en la infraestructura de ciberdefensa y llevar a cabo la solución
S0125	Habilidad para usar estadísticas y técnicas descriptivas básicas (por ejemplo, normalidad, distribución de modelos, diagramas de dispersión)
S0126	Habilidad para usar herramientas de análisis de datos (por ejemplo, Excel, STATA, SAS, SPSS)
S0127	Habilidad para usar herramientas de asignación de datos
S0128	Habilidad para emplear personal y sistemas de TI para el personal
S0129	Habilidad para usar técnicas de identificación y eliminación de valores atípicos
S0130	Habilidad para escribir secuencias de comandos utilizando R, Python, PIG, HIVE, SQL, etc.
S0131	Habilidad para analizar malware
S0132	Habilidad para llevar a cabo análisis del nivel de bits
S0133	Habilidad para procesar pruebas digitales, que incluya la protección y obtención de copias de pruebas sólidas con validez legal
S0134	Habilidad para llevar a cabo revisiones de sistemas
S0135	Habilidad para diseñar planes de prueba seguros (por ejemplo, unidad, integración, sistema, aceptación)
S0136	Habilidad para manejar principios, modelos, métodos (por ejemplo, vigilancia del rendimiento de sistemas de extremo a extremo) y herramientas de gestión de sistemas de redes
S0137	Habilidad para llevar a cabo evaluaciones de vulnerabilidades de las aplicaciones
S0138	Habilidad para usar las capacidades de cifrado y firma digital de la infraestructura de clave pública (PKI) en aplicaciones (por ejemplo, extensiones seguras multipropósito al correo de internet [S/MIME, por sus siglas en inglés], tráfico de SSL)
S0139	Habilidad para aplicar modelos de seguridad (por ejemplo, modelo Bell-LaPadula, modelo de integridad Biba, modelo de integridad Clark-Wilson)
S0140	Habilidad para aplicar el proceso de ingeniería de sistemas
S0141	Habilidad para evaluar diseños de sistemas de seguridad
S0142	Habilidad para investigar en busca de soluciones a problemas nuevos de clientes
S0143	Habilidad para llevar a cabo la planificación, gestión y mantenimiento de sistemas y servidores
S0144	Habilidad para corregir problemas físicos y técnicos que afectan el rendimiento de sistemas y servidores

Id. de la habilidad	Descripción
S0145	Habilidad para integrar y aplicar políticas que cumplan los objetivos de seguridad del sistema
S0146	Habilidad para crear políticas que faciliten a los sistemas lograr los objetivos de rendimiento (por ejemplo, enrutamiento de tráfico, acuerdos de nivel de servicio [SLA], especificaciones de la unidad central de procesamiento [CPU])
S0147	Habilidad para evaluar controles de seguridad en función de los principios y las normas fundamentales de ciberseguridad (por ejemplo, controles de seguridad críticos del Centro para la seguridad de internet [CIS CSC, por sus siglas en inglés], Publicación especial 800-53 del NIST, Marco de ciberseguridad, etc.)
S0148	Habilidad para diseñar la integración de procesos y soluciones tecnológicas, incluidos sistemas heredados y lenguajes de programación modernos
S0149	Habilidad para desarrollar aplicaciones que pueden registrar y manejar errores, excepciones y errores y registros de aplicaciones
S0150	Habilidad para implementar y poner a prueba planes de contingencia y recuperación para infraestructuras de redes
S0151	Habilidad para solucionar problemas de componentes erróneos del sistema (es decir, servidores)
S0152	Habilidad para convertir requisitos operativos en necesidades de protección (es decir, controles de seguridad)
S0153	Habilidad para identificar y prever problemas de rendimiento, disponibilidad, capacidad o configuración del sistema o servidor
S0154	Habilidad para instalar actualizaciones de sistemas y componentes (es decir, servidores, dispositivos, dispositivos de redes)
S0155	Habilidad para vigilar y optimizar el rendimiento de sistemas o servidores
S0156	Habilidad para efectuar análisis a nivel de paquete
S0157	Habilidad para recuperar sistemas o servidores con errores (por ejemplo, software de recuperación, clústeres de conmutación por error, replicación, etc.)
S0158	Habilidad para administrar sistemas operativos (por ejemplo, mantenimiento de cuentas, copias de seguridad de datos, mantenimiento del rendimiento de sistemas, instalación y configuración de hardware y software nuevos)
S0159	Habilidad para configurar y validar estaciones de trabajo y componentes periféricos de red de acuerdo con especificaciones o estándares aprobados
S0160	Habilidad para usar modelado de diseño (por ejemplo, lenguaje unificado de modelado)
S0161	Retirado: se integró en S0160.
S0162	Habilidad para trabajar con subredes
S0163	Retirado: se integró en S0060.
S0164	Habilidad para evaluar la aplicación de estándares criptográficos
S0166	Habilidad para identificar deficiencias en las capacidades de entrega técnica
S0167	Habilidad para reconocer vulnerabilidades en sistemas de seguridad (por ejemplo, análisis de vulnerabilidades y cumplimiento)
S0168	Habilidad para configurar las subredes físicas o lógicas que separan una red de área local (LAN) interna de otras redes que no son de confianza
S0169	Habilidad para llevar a cabo análisis de tendencias
S0170	Habilidad para configurar y utilizar componentes de protección informática (por ejemplo, firewalls de hardware, servidores, enrutadores, según corresponda)
S0171	Habilidad para efectuar evaluaciones de impactos o riesgos
S0172	Habilidad para aplicar técnicas de codificación seguras
S0173	Habilidad para usar herramientas de correlación de eventos de seguridad

Id. de la habilidad	Descripción
S0174	Habilidad para usar herramientas de análisis de código
S0175	Habilidad para hacer análisis de las causas principales
S0176	Habilidad para llevar a cabo actividades de planificación administrativa, que incluyan preparación de planes de soporte funcionales y específicos, preparación y gestión de correspondencia y procedimientos para la dotación de personal
S0177	Habilidad para analizar las redes de comunicación de un objetivo
S0178	Habilidad para analizar datos esenciales de redes (por ejemplo, archivos de configuración de enrutadores, protocolos de enrutamiento)
S0179	Habilidad para analizar herramientas de procesamiento de lenguaje que proporcionen retroalimentación a fin de mejorar el desarrollo de herramientas
S0180	Retirado: se integró en S0062.
S0181	Habilidad para analizar datos de recolección de punto medio
S0182	Habilidad para analizar datos internos y externos de comunicaciones de objetivos recolectadas de redes de área local (LAN) inalámbricas
S0183	Habilidad para analizar datos de recolección de terminales o entornos
S0184	Habilidad para analizar el tráfico a fin de identificar dispositivos de redes
S0185	Habilidad para aplicar métodos analíticos que se emplean normalmente para ayudar a la planificación y justificar las estrategias y planes de acción recomendados
S0186	Habilidad para aplicar procedimientos de planificación en casos de crisis
S0187	Habilidad para aplicar diversos métodos, herramientas y técnicas analíticos (por ejemplo, hipótesis paralelas; cadena de razonamiento; métodos de casos hipotéticos; detección de negación y engaño; alto impacto-baja probabilidad; análisis de redes, asociaciones o vínculos; análisis bayesiano, método Delphi y análisis de tendencias)
S0188	Habilidad para evaluar el marco de referencia de un objetivo (por ejemplo, motivación, capacidad técnica, estructura organizativa, confidencialidad)
S0189	Habilidad para evaluar o calcular los efectos generados durante y después de las ciberoperaciones
S0190	Habilidad para evaluar las herramientas actuales a fin de identificar los mejoramientos necesarios
S0191	Habilidad para evaluar la aplicabilidad de las herramientas analíticas disponibles para diversas situaciones
S0192	Habilidad para efectuar auditorías de firewalls, perímetros, enrutadores y sistemas de detección de intrusiones
S0193	Habilidad para cumplir con las restricciones legales de la información seleccionada como objetivo
S0194	Habilidad para llevar a cabo investigaciones no atribuibles
S0195	Habilidad para llevar a cabo investigaciones utilizando todas las fuentes disponibles
S0196	Habilidad para llevar a cabo investigaciones utilizando la red profunda
S0197	Habilidad para llevar a cabo análisis de redes sociales, análisis de listas de amigos o análisis de cookies
S0198	Habilidad para llevar a cabo análisis de redes sociales
S0199	Habilidad para crear y extraer información importante de capturas de paquetes
S0200	Habilidad para establecer requisitos de recolección compatibles con las actividades de adquisición de datos
S0201	Habilidad para crear planes de ayuda de operaciones remotas (es decir, sitios calientes, templados, fríos, alternativos; recuperación ante desastres)
S0202	Habilidad para técnicas de extracción de datos (por ejemplo, búsqueda de sistemas de archivos) y análisis

Id. de la habilidad	Descripción
S0203	Habilidad para definir y caracterizar todos los aspectos pertinentes del entorno operativo
S0204	Habilidad para representar datos de origen o colaterales en un mapa de redes
S0205	Habilidad para determinar las opciones de selección de objetivos apropiadas mediante la evaluación de las capacidades disponibles con respecto a los efectos deseados
S0206	Habilidad para determinar los parches instalados en diversos sistemas operativos e identificar las firmas de los parches
S0207	Habilidad para determinar el efecto de diversas configuraciones de enrutadores y firewalls en las tendencias de tráfico y en el rendimiento de la red en entornos de LAN y WAN
S0208	Habilidad para determinar la ubicación física de dispositivos de redes
S0209	Habilidad para establecer y ejecutar programas de evaluación integral de ciberoperaciones para evaluar y validar las características de rendimiento operativo
S0210	Habilidad para preparar informes de inteligencia
S0211	Habilidad para formular o recomendar métodos analíticos o soluciones a problemas y situaciones para los que no existe información completa o ningún precedente
S0212	Habilidad para difundir de manera oportuna los datos con mayor valor de inteligencia
S0213	Habilidad para documentar y comunicar información técnica y programática compleja
S0214	Habilidad para evaluar accesos en busca de valor de inteligencia
S0215	Habilidad para evaluar e interpretar metadatos
S0216	Habilidad para evaluar las capacidades disponibles con respecto a los efectos deseados con objeto de proporcionar planes de acción efectivos
S0217	Habilidad para evaluar fuentes de datos y determinar su pertinencia, confiabilidad y objetividad
S0218	Habilidad para evaluar información y determinar su confiabilidad, validez y pertinencia
S0219	Habilidad para evaluar información y reconocer su pertinencia, prioridad, etc.
S0220	Habilidad para explotar o consultar bases de datos de recolección de organizaciones o de socios
S0221	Habilidad para extraer información de capturas de paquetes
S0222	Habilidad para análisis de fusiones
S0223	Habilidad para generar planes de operación compatibles con los requisitos de las misiones y los objetivos
S0224	Habilidad para captar lo esencial de las comunicaciones de los objetivos
S0225	Habilidad para identificar las redes de comunicaciones de un objetivo
S0226	Habilidad para identificar las características de las redes de un objetivo
S0227	Habilidad para identificar interpretaciones analíticas alternativas a fin de minimizar resultados imprevistos
S0228	Habilidad para identificar elementos críticos de objetivos, incluidos elementos críticos de objetivos del dominio cibernético
S0229	Habilidad para identificar amenazas cibernéticas que puedan poner en peligro los intereses de las organizaciones o los socios
S0230	Retirado: se integró en S0066.
S0231	Habilidad para identificar la manera en que se comunica un objetivo
S0232	Habilidad para identificar deficiencias y limitaciones de inteligencia
S0233	Habilidad para identificar problemas de idioma que puedan afectar los objetivos de la organización
S0234	Habilidad para identificar personas que puedan encargarse del establecimiento de objetivos

Id. de la habilidad	Descripción
S0235	Habilidad para identificar idiomas y dialectos regionales que no sean de los objetivos
S0236	Habilidad para identificar los dispositivos que funcionan en cada nivel de modelos de protocolos
S0237	Habilidad para identificar, localizar y dar seguimiento a objetivos por medio de técnicas de análisis geoespacial
S0238	Habilidad para priorizar información relacionada con operaciones
S0239	Habilidad para interpretar lenguajes de programación compilados e interpretativos
S0240	Habilidad para interpretar metadatos y contenido de la manera en que los sistemas de recolección los aplican
S0241	Habilidad para interpretar los resultados de ruta de seguimiento de la manera en que se aplican al análisis y la reconstrucción de redes
S0242	Habilidad para interpretar los resultados de la detección de vulnerabilidades para identificar vulnerabilidades
S0243	Habilidad para la gestión del conocimiento, incluidas las técnicas de documentación técnica (por ejemplo, página wiki)
S0244	Habilidad para gestionar las relaciones con los clientes, que incluya determinación de necesidades o requisitos de los clientes, gestión de expectativas de los clientes y demostración de compromiso de lograr resultados de calidad
S0245	Habilidad para navegar por el software de visualización de redes
S0246	Habilidad para la normalización de números
S0247	Habilidad para fusionar datos provenientes de información de inteligencia existente para permitir la recolección nueva y continua
S0248	Habilidad para efectuar análisis de sistemas de objetivos
S0249	Habilidad para preparar y presentar sesiones informativas
S0250	Habilidad para preparar planes y su correspondencia
S0251	Habilidad para priorizar el material en el idioma del objetivo
S0252	Habilidad para procesar datos recolectados para el análisis de seguimiento
S0253	Habilidad para proporcionar análisis sobre asuntos relacionados con el objetivo (por ejemplo, idioma, cultura, comunicaciones)
S0254	Habilidad para proporcionar análisis a fin de ayudar a redactar informes progresivos posteriores a una acción
S0255	Habilidad para proporcionar información procesable de geolocalización en tiempo real utilizando las infraestructuras de objetivos
S0256	Habilidad para proporcionar conocimientos de sistemas de objetivos o de amenazas por medio de la identificación y el análisis de vínculos de relaciones físicas, funcionales o conductuales
S0257	Habilidad para leer, interpretar, escribir, modificar y ejecutar secuencias de comandos simples (por ejemplo, Perl, VBS) en sistemas Windows y Unix (por ejemplo, los que ejecutan tareas como análisis de archivos de datos extensos, automatización de tareas manuales y obtención o procesamiento de datos remotos)
S0258	Habilidad para reconocer e interpretar actividad malintencionada de red en el tráfico
S0259	Habilidad para reconocer técnicas de negación y engaño del objetivo
S0260	Habilidad para reconocer oportunidades de punto medio e información esencial
S0261	Habilidad para reconocer la pertinencia de la información
S0262	Habilidad para reconocer cambios importantes en las tendencias de comunicación de los objetivos
S0263	Habilidad para reconocer la información técnica que pueda ser usada como pistas en el análisis de metadatos

Id. de la habilidad	Descripción
S0264	Habilidad para reconocer la información técnica que pueda ser usada como pistas para habilitar operaciones remotas (los datos incluyen usuarios, contraseñas, direcciones de correo electrónico, intervalos de IP del objetivo, frecuencia en el comportamiento de la información de inteligencia de red digital [DNI, por sus siglas en inglés], servidores de correo, servidores de dominio, información de encabezado de SMTP)
S0265	Habilidad para reconocer la información técnica que pueda ser usada para el establecimiento de objetivos, incluida la preparación de inteligencia
S0266	Habilidad para los lenguajes de programación pertinentes (por ejemplo, C++, Python, etc.)
S0267	Habilidad para usar las herramientas de línea de comandos remotos y la interfaz gráfica de usuario (GUI, por sus siglas en inglés)
S0268	Habilidad para investigar información esencial
S0269	Habilidad para investigar las vulnerabilidades y los ataques de vulnerabilidades de seguridad que se usan en el tráfico
S0270	Habilidad para la ingeniería inversa (por ejemplo, edición hexadecimal, utilidades de paquetes binarios, depuración y análisis de cadenas) a fin de identificar funciones y propietarios de herramientas remotas
S0271	Habilidad para revisar y editar productos de evaluación
S0272	Habilidad para revisar y editar productos de inteligencia de diversas fuentes para las ciberoperaciones
S0273	Habilidad para revisar y editar planes
S0274	Habilidad para revisar y editar materiales de objetivos
S0275	Habilidad para administrar servidores
S0276	Habilidad para evaluar, recolectar y analizar metadatos de LAN inalámbricas
S0277	Habilidad para sintetizar, analizar y priorizar el significado en todos los conjuntos de datos
S0278	Habilidad para adaptar el análisis a los niveles necesarios (por ejemplo, de clasificación y organizativos)
S0279	Habilidad para establecer objetivos que ayuden directamente a las operaciones de recolección
S0280	Habilidad para identificar anomalías en las redes de objetivos (por ejemplo, intrusiones, flujo o procesamiento de datos, implementación del objetivo de nuevas tecnologías)
S0281	Habilidad para la escritura técnica
S0282	Habilidad para poner a prueba y evaluar herramientas para su implementación
S0283	Habilidad para transcribir comunicaciones en el idioma del objetivo
S0284	Habilidad para traducir materiales gráficos o de voz en el idioma del objetivo
S0285	Habilidad para usar operadores booleanos con objeto de construir consultas simples y complejas
S0286	Habilidad para usar bases de datos a fin de identificar información pertinente de objetivos
S0287	Habilidad para usar datos geoespaciales y aplicar recursos geoespaciales
S0288	Habilidad para usar varias herramientas analíticas, bases de datos y técnicas (por ejemplo, Analyst's Notebook, A-Space, Anchory, M3, pensamiento divergente y convergente, gráficos de vínculos, matrices, etc.)
S0289	Habilidad para usar varios motores de búsqueda (por ejemplo, Google, Yahoo, LexisNexis, DataStar) y herramientas al llevar a cabo búsquedas de código abierto
S0290	Habilidad para usar redes no atribuibles
S0291	Habilidad para usar métodos de investigación que incluyan varias fuentes distintas para reconstruir la red de un objetivo

Id. de la habilidad	Descripción
S0292	Habilidad para usar bases de datos y paquetes de software de selección de objetivos
S0293	Habilidad para usar herramientas, técnicas y procedimientos para explotar y establecer persistencia en un objetivo de forma remota
S0294	Habilidad para usar herramientas de ruta de seguimiento e interpretar los resultados de la manera en que se aplican al análisis y reconstrucción de redes
S0295	Habilidad para usar diversas herramientas de recolección de datos de código abierto (comercio en línea, DNS, correo, etc.)
S0296	Habilidad para usar retroalimentación a fin de mejorar procesos, productos y servicios
S0297	Habilidad para usar espacios de trabajo o herramientas de colaboración virtual (por ejemplo, espacios de trabajo interactivos [IWS, por sus siglas en inglés], videoconferencias [VTC, por sus siglas en inglés], salas de chat, SharePoint)
S0298	Habilidad para verificar la integridad de todos los archivos (por ejemplo, sumas de comprobación, disyunción exclusiva, hash seguro, restricciones de comprobación, etc.)
S0299	Habilidad para el análisis, creación de plantillas y geolocalización de objetivos de red inalámbrica
S0300	Habilidad para escribir (y presentar) requisitos que solucionen las deficiencias de capacidades técnicas
S0301	Habilidad para escribir sobre hechos e ideas de manera clara, convincente y organizada
S0302	Habilidad para escribir informes sobre efectividad
S0303	Habilidad para escribir, revisar y editar productos de inteligencia y evaluación de varias fuentes relacionados con la cibernética
S0304	Habilidad para acceder a información sobre los recursos actuales disponibles y su uso
S0305	Habilidad para acceder a bases de datos donde se mantienen los planes, directivas u orientación
S0306	Habilidad para analizar orientación estratégica para problemas que exigen aclaración u orientación adicional
S0307	Habilidad para analizar las fuentes de fortaleza y seguridad en el éxito de objetivos o amenazas
S0308	Habilidad para prever los requisitos de empleo de la capacidad de inteligencia
S0309	Habilidad para prever actividades clave de objetivos o amenazas que probablemente den lugar a una decisión de la dirección
S0310	Habilidad para aplicar normas analíticas en la evaluación de productos de inteligencia
S0311	Habilidad para emplear las capacidades, limitaciones y metodologías de asignación de tareas de las plataformas, sensores, arquitecturas y aparatos disponibles que se aplican a los objetivos de la organización
S0312	Habilidad para aplicar el proceso utilizado para evaluar el rendimiento y el impacto de las ciberoperaciones
S0313	Habilidad para expresar una declaración o requisito de necesidades y para integrar capacidades, accesos o procesos de recolección nuevos y emergentes en las operaciones de recolección
S0314	Habilidad para expresar las capacidades de inteligencia disponibles que ayudan a la ejecución del plan
S0315	Habilidad para expresar las necesidades del conjunto de planificadores a analistas de todas las fuentes
S0316	Habilidad para asociar las deficiencias de inteligencia a los requisitos prioritarios de información y las propiedades observables
S0317	Habilidad para comparar indicadores y propiedades observables con los requisitos

Id. de la habilidad	Descripción
S0318	Habilidad para conceptualizar la totalidad del proceso de inteligencia en dominios y dimensiones múltiples
S0319	Habilidad para convertir los requisitos de inteligencia en tareas de producción de inteligencia
S0320	Habilidad para coordinar la elaboración de productos de inteligencia a la medida
S0321	Habilidad para correlacionar las prioridades de inteligencia con la asignación de recursos y activos de inteligencia
S0322	Habilidad para formular indicadores de progreso o éxito operativo
S0323	Habilidad para crear y mantener al día los documentos de planificación y el seguimiento de servicios y producción
S0324	Habilidad para determinar la factibilidad de la recolección
S0325	Habilidad para formular un plan de recolección que muestre claramente la disciplina que se puede usar para recolectar la información necesaria
S0326	Habilidad para distinguir entre recursos nocionales y reales y su aplicabilidad al plan en desarrollo
S0327	Habilidad para procurar que la estrategia de recolección haga uso de todos los recursos disponibles
S0328	Habilidad para evaluar factores del entorno operativo relacionados con los objetivos y los requisitos de información
S0329	Habilidad para evaluar solicitudes de información a fin de determinar si existe información de respuesta
S0330	Habilidad para evaluar las capacidades, limitaciones y metodologías de asignación de tareas de las funcionalidades de recolección del organismo, teatro de operaciones, país, coalición y otras
S0331	Habilidad para expresar verbalmente y por escrito la relación entre las limitaciones de la capacidad de inteligencia y los riesgos y efectos de la toma de decisiones en toda la operación
S0332	Habilidad para extraer información de las herramientas y aplicaciones disponibles asociadas con los requisitos de recolección y la gestión de operaciones de recolección
S0333	Habilidad para representar gráficamente materiales de ayuda para la toma de decisiones que contengan cálculos de la capacidad de inteligencia y de los socios
S0334	Habilidad para identificar y aplicar la asignación de tareas, recolección, procesamiento, explotación y difusión a las disciplinas de recolección afines
S0335	Habilidad para identificar deficiencias de inteligencia
S0336	Habilidad para identificar el momento en que se satisfacen los requisitos de información prioritarios
S0337	Habilidad para implementar los procedimientos establecidos para evaluar las actividades de gestión y operaciones de recolección
S0338	Habilidad para interpretar la orientación de planificación a fin de discernir el nivel de ayuda analítica necesaria
S0339	Habilidad para interpretar informes de preparación, su pertinencia operativa y el impacto de la recolección de inteligencia
S0340	Habilidad para vigilar la situación de objetivos o amenazas y los factores del entorno
S0341	Habilidad para vigilar los efectos de la amenaza en las capacidades de los socios y mantener una estimación continua
S0342	Habilidad para optimizar el rendimiento del sistema de recolección por medio de ajustes, pruebas y reajustes repetidos

Id. de la habilidad	Descripción
S0343	Habilidad para organizar equipos de planificación de inteligencia, coordinar la ayuda de recolección y producción, y vigilar el estado
S0344	Habilidad para preparar y entregar informes, presentaciones y sesiones informativas, incluido el uso de ayudas visuales o tecnología para presentaciones
S0345	Habilidad para relacionar recursos y activos de inteligencia con los requisitos de inteligencia previstos
S0346	Habilidad para resolver los requisitos de recolección conflictivos
S0347	Habilidad para revisar especificaciones de rendimiento e información histórica acerca de los recursos de recolección
S0348	Habilidad para especificar las recolecciones o las asignaciones de tareas que se deben hacer a corto plazo
S0349	Habilidad para sincronizar los procedimientos de evaluación operativa con el proceso de requisitos de información críticos
S0350	Habilidad para sincronizar las actividades de planificación y la ayuda de inteligencia necesaria
S0351	Habilidad para convertir las capacidades, limitaciones y metodologías de asignación de tareas de la funcionalidades de recolección del organismo, teatro de operaciones, país, coalición y otras
S0352	Habilidad para usar herramientas y entornos de colaboración para las operaciones de recolección
S0353	Habilidad para usar sistemas o herramientas a fin de dar seguimiento a los requisitos de recolección y determinar si se han satisfecho
S0354	Habilidad para formular políticas que reflejen los objetivos principales de privacidad de la empresa
S0355	Habilidad para negociar los acuerdos de proveedores y evaluar las prácticas de privacidad de los proveedores
S0356	Habilidad para comunicarse con todos los niveles de gestión, incluidos los miembros de juntas (por ejemplo, habilidades interpersonales, accesibilidad, habilidades efectivas para escuchar, uso correcto del estilo e idioma del público)
S0357	Habilidad para prever nuevas amenazas a la seguridad
S0358	Habilidad para mantenerse atento a las infraestructuras técnicas en evolución
S0359	Habilidad para usar el razonamiento crítico a fin de analizar tendencias y relaciones organizativas
S0360	Habilidad para analizar y evaluar las capacidades y herramientas de las ciberoperaciones de socios internos y externos
S0361	Habilidad para analizar y evaluar los procesos de inteligencia de socios internos y externos, y la formulación de requisitos de información e información esencial
S0362	Habilidad para analizar y evaluar las capacidades y limitaciones de las organizaciones de socios internos y externos (las que tienen responsabilidades de asignación de tareas, recolección, procesamiento, explotación y difusión)
S0363	Habilidad para analizar y evaluar informes de socios internos y externos
S0364	Habilidad para percibir el contexto del entorno de amenazas de una organización
S0365	Habilidad para diseñar respuestas a incidentes para modelos de servicios en la nube
S0366	Habilidad para identificar las mejores capacidades para encontrar soluciones a problemas menos comunes y más complejos de sistemas
S0367	Habilidad para aplicar principios de ciberseguridad y privacidad a los requisitos organizativos (pertinentes a la confidencialidad, integridad, disponibilidad y autenticación, y sin rechazo de estas)

Id. de la habilidad	Descripción
S0368	Habilidad para usar la calificación de riesgos a fin de informar de métodos rentables basados en el rendimiento y ayudar a las organizaciones a identificar, evaluar y gestionar el riesgo a la ciberseguridad
S0369	Habilidad para identificar fuentes, características y usos de los recursos de datos de la organización
S0370	Habilidad para usar la estructura y los procesos de preparación de informes del proveedor de servicios de ciberdefensa dentro de la propia organización
S0371	Habilidad para responder y tomar medidas locales en respuesta a alertas de amenazas comunes de proveedores de servicios
S0372	Habilidad para interpretar, dar seguimiento y priorizar las necesidades de información y los requisitos de recolección de inteligencia en toda la empresa
S0373	Habilidad para comprobar que se recolecte información sobre rendición de cuentas de los componentes de la infraestructura de la cadena de suministro del sistema de información y de tecnología de la información y las comunicaciones
S0374	Habilidad para identificar los problemas de ciberseguridad y privacidad que surgen de las conexiones con clientes y organizaciones de socios internos y externos

A.7 Descripciones de las capacidades del Marco de la NICE

La Tabla 7 proporciona una lista de las capacidades necesarias en el ámbito de la ciberseguridad. La capacidad es la competencia para desempeñar un comportamiento observable o un comportamiento que da lugar a un producto observable. En la Lista detallada de funciones laborales del Apéndice B, se incluyen las descripciones de las capacidades seleccionadas de esta lista para cada función laboral. Esta lista se actualizará periódicamente [1]. Véase la fuente definitiva de la versión más reciente de este material en la Hoja de cálculo de referencia para la Publicación especial 800-181 del NIST [4].

Tabla 7: Descripciones de las capacidades del Marco de la NICE

Id. de la capacidad	Descripción
A0001	Capacidad para identificar problemas sistémicos de seguridad en función del análisis de datos de vulnerabilidades y configuraciones
A0002	Capacidad para identificar la tecnología de repositorios de conocimientos apropiada para una aplicación o entorno determinados
A0003	Capacidad para determinar la validez de los datos de tendencias tecnológicas
A0004	Capacidad para elaborar planes de estudios de manera que traten los temas al nivel adecuado para el público destinatario
A0005	Capacidad para descifrar la recolección de datos digitales
A0006	Capacidad para preparar y presentar sesiones informativas de educación y concientización para facilitar que los usuarios de sistemas, redes y datos conozcan y sigan las políticas y los procedimientos de seguridad de los sistemas
A0007	Capacidad para adaptar el análisis de código a consideraciones específicas de la aplicación
A0008	Capacidad para aplicar los métodos, estándares y sistemas para describir, analizar y documentar la arquitectura empresarial de tecnología de la información (TI) de una organización (por ejemplo, Marco de arquitectura del Open Group [TOGAF, por sus siglas en inglés], el Marco de arquitectura del Departamento de Defensa [DoDAF, por sus siglas en inglés], el Marco de arquitectura empresarial federal [FEAF, por sus siglas en inglés])
A0009	Capacidad para aplicar normas de gestión de riesgos de la cadena de suministro
A0010	Capacidad para analizar malware
A0011	Capacidad para responder preguntas de manera clara y concisa
A0012	Capacidad para formular preguntas aclaratorias
A0013	Capacidad para comunicar información, ideas o conceptos complejos de manera segura y bien organizada por medios orales, escritos o visuales
A0014	Capacidad para comunicarse con efectividad al escribir
A0015	Capacidad para llevar a cabo detecciones de vulnerabilidades y reconocer vulnerabilidades en los sistemas de seguridad
A0016	Capacidad para facilitar debates en grupos pequeños
A0017	Capacidad para medir el nivel de comprensión y conocimientos del estudiante
A0018	Capacidad para preparar y presentar sesiones informativas
A0019	Capacidad para producir documentación técnica
A0020	Capacidad para proporcionar retroalimentación efectiva a los estudiantes a fin de mejorar el aprendizaje
A0021	Capacidad para emplear y entender conceptos matemáticos complejos (por ejemplo, matemática discreta)

Id. de la capacidad	Descripción
A0022	Capacidad para aplicar los principios del aprendizaje de adultos
A0023	Capacidad para diseñar evaluaciones válidas y confiables
A0024	Capacidad para elaborar instrucciones y materiales didácticos claros
A0025	Capacidad para definir con precisión incidentes, problemas y eventos en el sistema de control para el registro de problemas
A0026	Capacidad para analizar los datos de pruebas
A0027	Capacidad para aplicar las metas y objetivos de una organización para diseñar y mantener la arquitectura
A0028	Capacidad para evaluar y pronosticar los requisitos de personal a fin de cumplir los objetivos de la organización
A0029	Capacidad para construir estructuras de datos complejas y lenguajes de programación de alto nivel
A0030	Capacidad para recolectar, verificar y validar los datos de pruebas
A0031	Capacidad para llevar a cabo e implementar investigación de mercados para conocer las capacidades del gobierno y el sector y el debido establecimiento de precios
A0032	Capacidad para elaborar planes de estudios a fin de emplearlos en un entorno virtual
A0033	Capacidad para formular políticas, planes y estrategias de conformidad con las leyes, reglamentos, políticas y estándares compatibles con las actividades cibernéticas de la organización
A0034	Capacidad para formular, actualizar o mantener procedimientos operativos estándar (SOP, por sus siglas en inglés)
A0035	Capacidad para seccionar un problema y examinar las interrelaciones entre los datos que, en apariencia, no están relacionados
A0036	Capacidad para identificar defectos de codificación básicos y comunes a alto nivel
A0037	Capacidad para aprovechar las mejores prácticas y las lecciones aprendidas de las organizaciones externas e instituciones académicas que se ocupan de cuestiones cibernéticas
A0038	Capacidad para optimizar los sistemas a fin de cumplir los requisitos de rendimiento de la empresa
A0039	Capacidad para supervisar el desarrollo y la actualización del costo estimado del ciclo de vida
A0040	Capacidad para convertir datos y resultados de pruebas en conclusiones evaluativas
A0041	Capacidad para utilizar herramientas de visualización de datos (por ejemplo, Flare, HighCharts, AmCharts, D3.js, Processing, interfaz de programación de aplicaciones [API, por sus siglas en inglés] Google Visualization, Tableau, Raphael.js)
A0042	Capacidad para crear oportunidades de trayectorias profesionales
A0043	Capacidad para llevar a cabo análisis forenses en los entornos de Windows y Unix/Linux y para estos
A0044	Capacidad para aplicar estructuras de lenguaje de programación (por ejemplo, revisión de código fuente) y lógica
A0045	Capacidad para evaluar y comprobar la confiabilidad del proveedor o producto
A0046	Capacidad para vigilar y evaluar el impacto potencial de las tecnologías emergentes en las leyes, los reglamentos o las políticas
A0047	Capacidad para desarrollar software seguro de acuerdo con metodologías, herramientas y prácticas para la implementación protegida de software
A0048	Capacidad para aplicar conceptos de arquitectura de la seguridad de la red, incluida topología, protocolos, componentes y principios (por ejemplo, aplicación de la defensa en profundidad)

Id. de la capacidad	Descripción
A0049	Capacidad para aplicar herramientas, métodos y técnicas de diseño de sistemas seguros
A0050	Capacidad para aplicar herramientas, métodos y técnicas de diseño de sistemas, incluidas las herramientas automatizadas de análisis y diseño de sistemas
A0051	Capacidad para llevar a cabo procesos de integración de tecnología
A0052	Capacidad para operar equipos de redes, incluidos concentradores, enrutadores, puentes, conmutadores, servidores, medios de transmisión y el hardware correspondiente
A0053	Capacidad para determinar la validez de los datos de tendencias del personal
A0054	Capacidad para aplicar metodología de diseño de sistemas didácticos (ISD, por sus siglas en inglés)
A0055	Capacidad para operar herramientas de red comunes (por ejemplo, ping, traceroute, nslookup)
A0056	Capacidad para comprobar que se sigan las prácticas de seguridad en todo el proceso de adquisición
A0057	Capacidad para adaptar planes de estudios de manera que traten los temas al nivel apropiado para el público destinatario
A0058	Capacidad para ejecutar la línea de comandos del sistema operativo (por ejemplo, ipconfig, netstat, dir, nbtstat)
A0059	Capacidad para operar las rutas LAN o WAN de la organización
A0060	Capacidad para construir arquitecturas y marcos
A0061	Capacidad para diseñar arquitecturas y marcos
A0062	Capacidad para vigilar las mediciones o los indicadores de rendimiento y disponibilidad del sistema
A0063	Capacidad para operar diferentes sistemas y métodos de comunicación electrónica (por ejemplo, correo electrónico, voz sobre protocolo de internet [VoIP], mensajería instantánea, foros web, difusiones de video en directo)
A0064	Capacidad para interpretar y convertir los requisitos del cliente en capacidades operativas
A0065	Capacidad para vigilar los flujos de tráfico en toda la red
A0066	Capacidad para obtener de forma precisa y completa todos los datos utilizados en los productos de inteligencia, evaluación o planificación
A0067	Capacidad para adaptarse y operar en un entorno de trabajo diverso, impredecible, difícil y acelerado
A0068	Capacidad para aplicar los procesos aprobados de desarrollo de planificación y dotación de personal
A0069	Capacidad para aplicar habilidades y estrategias de colaboración
A0070	Capacidad para aplicar habilidades críticas de lectura y razonamiento
A0071	Capacidad para aplicar experiencia lingüística y cultural al análisis
A0072	Capacidad para expresar claramente los requisitos de inteligencia en preguntas de investigación bien formuladas y variables de seguimiento de datos para fines de seguimiento de consultas
A0073	Capacidad para expresar claramente los requisitos de inteligencia en preguntas de investigación y solicitudes de información bien formuladas
A0074	Capacidad para colaborar efectivamente con los demás
A0076	Capacidad para coordinar y colaborar con analistas en lo que se refiere a los requisitos de vigilancia y el desarrollo de información esencial
A0077	Capacidad para coordinar las ciberoperaciones con otras funciones de la organización o actividades de ayuda
A0078	Capacidad para coordinar y colaborar con organizaciones subordinadas, laterales y de alto nivel, y distribuirles información

Id. de la capacidad	Descripción
A0079	Capacidad para emplear correctamente cada organización o elemento en el plan y la matriz de recolección
A0080	Capacidad para formular o recomendar métodos analíticos o soluciones a problemas y situaciones para los que no existe información completa o ningún precedente
A0081	Capacidad para formular o recomendar soluciones de planificación a problemas y situaciones para los que no existe ningún precedente
A0082	Capacidad para colaborar efectivamente por medio de equipos virtuales
A0083	Capacidad para evaluar información a fin de determinar su confiabilidad, validez y pertinencia
A0084	Capacidad para evaluar, analizar y sintetizar grandes cantidades de datos (que pueden estar fragmentados y ser contradictorios) en productos de alta calidad combinados de inteligencia o selección de objetivos
A0085	Capacidad para actuar con cordura cuando las políticas no estén bien definidas
A0086	Capacidad para ampliar el acceso a la red mediante el análisis de objetivos y la recolección a fin de identificar objetivos de interés
A0087	Capacidad para dirigir los trabajos de investigación con objeto de satisfacer las necesidades de toma de decisiones del cliente
A0088	Capacidad para funcionar efectivamente en un entorno dinámico y acelerado
A0089	Capacidad para funcionar en un entorno de colaboración, consultando continuamente con otros analistas y expertos, tanto internos como externos a la organización, para aprovechar la experiencia analítica y técnica
A0090	Capacidad para identificar socios externos con intereses comunes en materia de ciberoperaciones
A0091	Capacidad para identificar deficiencias de inteligencia
A0092	Capacidad para identificar y describir la vulnerabilidad del objetivo
A0093	Capacidad para identificar y describir técnicas y métodos para llevar a cabo la explotación técnica el objetivo
A0094	Capacidad para interpretar y aplicar leyes, reglamentos, políticas y orientación pertinentes a los objetivos cibernéticos de la organización
A0095	Capacidad para interpretar y convertir los requisitos del cliente en acciones operativas
A0096	Capacidad para interpretar y entender conceptos complejos y en evolución rápida
A0097	Capacidad para vigilar las operaciones del sistema y reaccionar a los eventos en respuesta a desencadenadores o a la observación de tendencias o de actividad inusual
A0098	Capacidad para participar como miembro de los equipos de planificación, grupos de coordinación y grupos de trabajo según sea necesario
A0099	Capacidad para poner en práctica tácticas, técnicas y procedimientos de recolección de redes, incluidas las capacidades y herramientas de descifrado
A0100	Capacidad para aplicar procedimientos de recolección inalámbrica, incluidas las capacidades y herramientas de descifrado
A0101	Capacidad para reconocer y mitigar sesgos cognitivos que puedan afectar el análisis
A0102	Capacidad para reconocer y mitigar engaños en informes y análisis
A0103	Capacidad para revisar materiales procesados en el idioma del objetivo para verificar su exactitud e integridad
A0104	Capacidad para seleccionar el implante apropiado para lograr las metas operativas
A0105	Capacidad para adaptar la información técnica y de planificación al nivel de comprensión del cliente
A0106	Capacidad para razonar críticamente
A0107	Capacidad para pensar como los actores de amenazas

Id. de la capacidad	Descripción
A0108	Capacidad para entender los objetivos y los efectos
A0109	Capacidad para usar varias fuentes de información de inteligencia en todas las disciplinas de inteligencia
A0110	Capacidad para vigilar los avances en las leyes de privacidad de la información a fin de facilitar la adaptación y el cumplimiento organizativos
A0111	Capacidad para trabajar con todos los departamentos y las unidades de negocios para implementar los principios y programas de privacidad de la organización y alinear los objetivos de privacidad con los objetivos de seguridad
A0112	Capacidad para vigilar los avances en las tecnologías de la privacidad de la información para garantizar la adaptación y el cumplimiento organizativos
A0113	Capacidad para determinar si un incidente de seguridad infringe un principio de privacidad o una norma legal que requiera una acción legal específica
A0114	Capacidad para elaborar u obtener planes de estudios que traten los temas al nivel adecuado para el público destinatario
A0115	Capacidad para trabajar con todos los departamentos y las unidades de negocios para implementar los principios y programas de privacidad de la organización y alinear los objetivos de privacidad con los objetivos de seguridad
A0116	Capacidad para priorizar y asignar recursos de ciberseguridad de forma correcta y eficiente
A0117	Capacidad para relacionar la estrategia, el negocio y la tecnología en el contexto de la dinámica organizativa
A0118	Capacidad para entender las cuestiones de tecnología, gestión y liderazgo relacionadas con los procesos de la organización y la solución de problemas
A0119	Capacidad para entender los conceptos básicos y problemas relacionados con la cibernética y su impacto organizativo
A0120	Capacidad para intercambiar información importante sobre el contexto del entorno de amenaza de una organización que mejore su postura de gestión de riesgos
A0121	Capacidad para diseñar la respuesta a incidentes para modelos de servicios en la nube
A0122	Capacidad para diseñar capacidades para encontrar soluciones a problemas menos comunes y más complejos de sistemas
A0123	Capacidad para aplicar principios de ciberseguridad y privacidad a los requisitos organizativos (pertinentes a la confidencialidad, integridad, disponibilidad y autenticación, y sin rechazo de estas)
A0124	Capacidad para establecer y mantener evaluaciones automatizadas de control de seguridad
A0125	Capacidad para crear una declaración de divulgación de privacidad basada en las leyes vigentes
A0126	Capacidad para dar seguimiento a la ubicación y configuración de dispositivos y software en red, en todos los departamentos, ubicaciones e instalaciones, y potencialmente, funciones de negocios compatibles
A0127	Capacidad para implementar tecnologías y herramientas de vigilancia continua
A0128	Capacidad para aplicar técnicas para detectar intrusiones basadas en servidores y redes con el uso de tecnologías de detección de intrusiones
A0129	Capacidad para verificar que los procesos de gestión de seguridad de la información se integren con los procesos de planificación estratégica y operativa
A0130	Capacidad para lograr que los funcionarios sénior de la organización proporcionen seguridad de la información para la información y los sistemas que ayudan a las operaciones y los recursos bajo su control

Id. de la capacidad	Descripción
A0131	Capacidad para conseguir que la organización cuente con personal suficientemente capacitado que ayude con el cumplimiento de los requisitos de seguridad en legislación, órdenes ejecutivas, políticas, directivas, instrucciones, normas y directrices
A0132	Capacidad para coordinarse con la dirección sénior de una organización a fin de proporcionar un método integral y holístico en toda la organización para solucionar riesgos: un método que proporcione mayor conocimiento de las operaciones integradas de la organización
A0133	Capacidad para coordinarse con la dirección sénior de una organización a fin de formular una estrategia de gestión de riesgos para la organización que proporcione una vista estratégica de los riesgos relacionados con la seguridad de la organización
A0134	Capacidad para coordinarse con la dirección sénior de una organización a fin de facilitar el intercambio de información relacionada con riesgos entre los funcionarios que autorizan y otros dirigentes sénior de la organización
A0135	Capacidad para coordinarse con la dirección sénior de una organización a fin de supervisar todas las actividades relacionadas con la gestión de riesgos en toda la organización y procurar que se tomen decisiones uniformes y efectivas sobre aceptación de riesgos
A0136	Capacidad para coordinarse con la dirección sénior de una organización a fin de facilitar que las decisiones de autorización tengan en cuenta todos los factores necesarios para el éxito de la misión y la empresa
A0137	Capacidad para coordinarse con la dirección sénior de una organización a fin de proporcionar un foro en toda la organización para que se consideren todas las fuentes de riesgo (incluido el riesgo agregado) en las operaciones y recursos organizativos, personas, otras organizaciones y el país
A0138	Capacidad para coordinarse con la dirección sénior de una organización a fin de promover la cooperación y la colaboración entre los funcionarios que autorizan e incluir las medidas de autorización que requieran una responsabilidad compartida
A0139	Capacidad para coordinarse con la dirección sénior de una organización a fin de lograr que la responsabilidad compartida de ayudar en las funciones de la misión y de negocios de la organización, usando proveedores externos de sistemas, servicios y aplicaciones, reciba la visibilidad necesaria y se eleve a las debidas autoridades responsables de la toma de decisiones
A0140	Capacidad para coordinarse con la dirección sénior de una organización a fin de identificar la postura de riesgo organizativo en función del riesgo agregado que conlleva la operación y el uso de los sistemas que son responsabilidad de la organización
A0141	Capacidad para trabajar en estrecha colaboración con los funcionarios que autorizan y sus representantes designados para ayudar a lograr la implementación efectiva de un programa de seguridad en toda la organización que proporcione seguridad adecuada a todos los sistemas y entornos de operación organizativos
A0142	Capacidad para trabajar en estrecha colaboración con los funcionarios que autorizan y sus representantes designados para ayudar a lograr la integración de las consideraciones de seguridad en los ciclos de programación, planificación y presupuesto, en las arquitecturas empresariales y en los ciclos de vida de desarrollo de sistemas y adquisiciones
A0143	Capacidad para trabajar en estrecha colaboración con los funcionarios que autorizan y sus representantes designados para ayudar a lograr que los sistemas organizativos y los controles comunes estén cubiertos por los planes de seguridad aprobados y posean autorizaciones vigentes

Id. de la capacidad	Descripción
A0144	Capacidad para trabajar en estrecha colaboración con los funcionarios que autorizan y sus representantes designados para ayudar a lograr que las actividades relacionadas con la seguridad necesarias en toda la organización se lleven a cabo de manera eficiente, rentable y oportuna
A0145	Capacidad para trabajar en estrecha colaboración con los funcionarios que autorizan y sus representantes designados para ayudar a lograr la presentación centralizada de informes sobre las actividades relacionadas con la seguridad
A0146	Capacidad para establecer las normas para el uso y la protección apropiados de la información y para mantener esa responsabilidad incluso cuando la información se comunique a otras organizaciones o se intercambie con estas
A0147	Capacidad para aprobar planes de seguridad, memorandos de acuerdo o de entendimiento, planes de acción e hitos, y determinar si los cambios de importancia en los sistemas o entornos de operación requieren una nueva autorización
A0148	Capacidad para servir como el enlace principal entre el arquitecto de la empresa y el ingeniero de seguridad de sistemas y para coordinarse con los propietarios de sistemas, proveedores de control común y funcionarios de seguridad de sistemas para la asignación de controles de seguridad como controles propios del sistema, híbridos o comunes
A0149	Capacidad para asesorar, en estrecha coordinación con los funcionarios de seguridad del sistema, a los funcionarios que autorizan, directores de sistemas de información, funcionarios sénior de seguridad de sistemas de información y al funcionario sénior responsable de la gestión de riesgos o de la (función) ejecutiva de riesgos, sobre una serie de cuestiones relacionadas con la seguridad (por ejemplo, establecer límites del sistema, evaluar la gravedad de las debilidades y deficiencias del sistema, planes de acción e hitos, métodos para la mitigación de riesgos, alertas de seguridad y efectos adversos potenciales de las vulnerabilidades identificadas)
A0150	Capacidad para llevar a cabo actividades de ingeniería de seguridad de sistemas (Publicación especial 800-160 del NIST)
A0151	Capacidad para captar y refinar los requisitos de seguridad y procurar que estos se integren efectivamente en los productos y sistemas de los componentes mediante una arquitectura, diseño, desarrollo y configuración de la seguridad firmes
A0152	Capacidad para emplear las mejores prácticas en la implementación de controles de seguridad dentro de un sistema, incluidas metodologías de ingeniería de software; principios de ingeniería de sistemas y seguridad; diseño, arquitectura y técnicas de codificación seguros
A0153	Capacidad para coordinar sus actividades relacionadas con la seguridad con arquitectos de seguridad, funcionarios sénior de seguridad de sistemas de información, propietarios de sistemas, proveedores de control común y funcionarios de seguridad de sistemas
A0154	Capacidad para llevar a cabo una evaluación completa de los controles administrativos, operativos y técnicos de la seguridad y de los mejoramientos de los controles empleados en un sistema, o heredados por el sistema, para determinar la efectividad de estos (es decir, la medida en la que los controles de seguridad se implementan correctamente, funcionan según lo previsto y producen el resultado deseado con respecto al cumplimiento de los requisitos de seguridad del sistema)
A0155	Capacidad para proporcionar una evaluación de la gravedad de las debilidades o deficiencias detectadas en el sistema y su entorno de operación, y recomendar medidas correctivas para solucionar las vulnerabilidades identificadas
A0156	Capacidad para preparar el informe final de evaluación de seguridad que contenga los resultados y las conclusiones de la evaluación

Id. de la capacidad	Descripción
A0157	Capacidad para evaluar un plan de seguridad y verificar que el plan proporcione un conjunto de controles de seguridad para el sistema que cumplan los requisitos de seguridad establecidos
A0158	Capacidad para lograr que los requisitos funcionales y de seguridad se incluyan debidamente en un contrato y que el contratista cumpla los requisitos funcionales y de seguridad establecidos en el contrato
A0159	Capacidad para interpretar la información recolectada por herramientas de redes (por ejemplo, nslookup, ping y traceroute)
A0160	Capacidad para interpretar, dar seguimiento y priorizar las necesidades de información y los requisitos de recolección de inteligencia en toda la empresa
A0161	Capacidad para integrar los requisitos de seguridad de la información en el proceso de adquisición, usando los controles de seguridad de referencia aplicables como una de las fuentes para los requisitos de seguridad, asegurando un proceso sólido de control de calidad del software y estableciendo varias fuentes (por ejemplo, rutas de entrega, para elementos críticos del sistema)
A0162	Capacidad para conseguir que el personal de seguridad del sistema de información y de adquisición, el asesor legal y demás asesores y partes interesadas correspondientes participen en la toma de decisiones desde la definición o revisión del concepto del sistema, y que intervengan en cada decisión sobre hitos, o la aprueben, durante todo el ciclo de vida de los sistemas
A0162	Capacidad para reconocer los aspectos únicos del entorno y la jerarquía de la seguridad de las comunicaciones (COMSEC)
A0163	Capacidad para interpretar la terminología, directrices y procedimientos de la seguridad de las comunicaciones (COMSEC)
A0164	Capacidad para identificar las funciones y responsabilidades del personal nombrado para la seguridad de las comunicaciones (COMSEC)
A0165	Capacidad para gestionar el procedimiento de uso, control y contabilidad de los materiales de la seguridad de las comunicaciones (COMSEC)
A0166	Capacidad para identificar los tipos de incidentes de seguridad de las comunicaciones (COMSEC) y la manera de informar de ellos
A0167	Capacidad para reconocer la importancia de auditar el material y las cuentas de la seguridad de las comunicaciones (COMSEC)
A0168	Capacidad para identificar los requisitos de la contabilidad en proceso para la seguridad de las comunicaciones (COMSEC)
A0170	Capacidad para identificar los sistemas de infraestructura crítica con tecnología de comunicación de la información diseñados sin considerar la seguridad del sistema
A0171	Capacidad para llevar a cabo la evaluación de necesidades de capacitación y formación
A0172	Capacidad para configurar las subredes físicas o lógicas que separan una red de área local (LAN) interna de otras redes que no son de confianza
A0173	Capacidad para reconocer que los cambios a los sistemas o entornos pueden modificar los riesgos residuales en relación con el apetito de riesgo
A0174	Capacidad para encontrar y navegar por la web oscura utilizando la red TOR para ubicar mercados y foros
A0175	Capacidad para examinar medios digitales en varias plataformas de sistemas operativos
A0176	Capacidad para mantener bases de datos (es decir, hacer copias de seguridad, restaurar, eliminar datos, archivos de registros de transacciones, etc.)

Apéndice B: Lista detallada de las funciones laborales

Este apéndice proporciona una descripción detallada de cada función laboral del Marco de la NICE. En la lista a continuación, se incluye la siguiente información para cada función laboral:

- el nombre de la función laboral;
- la identificación única de la función laboral del Marco de la NICE, basada en las abreviaturas de la Categoría y área de especialización del Marco de la NICE a las que pertenece esa función laboral;
- el área de especialización en la que reside la función laboral;
- la Categoría en la que reside la función laboral;
- una descripción de la función laboral;
- una lista de las tareas del Marco de la NICE que se prevé que desempeñe la persona que ocupa un puesto de ciberseguridad que incluya la función laboral;
- una lista de las áreas de conocimientos del Marco de la NICE que se prevé que muestre la persona que ocupa un puesto de ciberseguridad que incluya la función laboral;
- una lista de las habilidades del Marco de la NICE que se prevé que posea una persona que ocupa un puesto de ciberseguridad que incluya la función laboral; y
- una lista de las capacidades del Marco de la NICE que se prevé que demuestre una persona que ocupa un puesto de ciberseguridad que incluya la función laboral.

En las tablas a continuación, se describen las funciones laborales de Marco de la NICE con una lista sencilla de tareas, conocimientos, habilidades y capacidades. Véase la fuente definitiva de la versión más reciente de este material en la Hoja de cálculo de referencia para la Publicación especial 800-181 del NIST [4]. La Hoja de cálculo de referencia contiene listas más pormenorizadas de las tareas, conocimientos, habilidades y capacidades. Las funciones laborales se actualizarán periódicamente [1].

B.1 Suministrar protección (SP)

Nombre de la función laboral	**Funcionario que autoriza**
Id. de la función laboral	**SP-RSK-001**
Área de especialización	**Gestión de riesgos (RSK)**
Categoría	**Suministrar protección (SP)**
Descripción de la función laboral	Funcionario o ejecutivo sénior con autoridad para asumir formalmente la responsabilidad de operar un sistema de información a un nivel aceptable de riesgo para las operaciones organizativas (incluida la misión, las funciones, la imagen o la reputación), los recursos organizativos, las personas, otras organizaciones y el país (instrucción 4009 del CNSS).
Tareas	T0145, T0221, T0371, T0495

Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0070, K0084, K0089, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0295, K0322, K0342, K0622, K0624
Habilidades	S0034, S0367
Capacidades	A0028, A0033, A0077, A0090, A0094, A0111, A0117, A0118, A0119, A0123, A0170

Nombre de la función laboral	**Asesor de control de seguridad**
Id. de la función laboral	**SP-RSK-002**
Área de especialización	**Gestión de riesgos (RSK)**
Categoría	**Suministrar protección (SP)**
Descripción de la función laboral	Lleva a cabo evaluaciones independientes y completas de los controles de seguridad de la gestión, operativos y técnicos, y de los mejoramientos a los controles empleados en un sistema de tecnología de la información (TI), o heredados por ese sistema, para determinar la efectividad general de esos controles (según se define en la Publicación especial 800-37 del NIST).
Tareas	T0145, T0184, T0221, T0244, T0251, T0371, T0495, T0177, T0178, T0181, T0205, T0243, T0255, T0264, T0265, T0268, T0272, T0275, T0277, T0309, T0344
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0013, K0018, K0019, K0018, K0021, K0024, K0026, K0027, K0028, K0029, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0056, K0059, K0070, K0084, K0089, K0098, K0100, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0287, K0322, K0342, K0622, K0624
Habilidades	S0001, S0006, S0027, S0034, S0038, S0073, S0078, S0097, S0100, S0110, S0111, S0112, S0115, S0120, S0124, S0128, S0134, S0135, S0136, S0137, S0138, S0141, S0145, S0147, S0171, S0172, S0173, S0174, S0175, S0176, S0177, S0184, S0232, S0233, S0234, S0235, S0236, S0237, S0238, S0239, S0240, S0241, S0242, S0243, S0244, S0248, S0249, S0250, S0251, S0252, S0254, S0271, S0273, S0278, S0279, S0280, S0281, S0296, S0304, S0305, S0306, S0307, S0325, S0329, S0332, S0367, S0370, S0374
Capacidades	A0001, A0011, A0012, A0013, A0014, A0015, A0016, A0018, A0019, A0023, A0026, A0030, A0035, A0036, A0040, A0056, A0069, A0070, A0082, A0083, A0084, A0085, A0086, A0087, A0088, A0089, A0090, A0091, A0092, A0093, A0094, A0095, A0096, A0098, A0101, A0106, A0108, A0109, A0117, A0118, A0119, A0111, A0112, A0114, A0115, A0116, A0119, A0123, A0170

Nombre de la función laboral	**Desarrollador de software**
Id. de la función laboral	**SP-DEV-001**
Área de especialización	**Desarrollo de software (DEV)**
Categoría	**Suministrar protección (SP)**
Descripción de la función laboral	Elabora, crea, mantiene y escribe o codifica aplicaciones informáticas, software o programas especializados de utilidades nuevos (o modifica los existentes).
Tareas	T0009, T0011, T0013, T0014, T0022, T0026, T0034, T0040, T0046, T0057, T0077, T0100, T0111, T0117, T0118, T0171, T0176, T0181, T0189, T0217, T0228, T0236, T0267, T0303, T0311, T0324, T0337, T0416, T0417, T0436, T0455, T0500, T0553, T0554
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0332, K0342, K0343, K0624
Habilidades	S0001, S0014, S0017, S0019, S0022, S0031, S0034, S0060, S0135, S0138, S0149, S0174, S0175, S0367
Capacidades	A0007, A0021, A0047, A0123, A0170

Nombre de la función laboral	**Asesor de software seguro**
Id. de la función laboral	**SP-DEV-002**
Área de especialización	**Desarrollo de software (DEV)**
Categoría	**Suministrar protección (SP)**
Descripción de la función laboral	Analiza la seguridad de aplicaciones informáticas, software o programas especializados de utilidades nuevos o existentes, y proporciona resultados procesables.
Tareas	T0013, T0014, T0022, T0038, T0040, T0100, T0111, T0117, T0118, T0171, T0181, T0217, T0228, T0236, T0266, T0311, T0324, T0337, T0424, T0428, T0436, T0456, T0457, T0516, T0554
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0178, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0342, K0343, K0624
Habilidades	S0001, S0022, S0031, S0034, S0083, S0135, S0138, S0174, S0175, S0367
Capacidades	A0021, A0123, A0170

Nombre de la función laboral	**Arquitecto empresarial**
Id. de la función laboral	**SP-ARC-001**
Área de especialización	**Arquitectura de sistemas (ARC)**
Categoría	**Suministrar protección (SP)**
Descripción de la función laboral	Establece y mantiene los procesos de negocios, sistemas e información compatibles con las necesidades de la misión empresarial; elabora normas y requisitos relacionados con la tecnología de la información (TI) que describen las arquitecturas de referencia y del objetivo.
Tareas	T0051, T0084, T0090, T0108, T0196, T0205, T0307, T0314, T0328, T0338, T0427, T0440, T0448, T0473, T0517, T0521, T0542, T0555, T0557
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0024, K0027, K0028, K0030, K0035, K0037, K0043, K0044, K0052, K0056, K0060, K0061, K0063, K0074, K0075, K0082, K0091, K0093, K0102, K0170, K0179, K0180, K0198, K0200, K0203, K0207, K0211, K0212, K0214, K0227, K0240, K0264, K0275, K0286, K0287, K0291, K0293, K0299, K0322, K0323, K0325, K0326, K0332, K0333, K0487, K0516
Habilidades	S0005, S0024, S0027, S0050, S0060, S0122, S0367, S0374
Capacidades	A0008, A0015, A0027, A0038, A0051, A0060, A0123, A0170

Nombre de la función laboral	**Arquitecto de seguridad**
Id. de la función laboral	**SP-ARC-002**
Área de especialización	**Arquitectura de sistemas (ARC)**
Categoría	**Suministrar protección (SP)**
Descripción de la función laboral	Comprueba que los requisitos de seguridad de las partes interesadas, necesarios para proteger que los procesos de la misión y de negocios de la organización se tengan suficientemente en cuenta en todos los aspectos de la arquitectura empresarial, incluidos los modelos de referencia, las arquitecturas de segmentos y soluciones, y los sistemas resultantes compatibles con los procesos de la misión y de negocios.
Tareas	T0050, T0051, T0071, T0082, T0084, T0090, T0108, T0177, T0196, T0203, T0205, T0268, T0307, T0314, T0328, T0338, T0427, T0448, T0473, T0484, T0542, T0556
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0015, K0018, K0019, K0024, K0026, K0027, K0030, K0035, K0036, K0037, K0043, K0044, K0052, K0055, K0056, K0057, K0059, K0060, K0061, K0063, K0071, K0074, K0082, K0091, K0092, K0093, K0102, K0170, K0180, K0198, K0200, K0202, K0211, K0212, K0214, K0227, K0240, K0260, K0261, K0262, K0264, K0275, K0277, K0286, K0287, K0291, K0293, K0320, K0322, K0323, K0325, K0326, K0332, K0333, K0336, K0565, K0599
Habilidades	S0005, S0022, S0024, S0027, S0050, S0059, S0061, S0076, S0116, S0122, S0138, S0139, S0152, S0168, S0170, S367, S0374
Capacidades	A0008, A0014, A0015, A0027, A0038, A0048, A0049, A0050, A0061, A0123, A0148, A0149, A0170, A0172

Nombre de la función laboral	**Especialista en investigación y desarrollo**
Id. de la función laboral	**SP-TRD-001**
Área de especialización	**Investigación y desarrollo tecnológicos (TRD)**
Categoría	**Suministrar protección (SP)**
Descripción de la función laboral	Lleva a cabo la ingeniería de software y de sistemas y la investigación de sistemas de software para crear capacidades nuevas y lograr la integración total de la ciberseguridad. Lleva a cabo investigación tecnológica completa para evaluar las vulnerabilidades potenciales en los sistemas del ciberespacio.
Tareas	T0064, T0249, T0250, T0283, T0284, T0327, T0329, T0409, T0410, T0411, T0413, T0547
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0059, K0090, K0126, K0169, K0170, K0171, K0172, K0174, K0175, K0176, K0179, K0202, K0209, K0267, K0268, K0269, K0271, K0272, K0288, K0296, K0310, K0314, K0321, K0342, K0499
Habilidades	S0005, S0017, S0072, S0140, S0148, S0172
Capacidades	A0001, A0018, A0019, A0170

Nombre de la función laboral	**Planificador de requisitos de sistemas**
Id. de la función laboral	**SP-SRP-001**
Área de especialización	**Planificación de requisitos de sistemas (SRP)**
Categoría	**Suministrar protección (SP)**
Descripción de la función laboral	Consulta con los clientes para evaluar los requisitos funcionales y convertir esos requisitos en soluciones técnicas.
Tareas	T0033, T0039, T0045, T0052, T0062, T0127, T0156, T0174, T0191, T0235, T0273, T0300, T0313, T0325, T0334, T0454, T0463, T0497
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0012, K0018, K0019, K0032, K0035, K0038, K0043, K0044, K0045, K0047, K0055, K0056, K0059, K0060, K0061, K0063, K0066, K0067, K0073, K0074, K0086, K0087, K0090, K0091, K0093, K0101, K0102, K0126, K0163, K0164, K0168, K0169, K0170, K0180, K0200, K0267, K0287, K0325, K0332, K0333, K0622
Habilidades	S0005, S0006, S0008, S0010, S0050, S0134, S0367
Capacidades	A0064, A0123, A0170

Nombre de la función laboral	**Especialista en pruebas y evaluaciones del sistema**
Id. de la función laboral	**SP-TST-001**
Área de especialización	**Prueba y evaluación (TST)**
Categoría	**Suministrar protección (SP)**
Descripción de la función laboral	Planifica, prepara y pone a prueba los sistemas para evaluar los resultados con respecto a las especificaciones y los requisitos, y para analizar los resultados de las pruebas e informar de estos.
Tareas	T0058, T0080, T0125, T0143, T0257, T0274, T0393, T0426, T0511, T0512, T0513, T0539, T0540
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0027, K0028, K0037, K0044, K0057, K0088, K0091, K0102, K0139, K0126, K0169, K0170, K0179, K0199, K0203, K0212, K0250, K0260, K0261, K0262, K0287, K0332
Habilidades	S0015, S0021, S0026, S0030, S0048, S0060, S0061, S0082, S0104, S0107, S0110, S0112, S0115, S0117, S0367
Capacidades	A0026, A0030, A0040, A0123

Nombre de la función laboral	**Promotor de seguridad de sistemas de información**
Id. de la función laboral	**SP-SYS-001**
Área de especialización	**Desarrollo de sistemas (SYS)**
Categoría	**Suministrar protección (SP)**
Descripción de la función laboral	Diseña, desarrolla, pone a prueba y evalúa la seguridad del sistema de información en todo el ciclo de vida de desarrollo de sistemas.
Tareas	T0012, T0015, T0018, T0019, T0021, T0032, T0053, T0055, T0056, T0061, T0069, T0070, T0076, T0078, T0105, T0107, T0109, T0119, T0122, T0124, T0181, T0201, T0205, T0228, T0231, T0242, T0269, T0270, T0271, T0272, T0304, T0326, T0359, T0446, T0449, T0466, T0509, T0518, T0527, T0541, T0544
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0024, K0027, K0028, K0030, K0032, K0035, K0036, K0044, K0045, K0049, K0050, K0052, K0055, K0056, K0060, K0061, K0063, K0065, K0066, K0067, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0093, K0102, K0126, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0332, K0333, K0336
Habilidades	S0001, S0022, S0023, S0024, S0031, S0034, S0036, S0085, S0145, S0160, S0367
Capacidades	A0001, A0008, A0012, A0013, A0015, A0019, A0026, A0040, A0048, A0049, A0050, A0056, A0061, A0074, A0089, A0098, A0108, A0119, A0123, A0170

Nombre de la función laboral	**Desarrollador de sistemas**
Id. de la función laboral	**SP-SYS-002**
Área de especialización	**Desarrollo de sistemas (SYS)**
Categoría	**Suministrar protección (SP)**
Descripción de la función laboral	Diseña, desarrolla, pone a prueba y evalúa los sistemas de información en todo el ciclo de vida de desarrollo de sistemas.
Tareas	T0012, T0021, T0053, T0056, T0061, T0067, T0070, T0107, T0109, T0119, T0181, T0201, T0205, T0228, T0242, T0304, T0326, T0350, T0358, T0359, T0378, T0406, T0447, T0449, T0464, T0466, T0480, T0488, T0518, T0528, T0538, T0541, T0544, T0558, T0559, T0560
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0024, K0027, K0028, K0030, K0032, K0035, K0036, K0044, K0045, K0049, K0050, K0052, K0055, K0056, K0060, K0061, K0063, K0065, K0066, K0067, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0093, K0102, K0126, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0207, K0212, K0227, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0332, K0333, K0336
Habilidades	S0018, S0022, S0023, S0024, S0025, S0031, S0034, S0036, S0060, S0085, S0097, S0136, S0145, S0146, S0160, S0367
Capacidades	A0123, A0170

B.2 Operar y mantener (OM)

Nombre de la función laboral	**Administrador de bases de datos**
Id. de la función laboral	**OM-DTA-001**
Área de especialización	**Administración de datos (DTAA)**
Categoría	**Operar y mantener (OM)**
Descripción de la función laboral	Administra los sistemas de bases de datos o de gestión de datos que permiten almacenar, consultar y utilizar datos de manera segura.
Tareas	T0008, T0137, T0139, T0140, T0146, T0152, T0162, T0210, T0305, T0306, T0330, T0422, T0459, T0490
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0020, K0021, K0022, K0023, K0025, K0031, K0056, K0060, K0065, K0069, K0083, K0097, K0197, K0260, K0261, K0262, K0277, K0278, K0287, K0420
Habilidades	S0002, S0013, S0037, S0042, S0045
Capacidades	A0176

Nombre de la función laboral	**Analista de datos**
Id. de la función laboral	**OM-DTA-002**
Área de especialización	**Administración de datos (DTA)**
Categoría	**Operar y mantener (OM)**
Descripción de la función laboral	Examina datos de varias fuentes distintas con el fin de hacer recomendaciones sobre seguridad y privacidad. Diseña e implementa algoritmos, procesos de flujo de trabajo y diseños personalizados para los conjuntos de datos complejos de escala empresarial que se usan para modelado, extracción de datos e investigación.
Tareas	T0007, T0008, T0068, T0146, T0195, T0210, T0342, T0347, T0349, T0351, T0353, T0361, T0366, T0381, T0382, T0383, T0385, T0392, T0402, T0403, T0404, T0405, T0460
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0016, K0020, K0022, K0023, K0025, K0031, K0051, K0052, K0056, K0060, K0065, K0068, K0069, K0083, K0095, K0129, K0139, K0140, K0193, K0197, K0229, K0236, K0238, K0325, K0420
Habilidades	S0013, S0017, S0202, S0028, S0029, S0037, S0060, S0088, S0089, S0094, S0095, S0103, S0106, S0109, S0113, S0114, S0118, S0119, S0123, S0125, S0126, S0127, S0129, S0130, S0160, S0369
Capacidades	A0029, A0035, A0036, A0041, A0066

Nombre de la función laboral	**Administrador de conocimientos**
Id. de la función laboral	**OM-KMG-001**
Área de especialización	**Gestión del conocimiento (KMG)**
Categoría	**Operar y mantener (OM)**
Descripción de la función laboral	Se encarga de gestionar y administrar procesos y herramientas para que la organización pueda identificar, documentar y acceder al capital intelectual y al contenido de la información.
Tareas	T0037, T0060, T0154, T0185, T0209, T0339, T0421, T0452, T0524
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0094, K0095, K0096, K0146, K0194, K0195, K0228, K0260, K0261, K0262, K0283, K0287, K0315, K0338, K0420
Habilidades	S0011, S0012, S0049, S0055
Capacidades	A0002

Nombre de la función laboral	**Especialista en soporte técnico**
Id. de la función laboral	**OM-STS-001**
Área de especialización	**Servicio de atención al cliente y soporte técnico (STS)**
Categoría	**Operar y mantener (OM)**
Descripción de la función laboral	Proporciona soporte técnico a los clientes que necesitan ayuda para usar el hardware y el software a nivel de cliente según los componentes de procesos organizativos establecidos o aprobados (es decir, un plan maestro de gestión de incidentes, cuando corresponda).
Tareas	T0125, T0237, T0308, T0315, T0331, T0468, T0482, T0491, T0494, T0496, T0502, T0530
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0053, K0088, K0109, K0114, K0116, K0194, K0224, K0237, K0242, K0247, K0260, K0261, K0262, K0287, K0292, K0294, K0302, K0317, K0330
Habilidades	S0039, S0058, S0142, S0159, S0365
Capacidades	A0025, A0034, A0122

Nombre de la función laboral	**Especialista en operaciones de red**
Id. de la función laboral	**OM-NET-001**
Área de especialización	**Servicios de red (NET)**
Categoría	**Operar y mantener (OM)**
Descripción de la función laboral	Planifica, implementa y maneja servicios y sistemas de redes, incluidos el hardware y los entornos virtuales.
Tareas	T0035, T0065, T0081, T0121, T0125, T0126, T0129, T0153, T0160, T0200, T0232
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0010, K0011, K0029, K0038, K0049, K0050, K0053, K0061, K0071, K0076, K0093, K0104, K0108, K0111, K0113, K0135, K0136, K0137, K0138, K0159, K0160, K0179, K0180, K0200, K0201, K0203, K0260, K0261, K0262, K0274, K0287, K0332, K0622
Habilidades	S0004, S0035, S0040, S0041, S0056, S0077, S0079, S0084, S0150, S0162, S0170
Capacidades	A0052, A0055, A0058, A0059, A0062, A0063, A0065, A0159

Nombre de la función laboral	**Administrador de sistemas**
Id. de la función laboral	**OM-ADM-001**
Área de especialización	**Administración de sistemas (ADM)**
Categoría	**Operar y mantener (OM)**
Descripción de la función laboral	Se encarga de configurar y mantener un sistema o componentes específicos de un sistema (por ejemplo, instalar, configurar y actualizar hardware y software; establecer y manejar cuentas de usuarios; supervisar o llevar a cabo tareas de copias de seguridad y recuperación; implementar controles de seguridad operativos y técnicos; y cumplir las políticas y los procedimientos de seguridad de la organización).
Tareas	T0029, T0054, T0063, T0136, T0144, T0186, T0207, T0418, T0431, T0435, T0458, T0461, T0498, T0501, T0507, T0514, T0515, T0531
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0049, K0050, K0053, K0064, K0077, K0088, K0100, K0103, K0104, K0117, K0130, K0158, K0167, K0179, K0260, K0261, K0262, K0274, K0280, K0289, K0318, K0332, K0346
Habilidades	S0016, S0033, S0043, S0073, S0076, S0111, S0143, S0144, S0151, S0153, S0154, S0155, S0157, S0158
Capacidades	S0154, S0158

Nombre de la función laboral	**Analista de seguridad de sistemas**
Id. de la función laboral	**OM-ANA-001**
Área de especialización	**Análisis de sistemas (ANA)**
Categoría	**Operar y mantener (OM)**
Descripción de la función laboral	Se encarga del análisis y el desarrollo de la integración, las pruebas, operaciones y mantenimiento de la seguridad de los sistemas.
Tareas	T0015, T0016, T0017, T0085, T0086, T0088, T0123, T0128, T0169, T0177, T0187, T0194, T0202, T0205, T0243, T0309, T0344, T0462, T0469, T0470, T0475, T0477, T0485, T0489, T0492, T0499, T0504, T0508, T0526, T0545, T0548
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0019, K0024, K0035, K0036, K0040, K0044, K0049, K0052, K0056, K0060, K0061, K0063, K0075, K0082, K0093, K0102, K0179, K0180, K0200, K0203, K0227, K0260, K0261, K0262, K0263, K0266, K0267, K0275, K0276, K0281, K0284, K0285, K0287, K0290, K0297, K0322, K0333, K0339
Habilidades	S0024, S0027, S0031, S0036, S0060, S0141, S0147, S0167, S0367
Capacidades	A0015, A0123

B.3 Supervisar y gobernar (OV)

Nombre de la función laboral	**Asesor de derecho informático**
Id. de la función laboral	**OV-LGA-001**
Área de especialización	**Asesoramiento legal y promoción (LGA)**
Categoría	**Supervisar y gobernar (OV)**
Descripción de la función laboral	Ofrece asesoramiento jurídico y recomendaciones sobre temas pertinentes relacionados con el derecho informático.
Tareas	T0006, T0098, T0102, T0131, T0220, T0419, T0434, T0465, T0474, T0476, T0478, T0487, T0522
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0059, K0107, K0157, K0261, K0262, K0267, K0312, K0316, K0341, K0615
Habilidades	S0356
Capacidades	A0046

Nombre de la función laboral	**Funcionario de privacidad o administrador de cumplimiento de la privacidad**
Id. de la función laboral	**OV-LGA-002**
Área de especialización	**Asesoramiento legal y promoción (LGA)**
Categoría	**Supervisar y gobernar (OV)**
Descripción de la función laboral	Establece y supervisa el programa de cumplimiento de privacidad y al personal del programa de privacidad, respaldando el cumplimiento de la privacidad, la gobernanza y las políticas, y atiende las necesidades de respuesta a incidentes de los ejecutivos de privacidad y seguridad y de sus equipos.
Tareas	T0003, T0004, T0029, T0930, T0032, T0066, T0098, T0099, T0131, T0133, T0188, T0381, T0384, T0478, T0861, T0862, T0863, T0864, T0865, T0866, T0867, T0868, T0869, T0870, T0871, T0872, T0873, T0874, T0875, T0876, T0877, T0878, T0879, T0880, T0881, T0882, T0883, T0884, T0885, T0886, T0887, T0888, T0889, T0890, T0891, T0892, T0893, T0894, T0895, T0896, T0897, T0898, T0899, T0900, T0901, T0902, T0903, T0904, T0905, T0906, T0907, T0908, T0909, T0910, T0911, T0912, T0913, T0914, T0915, T0916, T0917, T0918, T0919
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0066, K0168, K0612, K0613, K0614, K0615
Habilidades	S0354, S0355, S0356
Capacidades	A0024, A0033, A0034, A0104, A0105, A0110, A0111, A0112, A0113, A0114, A0115, A0125

Nombre de la función laboral	**Promotor de planes de estudios de instrucción cibernética**
Id. de la función laboral	**OV-TEA-001**
Área de especialización	**Capacitación, educación y concientización (TEA)**
Categoría	**Supervisar y gobernar (OV)**
Descripción de la función laboral	Diseña, planifica, coordina y evalúa cursos, métodos y técnicas de capacitación y educación en cibernética según las necesidades didácticas.
Tareas	T0230, T0247, T0248, T0249, T0345, T0352, T0357, T0365, T0367, T0380, T0437, T0442, T0450, T0451, T0534, T0536, T0926
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0059, K0124, K0146, K0147, K0204, K0208, K0213, K0216, K0217, K0220, K0243, K0239, K0245, K0246, K0250, K0252, K0287, K0628
Habilidades	S0064, S0066, S0070, S0102, S0166, S0296
Capacidades	A0004, A0013, A0015, A0018, A0019, A0022, A0024, A0032, A0054, A0057, A0055, A0057, A0058, A0063, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171

Nombre de la función laboral	**Instructor de cibernética**
Id. de la función laboral	**OV-TEA-002**
Área de especialización	**Capacitación, educación y concientización (TEA)**
Categoría	**Supervisar y gobernar (OV)**
Descripción de la función laboral	Diseña e imparte la capacitación o la formación del personal en el campo de la cibernética.
Tareas	T0030, T0073, T0101, T0224, T0230, T0247, T0316, T0317, T0318, T0319, T0320, T0321, T0322, T0323, T0352, T0365, T0367, T0381, T0382, T0395, T0443, T0444, T0450, T0451, T0467, T0519, T0520, T0535, T0536, T0926
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0059, K0115, K0124, K0130, K0146, K0147, K0204, K0208, K0213, K0215, K0216, K0217, K0218, K0220, K0226, K0239, K0245, K0246, K0250, K0252, K0287, K0313, K0319, K0628
Habilidades	S0001, S0004, S0006, S0051, S0052, S0053, S0055, S0056, S0057, S0060, S0064, S0070, S0073, S0075, S0076, S0081, S0084, S0097, S0100, S0101, S0121, S0131, S0156, S0184, S0270, S0271, S0281, S0293, S0301, S0356, S0358
Capacidades	A0006, A0011, A0012, A0013, A0014, A0015, A0016, A0017, A0018, A0019, A0020, A0022, A0023, A0024, A0032, A0055, A0057, A0057, A0058, A0063, A0066, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171

Nombre de la función laboral	Administrador de seguridad de sistemas de información
Id. de la función laboral	OV-MGT-001
Área de especialización	Gestión de ciberseguridad (MGT)
Categoría	Supervisar y gobernar (OV)
Descripción de la función laboral	Se encarga de la ciberseguridad de un programa, organización, sistema o enclave.
Tareas	T0001, T0002, T0003, T0004, T0005, T0024, T0025, T0044, T0089, T0091, T0092, T0093, T0095, T0097, T0099, T0106, T0115, T0130, T0132, T0133, T0134, T0135, T0147, T0148, T0149, T0151, T0157, T0158, T0159, T0192, T0199, T0206, T0211, T0213, T0215, T0219, T0227, T0229, T0234, T0239, T0248, T0254, T0255, T0256, T0263, T0264, T0265, T0275, T0276, T0277, T0280, T0281, T0282
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0018, K0021, K0026, K0033, K0038, K0040, K0042, K0043, K0046, K0048, K0053, K0054, K0058, K0059, K0061, K0070, K0072, K0076, K0077, K0087, K0090, K0092, K0101, K0106, K0121, K0126, K0149, K0150, K0151, K0163, K0167, K0168, K0169, K0170, K0179, K0180, K0199, K0260, K0261, K0262, K0267, K0287, K0332, K0342, K0622, K0624
Habilidades	S0018, S0027, S0086
Capacidades	A0128, A0161, A0170

Nombre de la función laboral	Administrador de seguridad de las comunicaciones (COMSEC)
Id. de la función laboral	OV-MGT-002
Área de especialización	Gestión de ciberseguridad (MGT)
Categoría	Supervisar y gobernar (OV)
Descripción de la función laboral	Administra los recursos de seguridad de las comunicaciones (COMSEC) de una organización (instrucción 4009 del CNSS) o custodia las claves de un sistema de gestión de claves criptográficas (CKMS).
Tareas	T0003, T0004, T0025, T0044, T0089, T0095, T0099, T0215, T0229
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0026, K0038, K0042, K0090, K0101, K0121, K0126, K0163, K0267, K0285, K0287, K0622
Habilidades	S0027, S0059, S0138
Capacidades	A0162, A0163, A0164, A0165, A0166, A0167, A0168

Nombre de la función laboral	Organizador y administrador del personal de cibernética
Id. de la función laboral	OV-SPP-001
Área de especialización	Políticas y planificación estratégica (SPP)
Categoría	Supervisar y gobernar (OV)
Descripción de la función laboral	Formula planes, estrategias y orientación para el personal del ciberespacio a fin de satisfacer los requisitos de personal, capacitación y educación, y para adoptar los cambios de requisitos de políticas, doctrina, equipos, estructura del personal, educación y capacitación en materia de ciberespacio.
Tareas	T0001, T0004, T0025, T0044, T0074, T0094, T0099, T0116, T0222, T0226, T0341, T0352, T0355, T0356, T0362, T0363, T0364, T0365, T0368, T0369, T0372, T0373, T0374, T0375, T0376, T0384, T0387, T0388, T0390, T0391, T0408, T0425, T0429, T0437, T0441, T0445, T0472, T0481, T0505, T0506, T0529, T0533, T0536, T0537, T0552
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0072, K0101, K0127, K0146, K0147, K0168, K0169, K0204, K0215, K0233, K0234, K0241, K0243, K0309, K0311, K0313, K0335
Habilidades	S0108, S0128
Capacidades	A0023, A0028, A0033, A0037, A0042, A0053

Nombre de la función laboral	Planificador de políticas y estrategias cibernéticas
Id. de la función laboral	OV-SPP-002
Área de especialización	Políticas y planificación estratégica (SPP)
Categoría	Supervisar y gobernar (OV)
Descripción de la función laboral	Elabora y mantiene planes, estrategias y políticas de ciberseguridad para adoptar y alinear las iniciativas organizativas de ciberseguridad y de cumplimiento reglamentario.
Tareas	T0074, T0094, T0222, T0226, T0341, T0369, T0384, T0390, T0408, T0425, T0429, T0441, T0445, T0472, T0505, T0506, T0529, T0533, T0537
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0127, K0146, K0168, K0234, K0248, K0309, K0311, K0313, K0335, K0624
Habilidades	S0176, S0250
Capacidades	A0003, A0033, A0037

Nombre de la función laboral	**Director ejecutivo de cibernética**
Id. de la función laboral	**OV-EXL-001**
Área de especialización	**Dirección ejecutiva de cibernética (EXL)**
Categoría	**Supervisar y gobernar (OV)**
Descripción de la función laboral	Ejerce la autoridad para tomar decisiones y establece la visión y la dirección de los recursos o las operaciones de cibernética y afines a la cibernética de la organización.
Tareas	T0001, T0002, T0004, T0006, T0025, T0066, T0130, T0134, T0135, T0148, T0151, T0227, T0229, T0229, T0248, T0254, T0263, T0264, T0282, T0337, T0356, T0429, T0445, T0509, T0763, T0871, T0872, T0927, T0928
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0070, K0106, K0314, K0296, K0147, K0624, K0628
Habilidades	S0018, S0356, S0357, S0358, S0359
Capacidades	A0033, A0070, A0085, A0094, A0105, A0106, A0116, A0117, A0118, A0119, A0129, A0130, A0130

Nombre de la función laboral	**Administrador de programas**
Id. de la función laboral	**OV-PMA-001**
Área de especialización	**Gestión de programas, proyectos y adquisiciones (PMA)**
Categoría	**Supervisar y gobernar (OV)**
Descripción de la función laboral	Dirige, coordina, comunica, integra y rinde cuentas del éxito general del programa, facilitando su compatibilidad con las prioridades del organismo o la empresa.
Tareas	T0066, T0072, T0174, T0199, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0377, T0379, T0407, T0412, T0414, T0415, T0481, T0493, T0551
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0072, K0090, K0101, K0120, K0126, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270
Habilidades	S0038, S0372
Capacidades	A0009, A0039, A0045, A0056,

Nombre de la función laboral	**Administrador de proyectos de tecnología de la información (TI)**
Id. de la función laboral	**OV-PMA-002**
Área de especialización	**Gestión de programas, proyectos y adquisiciones (PMA)**
Categoría	**Supervisar y gobernar (OV)**
Descripción de la función laboral	Administra directamente los proyectos de tecnología de la información.
Tareas	T0072, T0174, T0196, T0199, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0340, T0354, T0370, T0377, T0379, T0389, T0394, T0407, T0412, T0414, T0415, T0481, T0493, T0551
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0012, K0043, K0047, K0048, K0059, K0072, K0090, K0101, K0120, K0126, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270
Habilidades	S0038, S0372
Capacidades	A0009, A0039, A0045, A0056

Nombre de la función laboral	**Administrador de soporte de productos**
Id. de la función laboral	**OV-PMA-003**
Área de especialización	**Gestión de programas, proyectos y adquisiciones (PMA)**
Categoría	**Supervisar y gobernar (OV)**
Descripción de la función laboral	Administra el paquete de funciones de soporte necesarias para establecer y mantener la preparación y la capacidad operativa de los sistemas y componentes.
Tareas	T0072, T0174, T0196, T0204, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0370, T0377, T0389, T0394, T0412, T0414, T0493, T0525, T0551, T0553
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0048, K0059, K0072, K0090, K0120, K0126, K0148, K0150, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0249, K0257, K0270
Habilidades	S0038, S0372
Capacidades	A0009, A0031, A0039, A0045, A0056

Nombre de la función laboral	**Administrador de inversiones y carteras de TI**
Id. de la función laboral	**OV-PMA-004**
Área de especialización	**Gestión de programas, proyectos y adquisiciones (PMA)**
Categoría	**Supervisar y gobernar (OV)**
Descripción de la función laboral	Gestiona una cartera de inversiones de TI que se ajuste a las necesidades generales de las prioridades de la empresa y la misión.
Tareas	T0220, T0223, T0277, T0302, T0377, T0415, T0493, T0551
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0072, K0120, K0126, K0146, K0154, K0165, K0169, K0235, K0257, K0270
Habilidades	S0372
Capacidades	A0039

Nombre de la función laboral	**Auditor de programas de TI**
Id. de la función laboral	**OV-PMA-005**
Área de especialización	**Gestión de programas, proyectos y adquisiciones (PMA)**
Categoría	**Supervisar y gobernar (OV)**
Descripción de la función laboral	Lleva a cabo evaluaciones de un programa de TI o de sus componentes individuales para determinar el cumplimiento con las normas publicadas.
Tareas	T0072, T0207, T0208, T0223, T0256, T0389, T0412, T0415
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0047, K0048, K0072, K0090, K0120, K0126, K0148, K0154, K0165, K0169, K0198, K0200, K0235, K0257, K0270
Habilidades	S0038, S0085, S0372
Capacidades	A0056

B.4 Proteger y defender (PR)

Nombre de la función laboral	**Analista de ciberdefensa**
Id. de la función laboral	**PR-CDA-001**
Área de especialización	**Análisis de la ciberdefensa (CDA)**
Categoría	**Proteger y defender (PR)**
Descripción de la función laboral	Usa los datos recolectados de una variedad de herramientas de ciberdefensa (por ejemplo, alertas del sistema de detección de intrusiones [IDS], firewalls , registros de tráfico de red) para analizar los eventos que ocurren dentro de sus entornos con el fin de mitigar amenazas.
Tareas	T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624
Habilidades	S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370
Capacidades	A0010, A0015, A0066, A0123, A0128, A0159

Nombre de la función laboral	**Especialista en soporte de la infraestructura de ciberdefensa**
Id. de la función laboral	**PR-INF-001**
Área de especialización	**Soporte de la infraestructura de ciberdefensa (INF)**
Categoría	**Proteger y defender (PR)**
Descripción de la función laboral	Pone a prueba, implementa, distribuye, mantiene y administra el hardware y el software de la infraestructura.
Tareas	T0042, T0180, T0261, T0335, T0348, T0420, T0438, T0483, T0486
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0033, K0042, K0044, K0058. K0061, K0062, K0104, K0106, K0135, K0157, K0179, K0205, K0258, K0274, K0324, K0332, K0334
Habilidades	S0007, S0053, S0054, S0059, S0077, S0079, S0121, S0124, S0367
Capacidades	A0123

Nombre de la función laboral	**Coordinador de la respuesta a incidentes de defensa de la ciberseguridad**
Id. de la función laboral	**PR-CIR-001**
Área de especialización	**Respuesta a incidentes (CIR)**
Categoría	**Proteger y defender (PR)**
Descripción de la función laboral	Investiga, analiza y responde a incidentes de ciberseguridad dentro del entorno o enclave de la red.
Tareas	T0041, T0047, T0161, T0163, T0164, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0395, T0503, T0510
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0026, K0033, K0034, K0041, K0042, K0046, K0058, K0062, K0070, K0106, K0157, K0161, K0162, K0167, K0177, K0179, K0221, K0230, K0259, K0287, K0332, K0565, K0624
Habilidades	S0003, S0047, S0077, S0078, S0079, S0080, S0173, S0365
Capacidades	A0121, A0128

Nombre de la función laboral	**Analista de evaluaciones de vulnerabilidades**
Id. de la función laboral	**PR-VAM-001**
Área de especialización	**Evaluación y gestión de vulnerabilidades (VAM)**
Categoría	**Proteger y defender (PR)**
Descripción de la función laboral	Lleva a cabo evaluaciones de sistemas y redes dentro del entorno o enclave de la red e identificar los puntos donde esos sistemas o redes se desvían de las configuraciones aceptables, las políticas locales o las del enclave. Mide la efectividad de la arquitectura de defensa en profundidad contra las vulnerabilidades conocidas.
Tareas	T0010, T0028, T0138, T0142, T0188, T0252, T0549, T0550
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0021, K0033, K0044, K0056, K0061, K0068, K0070, K0089, K0106, K0139, K0161, K0162, K0167, K0177, K0179, K0203, K0206, K0210, K0224, K0265, K0287, K0301, K0308, K0332, K0342, K0344, K0624
Habilidades	S0001, S0009, S0025, S0044, S0051, S0052, S0081, S0120, S0137, S0171, S0364, S0367
Capacidades	A0001, A0044, A0120, A0123

B.5 Analizar (AN)

Nombre de la función laboral	**Analista de amenazas y advertencias**
Id. de la función laboral	**AN-TWA-001**
Área de especialización	**Análisis de amenazas y advertencias (TWA)**
Categoría	**Analizar (AN)**
Descripción de la función laboral	Establece ciberindicadores para mantener la concientización del estado sumamente dinámico del entorno operativo. Recolecta, procesa, analiza y difunde evaluaciones de ciberamenazas o advertencias.
Tareas	T0569, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0660, T0685, T0687, T0707, T0708, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0783, T0785, T0786, T0792, T0800, T0805, T0834
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0349, K0362, K0377, K0392, K0395, K0405, K0409, K0415, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0471, K0480, K0499, K0511, K0516, K0556, K0560, K0561, K0565, K0603, K0604, K0610, K0612, K0614
Habilidades	S0194, S0196, S0203, S0211, S0218, S0227, S0228, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303
Capacidades	A0013, A0066, A0072, A0080, A0082, A0083, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109

Nombre de la función laboral	**Analista de explotaciones**
Id. de la función laboral	**AN-EXP-001**
Área de especialización	**Análisis de explotación (EXP)**
Categoría	**Analizar (AN)**
Descripción de la función laboral	Colabora para identificar las deficiencias en el acceso y la recolección que se puedan corregir por medio de actividades de recolección o preparación cibernéticas. Aprovecha todo recurso y técnica analítica autorizados para penetrar en las redes seleccionadas como objetivo.
Tareas	T0028, T0266, T0570, T0572, T0574, T0591, T0600, T0603, T0608, T0614, T0641, T0695, T0701, T0720, T0727, T0736, T0738, T0754, T0775, T0777
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0131, K0142, K0143, K0177, K0224, K0349, K0362, K0417, K0444, K0471, K0560, K0351, K0354, K0368, K0371, K0376, K0379, K0388, K0393, K0394, K0397, K0418, K0430, K0443, K0447, K0451, K0470, K0473, K0484, K0487, K0489, K0509, K0510, K0523, K0529, K0535, K0544, K0557, K0559, K0608
Habilidades	S0066, S0184, S0199, S0200, S0201, S0204, S0207, S0214, S0223, S0236, S0237, S0239, S0240, S0245, S0247, S0258, S0260, S0264, S0269, S0279, S0286, S0290, S0294, S0300
Capacidades	A0013, A0066, A0080, A0084, A0074, A0086, A0092, A0093, A0104

Nombre de la función laboral	**Analista de todas las fuentes**
Id. de la función laboral	**AN-ASA-001**
Área de especialización	**Análisis de todas las fuentes (ASA)**
Categoría	**Analizar (AN)**
Descripción de la función laboral	Analiza datos o información de una o varias fuentes para llevar a cabo la preparación del entorno, responder a las solicitudes de información y presentar los requisitos de recolección de inteligencia y producción compatibles con la planificación y las operaciones.
Tareas	T0569, T0582, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0642, T0660, T0678, T0685, T0686, T0687, T0707, T0708, T0710, T0713, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0771, T0782, T0783, T0785, T0786, T0788, T0789, T0792, T0797, T0800, T0805, T0834
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0221, K0349, K0357, K0362, K0377, K0392, K0395, K0405, K0409, K0410, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449 K0457, K0458, K0460, K0464, K0465, K0469, K0471, K0480, K0507, K0511, K0516, K0533, K0542, K0549, K0551, K0556, K0560, K0561, K0565, K0577, K0598, K0603, K0604, K0610, K0612, K0614
Habilidades	S0194, S0203, S0211, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303, S0189, S0254, S0360
Capacidades	A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0085, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0108, A0109

Nombre de la función laboral	**Especialista en evaluaciones de misiones**
Id. de la función laboral	**AN-ASA-002**
Área de especialización	**Análisis de todas las fuentes (ASA)**
Categoría	**Analizar (AN)**
Descripción de la función laboral	Elabora planes de evaluación y medidas del rendimiento o la efectividad. Lleva a cabo evaluaciones estratégicas y operativas de la efectividad según sea necesario para los eventos cibernéticos. Determina si los sistemas funcionan según lo previsto y aporta información para determinar la efectividad operativa.
Tareas	T0582, T0583, T0585, T0586, T0588, T0589, T0593, T0597, T0611, T0615, T0617, T0624, T0660, T0661, T0663, T0678, T0684, T0685, T0686, T0707, T0718, T0748, T0749, T0752, T0758, T0761, T0782, T0783, T0785, T0786, T0788, T0789, T0793, T0797, T0834
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0349, K0362, K0377, K0392, K0395, K0405, K0409, K0410, K0414, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0457, K0460, K0464, K0465, K0469, K0471, K0480, K0507, K0511, K0516, K0549, K0551, K0556, K0560, K0561, K0565, K0598, K0603, K0604, K0610, K0612, K0614

Habilidades	S0189, S0194, S0203, S0211, S0216, S0218, S0227, S0228, S0229, S0249, S0254, S0256, S0271, S0278, S0285, S0288, S0289, S0292, S0296, S0297, S0303, S0360
Capacidades	A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109, A0085, A0108

Nombre de la función laboral	**Desarrollador de objetivos**
Id. de la función laboral	**AN-TGT-001**
Área de especialización	**Objetivos (TGT)**
Categoría	**Analizar (AN)**
Descripción de la función laboral	Efectúa análisis de sistemas de objetivos, establece o mantiene carpetas electrónicas de objetivos que incluyan las aportaciones hechas a la preparación de entornos o las fuentes de inteligencia internas o externas. Se coordina con las organizaciones de inteligencia y actividades de objetivos de los socios, y presenta los objetivos candidatos a investigación y validación.
Tareas	T0597, T0617, T0707, T0582, T0782, T0797, T0588, T0624, T0661, T0663, T0684, T0642, T0710, T0561, T0594, T0599, T0633, T0650, T0652, T0688, T0717, T0731, T0744, T0769, T0770, T0776, T0781, T0790, T0794, T0798, T0799, T0802, T0815, T0824, T0835
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0142, K0177, K0349, K0351, K0357, K0362, K0379, K0381, K0392, K0395, K0402, K0409, K0413, K0417,K0426, K0427, K0431, K0436, K0437, K0439, K0440, K0444, K0445, K0446, K0449, K0457, K0458, K0460, K0461, K0464, K0465, K0466, K0471, K0473, K0478, K0479, K0497, K0499, K0507, K0516, K0533, K0542, K0543, K0546, K0547, K0549, K0551, K0555, K0556, K0560 K0561, K0565, K0598, K0603, K0604, K0614
Habilidades	S0194, S0203, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0189, S0228, S0216, S0292, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0302, S0360, S0361
Capacidades	A0013, A0066, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073

Nombre de la función laboral	**Analista de redes de objetivos**
Id. de la función laboral	**AN-TGT-002**
Área de especialización	**Objetivos (TGT)**
Categoría	**Analizar (AN)**
Descripción de la función laboral	Lleva a cabo análisis avanzados de recolección y datos de código abierto para lograr la continuidad de objetivos, generar perfiles de objetivos y sus actividades, y establecer técnicas para obtener más información sobre objetivos. Determina la manera en que los objetivos se comunican, desplazan, operan y viven en función del conocimiento de sus tecnologías y redes digitales, y las aplicaciones sobre estos.

Tareas	T0617, T0707, T0582, T0797, T0624, T0710, T0599, T0650, T0802, T0595, T0606, T0607, T0621, T0653, T0692, T0706, T0715, T0722, T0745, T0765, T0767, T0778, T0803, T0807
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0177, K0349, K0362, K0444, K0471, K0392, K0395, K0431, K0436, K0440, K0445, K0449, K0516, K0379, K0473, K0413, K0439, K0479, K0547, K0487, K0544, K0559, K0389, K0403, K0424, K0442, K0462, K0472, K0483, K0499, K0500, K0520, K0550, K0567, K0592, K0599, K0600
Habilidades	S0194, S0203, S0229, S0256, S0228, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0177, S0178, S0181, S0183, S0191, S0197, S0217, S0219, S0220, S0225, S0231, S0234, S0244, S0246, S0259, S0261, S0262, S0263, S0268, S0277, S0280, S0291, S0301
Capacidades	A0013, A0066, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073

Nombre de la función laboral	**Analista lingüístico multidisciplinario**
Id. de la función laboral	**AN-LNG-001**
Área de especialización	**Análisis lingüístico (LNG)**
Categoría	**Analizar (AN)**
Descripción de la función laboral	Aplica la experiencia lingüística y cultural, junto con conocimientos técnicos y sobre amenazas u objetivos, para procesar, analizar o difundir información de inteligencia proveniente de material lingüístico, gráfico o de voz. Establece y mantiene bases de datos y ayudas de trabajo específicas del idioma para facilitar la ejecución de acciones cibernéticas y lograr el intercambio de conocimientos críticos. Aporta experiencia en el tema a proyectos interdisciplinarios o con uso intensivo de idiomas extranjeros.
Tareas	T0650, T0606, T0715, T0745, T0761, T0837, T0838, T0839, T0840, T0841, T0842, T0843, T0844, T0845, T0846, T0847, T0848, T0849, T0850, T0851, T0852, T0853, T0854, T0855, T0856, T0857, T0858, T0859, TO860
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0143, K0177, K0431, K0449, K0413, K0487, K0462, K0520, K0550, K0567, K0599, K0600, K0417, K0377, K0356, K0359, K0391, K0396, K0398, K0407, K0416, K0476, K0488, K0491, K0493, K0499, K0524, K0532, K0539, K0540, K0541, K0545, K0548, K0564, K0571, K0574, K0579, K0596, K0606, K0607
Habilidades	S0187, S0217, S0244, S0259, S0262, S0277, S0218, S0184, S0290, S0179, S0188, S0193, S0195, S0198, S0210, S0212, S0215, S0224, S0226, S0232, S0233, S0235, S0241, S0251, S0253, S0265, S0283, S0284
Capacidades	A0013, A0089, A0071, A0103

B.6 Recolectar y operar (CO)

Nombre de la función laboral	**Administrador de recolección de todas las fuentes**
Id. de la función laboral	**CO-CLO-001**
Área de especialización	**Operaciones de recolección (CLO)**
Categoría	**Recolectar y operar (CO)**
Descripción de la función laboral	Identifica las autoridades y el entorno de recolección, incorpora los requisitos de información prioritarios en la gestión de la recolección y establece conceptos para lograr los objetivos de la dirección. Determina las capacidades de los recursos de recolección disponibles, define nuevas capacidades de recolección y elabora y difunde planes de recolección. Vigila la ejecución de la tarea asignada de recolección para lograr la ejecución efectiva del plan de recolección.
Tareas	T0562, T0564, T0568, T0573, T0578, T0604, T0605, T0625, T0626, T0631, T0632, T0634, T0645, T0646, T0647, T0649, T0651, T0657, T0662, T0674, T0681, T0683, T0698, T0702, T0714, T0716, T0721, T0723, T0725, T0734, T0737, T0750, T0753, T0755, T0757, T0773, T0779, T0806, T0809, T0810, T0811, T0812, T0814, T0820, T0821, T0827
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0109, K0177, K0431, K0449, K0417, K0579, K0596, K0444, K0471, K0392, K0395, K0440, K0445, K0516, K0560, K0427, K0446, K0561, K0565, K0405, K0480, K0610, K0612, K0353, K0361, K0364, K0380, K0382, K0383, K0386, K0387, K0390, K0401, K0404, K0412, K0419, K0425, K0435, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0482, K0492, K0495, K0496, K0498, K0503, K0505, K0513, K0521, K0522, K0526, K0527, K0552, K0553, K0554, K0558, K0562, K0563, K0569, K0570, K0580, K0581, K0583, K0584, K0587, K0588, K0601, K0605, K0613
Habilidades	S0238, S0304, S0305, S0311, S0313, S0316, S0317, S0324, S0325, S0327, S0328, S0330, S0332, S0334, S0335, S0336, S0339, S0342, S0344, S0347, S0351, S0352, S0362
Capacidades	A0069, A0070, A0076, A0078, A0079

Nombre de la función laboral	Administrador de requisitos de recolección de todas las fuentes
Id. de la función laboral	CO-CLO-002
Área de especialización	Operaciones de recolección (CLO)
Categoría	Recolectar y operar (CO)
Descripción de la función laboral	Evalúa las operaciones de recolección y elabora estrategias para los requisitos de recolección en función de los efectos utilizando las fuentes y los métodos disponibles para mejorar la recolección. Elabora, procesa, valida y coordina la presentación de los requisitos de recolección. Evalúa el rendimiento de los recursos de recolección y las operaciones de recolección.
Tareas	T0564, T0568, T0578, T0605, T0651, T0714, T0725, T0734, T0809, T0810, T0811, T0565, T0577, T0580, T0596, T0602, T0613, T0668, T0673, T0675, T0682, T0689, T0693, T0694, T0730, T0746, T0780, T0819, T0822, T0830, T0831, T0832, T0833
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0109, K0177, K0353, K0361, K0364, K0380, K0382, K0383, K0384, K0386, K0387, K0390, K0395, K0401, K0404, K0412, K0417, K0419, K0421, K0425, K0427, K0431, K0435, K0444, K0445, K0446, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0480, K0482, K0492, K0495, K0496, K0498, K0505, K0513, K0516, K0521, K0526, K0527, K0552, K0554, K0558, K0560, K0561, K0562, K0563, K0565, K0568, K0569, K0570, K0579, K0580, K0581, K0584, K0587, K0588, K0596, K0605, K0610, K0612
Habilidades	S0304, S0305, S0316, S0317, S0327, S0330, S0334, S0335, S0336, S0339, S0344, S0347, S0352, S0329 S0337, S0346, S0348, S0353, S0362
Capacidades	A0069, A0070, A0078

Nombre de la función laboral	**Planificador de ciberinteligencia**
Id. de la función laboral	**CO-OPL-001**
Área de especialización	**Planificación ciberoperativa (OPL)**
Categoría	**Recolectar y operar (CO)**
Descripción de la función laboral	Elabora planes de inteligencia detallados para satisfacer los requisitos de las ciberoperaciones. Colabora con los planificadores de las ciberoperaciones para identificar, validar e imponer requisitos de recolección y análisis. Participa en la selección, validación y sincronización de objetivos, y en la ejecución de acciones cibernéticas. Sincroniza las actividades de inteligencia para lograr los objetivos de la organización en el ciberespacio.
Tareas	T0734, T0563, T0575, T0576, T0579, T0581, T0587, T0590, T0592, T0601, T0627, T0628, T0630, T0636, T0637, T0638, T0639, T0640, T0648, T0656, T0659, T0667, T0670, T0676, T0680, T0690, T0691, T0705, T0709, T0711, T0719, T0726, T0728, T0733, T0735, T0739, T0743, T0760, T0763, T0772, T0784, T0801, T0808, T0816, T0836
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0108, K0109, K0120, K0431, K0417, K0444, K0395, K0445, K0560, K0427, K0446, K0561, K0565, K0480, K0610, K0612, K0435, K0471, K0392, K0440, K0405, K0377, K0349, K0362, K0436, K0379, K0403, K0460, K0464, K0556, K0603, K0614, K0465, K0507, K0598, K0511, K0414, K0577, K0347, K0350, K0352, K0355, K0358, K0399, K0400, K0408, K0411, K0422, K0432, K0455, K0456, K0459, K0463, K0494, K0499, K0501, K0502, K0504, K0506, K0508, K0512, K0514, K0517, K0518, K0519, K0525, K0538, K0566, K0572, K0575, K0578, K0582, K0585, K0586, K0589, K0590, K0591, K0593, K0594, K0595, K0599, K0602
Habilidades	S0218, S0203, S0249, S0278, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0272, S0273, S0306, S0307, S0308, S0309, S0310, S0312, S0314, S0315, S0318, S0319, S0320, S0321, S0322, S0323, S0331, S0333, S0338, S0340, S0341, S0343, S0345, S0350, S0360
Capacidades	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105, A0160

Nombre de la función laboral	**Planificador de ciberoperaciones**
Id. de la función laboral	**CO-OPL-002**
Área de especialización	**Planificación ciberoperativa (OPL)**
Categoría	**Recolectar y operar (CO)**
Descripción de la función laboral	Elabora planes detallados para llevar a cabo o respaldar la gama aplicable de ciberoperaciones mediante la colaboración con otros planificadores, operadores o analistas. Participa en la selección, validación y sincronización de objetivos, y facilita la integración durante la ejecución de acciones cibernéticas.
Tareas	T0734, T0563, T0579, T0581, T0592, T0627, T0628, T0640, T0648, T0667, T0670, T0680, T0690, T0719, T0733, T0739, T0743, T0763, T0772, T0801, T0836, T0571, T0622, T0635, T0654, T0655, T0658, T0665, T0672, T0679, T0699, T0703, T0704, T0732, T0741, T0742, T0747, T0764, T0787, T0791, T0795, T0813, T0823
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0108, K0109, K0347, K0349, K0350, K0352, K0362, K0377, K0379, K0392, K0395, K0399, K0400, K0403, K0408, K0411, K0414, K0417, K0422, K0431, K0432, K0435, K0436, K0444, K0445, K0446, K0455, K0464, K0465, K0471, K0480, K0494, K0497, K0499, K0501, K0502, K0504, K0506, K0507, K0508, K0511, K0512, K0514, K0516, K0518, K0519, K0525, K0534, K0538, K0556, K0560, K0561, K0565 K0566, K0572, K0576, K0582, K0585, K0586, K0589, K0590, K0593, K0594, K0597, K0598, K0599, K0603, K0610, K0612, K0614
Habilidades	S0218, S0249, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0273, S0309, S0312, S0322, S0333, S0209, S0326, S0349, S0360
Capacidades	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

Nombre de la función laboral	**Planificador de la integración de los socios**
Id. de la función laboral	**CO-OPL-003**
Área de especialización	**Planificación ciberoperativa (OPL)**
Categoría	**Recolectar y operar (CO)**
Descripción de la función laboral	Trabaja para promover la cooperación entre los socios de las ciberoperaciones a través de las fronteras organizativas o nacionales. Contribuye a la integración de los equipos cibernéticos de socios ofreciendo orientación, recursos y colaboración para establecer las mejores prácticas y facilitar el respaldo organizativo a fin de lograr los objetivos de las acciones cibernéticas integradas.
Tareas	T0581, T0582, T0627, T0670, T0739, T0763, T0772, T0836, T0571, T0635, T0665, T0699, T0732, T0747, T0764, T0787, T0795, T0823, T0601, T0760, T0784, T0629, T0666, T0669, T0671, T0700, T0712, T0729, T0759, T0766, T0817, T0818, T0825, T0826

Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0431, K0417, K0444, K0395, K0435, K0392, K0377, K0362, K0436, K0379, K0403, K0465, K0507, K0598, K0511, K0414, K0350, K0400, K0408, K0411, K0422, K0432, K0455, K0499, K0501, K0504, K0506, K0508, K0512, K0514, K0538, K0585, K0599
Habilidades	S0218, S0249, S0296, S0297, S0185, S0186, S0213, S0250, S0326, S0360
Capacidades	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

Nombre de la función laboral	**Ciberoperador**
Id. de la función laboral	**CO-OPS-001**
Área de especialización	**Ciberoperaciones (OPS)**
Categoría	**Recolectar y operar (CO)**
Descripción de la función laboral	Lleva a cabo la recolección, procesamiento o geolocalización de sistemas para aprovechar las vulnerabilidades, ubicar o dar seguimiento a los objetivos de interés. Efectúa navegación de redes y análisis forenses tácticos y, cuando se le ordena, ejecuta operaciones en las redes.
Tareas	T0566, T0567, T0598, T0609, T0610, T0612, T0616, T0618, T0619, T0620, T0623, T0643, T0644, T0664, T0677, T0696, T0697, T0724, T0740, T0756, T0768, T0774, T0796, T0804, T0828, T0829
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0021, K0051, K0109, K0142, K0224, K0363, K0372, K0373, K0375, K0379, K0403, K0406, K0420, K0423, K0428, K0427, K0429, K0430, K0433, K0438, K0440, K0452, K0468, K0481, K0485, K0486, K0480, K0516, K0528, K0530, K0531, K0536, K0560, K0565, K0573, K0608, K0609
Habilidades	S0062, S0183, S0236, S0182, S0190, S0192, S0202, S0206, S0221, S0242, S0243, S0252, S0255, S0257, S0266, S0267, S0270, S0275, S0276, S0281, S0282, S0293, S0295, S0298, S0299, S0363
Capacidades	A0095, A0097, A0099, A0100

B.7 Investigar (IN)

Nombre de la función laboral	**Investigador de ciberdelitos**
Id. de la función laboral	**IN-INV-001**
Área de especialización	**Ciberinvestigación (INV)**
Categoría	**Investigar (IN)**
Descripción de la función laboral	Identifica, recolecta, analiza y preserva pruebas utilizando técnicas analíticas y de investigación controladas y documentadas.
Tareas	[**Nota**: Algunas de estas actividades solo pueden ser llevadas a cabo por personal con autoridad policial o de contrainteligencia]. T0031, T0059, T0096, T0103, T0104, T0110, T0112, T0113, T0114, T0120, T0193, T0225, T0241, T0343, T0346, T0360, T0386, T0423, T0430, T0433, T0453, T0471, T0479, T0523
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0046, K0070, K0107, K0110, K0114, K0118, K0123, K0125, K0128, K0144, K0155, K0156, K0168, K0209, K0231, K0244, K0251, K0351, K0624
Habilidades	S0047, S0068, S0072, S0086
Capacidades	A0174, A0175

Nombre de la función laboral	**Analista forense policial y de contrainteligencia**
Id. de la función laboral	**IN-FOR-001**
Área de especialización	**Investigación forense digital (FOR)**
Categoría	**Investigar (IN)**
Descripción de la función laboral	Lleva a cabo investigaciones a fondo sobre delitos informáticos estableciendo pruebas documentales o físicas, incluidos los medios y registros digitales asociados con incidentes de ciberintrusiones.
Tareas	T0027, T0036, T0048, T0075, T0087, T0103, T0113, T0120, T0165, T0167, T0168, T0172, T0173, T0179, T0182, T0190, T0193, T0212, T0216, T0238, T0240, T0241, T0246, T0253, T0285, T0286, T0287, T0288, T0289, T0432, T0439, T0471, T0532
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0021, K0042, K0060, K0070, K0077, K0078, K0107, K0109, K0117, K0118, K0119, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0134, K0145, K0155, K0156, K0167, K0168, K0179, K0182, K0183, K0184, K0185, K0186, K0187, K0188, K0189, K0305, K0624
Habilidades	S0032, S0046, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093
Capacidades	A0005, A0175

Nombre de la función laboral	**Analista forense de ciberdefensa**
Id. de la función laboral	**IN-FOR-002**
Área de especialización	**Investigación forense digital (FOR)**
Categoría	**Investigar (IN)**
Descripción de la función laboral	Analiza pruebas digitales e investiga incidentes de seguridad informática para obtener información útil compatible con la mitigación de vulnerabilidades del sistema o la red.
Tareas	T0027, T0036, T0048, T0049, T0075, T0087, T0103, T0113, T0165, T0167, T0168, T0172, T0173, T0175, T0179, T0182, T0190, T0212, T0216, T0238, T0240, T0241, T0253, T0279, T0285, T0286, T0287, T0288, T0289, T0312, T0396, T0397, T0398, T0399, T0400, T0401, T0432, T0532, T0546
Conocimientos	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0042, K0060, K0070, K0077, K0078, K0109, K0117, K0118, K0119, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0134, K0145, K0155, K0156, K0167, K0168, K0179, K0182, K0183, K0184, K0185, K0186, K0187, K0188, K0189, K0224, K0254, K0255, K0301, K0304, K0347, K0624
Habilidades	S0032, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093, S0131, S0132, S0133, S0156
Capacidades	A0005, A0043

Apéndice C: Recursos para la formación del personal

C.1 Conjunto de herramientas para la formación del personal de ciberseguridad del DHS

El Conjunto de herramientas para la formación del personal de ciberseguridad (CWDT, por sus siglas en inglés) del DHS [8] ayuda a las organizaciones a entender sus necesidades de personal de ciberseguridad y de dotación de personal para proteger su información, clientes y redes. Este conjunto de herramientas incluye plantillas para trayectorias profesionales en ciberseguridad y recursos para captar, contratar y retener a los mejores talentos en el campo de la ciberseguridad. El CWDT proporciona herramientas de ayuda para conocer los riesgos del personal de ciberseguridad de una organización y hacer un inventario de ese personal. Además, aprovecha las áreas de especialización, los conocimientos, habilidades y capacidades (CHC) y las tareas del Marco de la NICE. El CWDT señala que el primer paso para preparar la formación del personal de ciberseguridad es tener una visión común para organizar ese personal. Una visión común ayuda a los directores en su respuesta a los entornos cambiantes, y proporciona datos para ajustar mejor los recursos, observar las tendencias laborales y resaltar las áreas de riesgo potencial. Este conocimiento es especialmente importante en el entorno en evolución continua de la ciberseguridad. El CWDT incluye un Modelo de madurez de capacidades (CMM, por sus siglas en inglés) para la planificación del personal de ciberseguridad, es decir, un recurso de autoevaluación que ayuda a determinar la madurez de la capacidad de una organización para planificar su personal de ciberseguridad.

El CWDT incluye perfiles de guía orientados a la retención del personal en todo nivel, sean profesionales en ciberseguridad principiantes, intermedios o expertos.

C.1.1 Niveles de competencia y trayectorias profesionales

Cuando se diseñan las trayectorias profesionales y se dan a conocer a los empleados, estos pueden identificar sus niveles de competencia y avanzar en el campo de la ciberseguridad.

El CWDT consta de un proceso de tres pasos para establecer las trayectorias profesionales de ciberseguridad en la propia organización.

- Paso 1: Familiarizarse con los niveles de competencia y estudiar ejemplos de trayectorias profesionales.
- Paso 2: Usar una plantilla del CWDT para diseñar trayectorias profesionales de ciberseguridad específicas y adaptadas a la organización, completando las secciones "*Experiencias y credenciales sugeridas*", "*Competencias y ejemplos de habilidades y CHC*" y "*Actividades de capacitación y formación sugeridas*".
- Paso 3: Comunicar las trayectorias profesionales a los administradores y el personal de ciberseguridad.

C.2 Herramienta Baldrige Cybersecurity Excellence Builder

Una vez que una organización haya determinado sus requisitos de ciberseguridad (por ejemplo, mediante una auditoría de ciberseguridad o una autoevaluación interna), puede hacer referencia al Marco de la NICE para precisar las funciones laborales y las tareas que servirán para cumplir esos requisitos. Aun cuando se han usado históricamente términos generales como "profesionales cibernéticos" para medir las necesidades, la especificidad del Marco de la NICE ofrece un método mejor para describir decenas de las funciones laborales individuales que se necesitan. Al determinar las competencias requeridas y disponibles, y al detectar las deficiencias entre las habilidades necesarias y las disponibles, la organización puede definir sus necesidades críticas. El Marco de la NICE ayuda a una organización a responder a las siguientes preguntas (extraídas del programa Baldrige Cybersecurity Excellence Builder [9], para la excelencia en la ciberseguridad) sobre el mantenimiento de un entorno de trabajo efectivo y propicio para lograr sus metas de ciberseguridad:

- ¿Cómo evalúa las necesidades de competencias y capacidades de su personal relacionadas con la ciberseguridad?
- ¿Cómo organiza y gestiona a su personal de ciberseguridad para establecer funciones y responsabilidades?
- ¿Cómo prepara a su personal para las necesidades cambiantes de competencias y capacidades en el campo de la ciberseguridad?

A medida que más organizaciones evalúen a su personal de ciberseguridad, el léxico común del Marco de la NICE facilitará la evaluación de capacidades y competencias en muchas organizaciones, sectores industriales y regiones.

C.3 Herramienta para redactar descripciones de puestos

La herramienta PushbuttonPD™ de la Iniciativa de ayuda a la gestión de habilidades cibernéticas del DHS [10] permite que los administradores, supervisores y especialistas en RR. HH. redacten con rapidez una descripción de puestos (DP) para los empleados federales sin necesidad de capacitación extensa ni conocimiento previo de la clasificación de puestos. La herramienta está diseñada para presentar la terminología, proveniente de varias fuentes y normas autoritativas y críticas para la misión, que se emplea al describir las responsabilidades, tareas y conocimientos, habilidades y capacidades, y capturar de inmediato los requisitos del funcionario de contratación para presentarlos en un paquete sólido de contratación que se puede integrar fácilmente en los procesos existentes de RR. HH. del organismo. Las organizaciones pueden probar la herramienta PushbuttonPD™ y observar cómo extrae y presenta el material del Marco de la NICE en la descripción de un puesto.

Apéndice D: Referencia cruzada a documentos de orientación y directrices

La tercera meta estratégica de la NICE, Guiar la formación profesional y la planificación del personal, tiene por objeto que los empleadores consideren las demandas del mercado y mejoren la captación, contratación, formación y retención de talentos de ciberseguridad. Un objetivo dentro de esta meta estratégica es publicar y promover el conocimiento del Marco de la NICE y su adopción. En este caso, adopción se refiere a usar el Marco de la NICE como recurso de referencia para las acciones relacionadas con el personal, la capacitación y la educación en materia de ciberseguridad.

Una forma de fomentar la adopción del Marco de la NICE es promover que los autores de documentos de orientación y directrices de ciberseguridad hagan una referencia cruzada de parte del contenido de esos documentos a los componentes del Marco de la NICE. El Apéndice D incluye ejemplos de referencias cruzadas de publicaciones que podrían impulsar la adopción del Marco de la NICE.

D.1 Marco de ciberseguridad

En 2014, el NIST publicó el Marco para el mejoramiento de la ciberseguridad en infraestructuras críticas [11], conocido comúnmente como el Marco de ciberseguridad. El Marco de ciberseguridad, creado en respuesta a la Orden ejecutiva (OE) 13636 [12], proporciona un método rentable basado en el desempeño para ayudar a las organizaciones a identificar, evaluar y gestionar el riesgo a la ciberseguridad. Fue elaborado por medio de una serie de talleres públicos convocados por el NIST para entender mejor las normas y metodologías que contribuyen a lograr una gestión efectiva de los riesgos y la manera en que podrían implementarse las buenas prácticas voluntarias existentes a fin de mejorar la ciberseguridad.

La *Hoja de ruta del NIST para mejorar la ciberseguridad en infraestructuras críticas* [13] es un documento complementario del Marco de ciberseguridad que señala la necesidad de personal de ciberseguridad capacitado para satisfacer las necesidades especiales de ciberseguridad de la infraestructura crítica. La hoja reconoce que, a medida que evolucionan los entornos de amenaza y tecnología de la ciberseguridad, el personal debe seguir adaptándose para diseñar, desarrollar, implementar, mantener y mejorar constantemente las prácticas necesarias para la ciberseguridad.

El Marco de ciberseguridad se compone de tres partes: el Núcleo, los Niveles de implementación y los Perfiles. Cada componente del Marco de ciberseguridad refuerza la conexión entre los impulsores empresariales y las actividades de ciberseguridad. Los elementos del Núcleo del Marco funcionan en conjunto de la manera siguiente:

- Las **Funciones** organizan las actividades básicas de ciberseguridad en su nivel más alto. Estas Funciones (Identificar, Proteger, Detectar, Responder y Recuperar) se describen en detalle más adelante.
- Las **Categorías** son las subdivisiones de una Función en grupos de resultados de ciberseguridad estrechamente vinculados con las necesidades y actividades programáticas.

- Las **Subcategorías** dividen aún más una Categoría en resultados específicos de actividades técnicas o de gestión. Proporcionan un conjunto de resultados que, aunque no son exhaustivos, contribuyen al logro de los resultados en cada Categoría.
- Las **referencias informativas** son secciones específicas de normas, directrices y prácticas comunes entre los sectores críticos de la infraestructura, y muestran un método para lograr los resultados asociados con cada Subcategoría. Las referencias informativas que se presentan en el Núcleo del Marco sirven de ejemplo, mas no son exhaustivas. Representan la orientación entre sectores más consultada durante el proceso de elaboración del Marco.

Cada una de las Funciones del Núcleo contribuye a un conocimiento de alto nivel de las necesidades de ciberseguridad de la organización:

- **Identificar (ID)**: Define el conocimiento organizativo para gestionar el riesgo a la ciberseguridad de los sistemas, recursos, datos y capacidades.
- **Proteger (PR)**: Establece e implementa las debidas salvaguardias para asegurar la prestación de servicios de infraestructura críticos.
- **Detectar (DE)**: Establece e implementa actividades apropiadas para detectar la ocurrencia de un evento de ciberseguridad.
- **Responder (RS)**: Establece e implementa las actividades correspondientes para tomar medidas en relación con un evento de ciberseguridad detectado.
- **Recuperar (RC)**: Establece e implementa actividades apropiadas para mantener los planes de resiliencia y restaurar las capacidades o los servicios que se hayan visto afectados debido a un evento de ciberseguridad.

Estas funciones se correlacionan de muchas maneras con las Categorías del Marco de la NICE. En la Tabla 8, se describen las relaciones entre las Funciones del Marco de ciberseguridad y las Categorías del Marco de la NICE.

Tabla 8: Correspondencia entre las Categorías de personal del Marco de la NICE y las Funciones del Marco de ciberseguridad

Categoría del Marco de la NICE	Descripción de la Categoría	Funciones afines del Marco de ciberseguridad
Suministrar protección (SP)	Conceptualiza, diseña o establece sistemas seguros de tecnología de la información (TI), asumiendo la responsabilidad de los aspectos de la organización de sistemas o de redes.	Identificar (ID), Proteger (PR)
Operar y mantener (OM)	Proporciona la gestión y el mantenimiento necesarios para lograr que el funcionamiento y la seguridad del sistema de tecnología de la información (TI) sean efectivos y eficientes.	Proteger (PR), Detectar (DE)
Supervisar y gobernar (OV)	Ofrece liderazgo, gestión, dirección o desarrollo y promoción para que la organización pueda llevar a cabo con efectividad el trabajo de ciberseguridad.	Identificar (ID), Proteger (PR), Detectar (DE), Recuperar (RC)
Proteger y defender (PR)	Identifica, analiza y mitiga las amenazas a los sistemas o las redes de tecnología de la información (TI) internos.	Proteger (PR), Detectar (DE), Responder (RS)
Analizar (AN)	Hace revisiones y evaluaciones muy especializadas de la información entrante sobre ciberseguridad a fin de determinar su utilidad para inteligencia.	Identificar (ID), Detectar (DE), Responder (RS)
Recolectar y operar (CO)	Efectúa operaciones especializadas de negación y engaño, y de recolección de información sobre ciberseguridad que pueda ser usada para generar inteligencia.	Detectar (DE), Proteger (PR), Responder (RS)
Investigar (IN)	Investiga los eventos de ciberseguridad o los delitos relacionados con sistemas, redes y pruebas digitales de tecnología de la información (TI).	Detectar (DE), Responder (RS), Recuperar (RC)

D.1.2 Ejemplo de la integración del Marco de la ciberseguridad con el Marco de la NICE

El Marco de ciberseguridad y el Marco de la NICE se elaboraron por separado; sin embargo, se complementan entre sí con la descripción de un método jerárquico para lograr las metas de ciberseguridad, como se muestra en el ejemplo siguiente:

La función **Responder** del Marco de ciberseguridad incluye una Categoría **Mitigación (RS.MI)**. Esta Categoría incluye una Subcategoría **RS.MI-2** que señala el resultado de "Los incidentes son mitigados". El Marco de ciberseguridad describe este resultado y ofrece varias referencias informativas acerca de los controles de seguridad para lograrlo; no obstante, este marco no

proporciona ninguna guía informativa acerca de la persona que debe tener la responsabilidad de lograr el resultado, ni de los conocimientos, habilidades o capacidades que se aplicarían.

Al revisar el Marco de la NICE, identificamos la función **Coordinador de la respuesta a incidentes de defensa de la ciberseguridad (PR-CIR-001)** en la Categoría **Proteger y defender (PR)** del área de especialización **Respuesta a incidentes (CIR)**. Podemos revisar la descripción de esta función para verificar que se ajusta al resultado **RS.MI-2** del Marco de ciberseguridad:

> Responde a interrupciones dentro del dominio pertinente para mitigar amenazas inmediatas y potenciales. Utiliza métodos de mitigación, preparación, respuesta y recuperación para maximizar la supervivencia, la preservación de la propiedad y la seguridad de la información. Investiga y analiza las actividades de respuesta pertinentes y evalúa la efectividad y los mejoramientos de las prácticas existentes.
>
> Investiga, analiza y responde a incidentes de ciberseguridad dentro del entorno o enclave de la red.

En el Apéndice A: de este documento, vemos que se podría prever que la persona cuyo puesto incluya esta función laboral desempeñará muchas de las tareas siguientes, las cuales se ajustan al resultado deseado del Marco de ciberseguridad:

- **T0041**: Coordinar y proporcionar soporte técnico experto a técnicos de ciberdefensa de toda la empresa para resolver los incidentes de defensa de la ciberseguridad.
- **T0047**: Correlacionar los datos de incidentes para identificar vulnerabilidades específicas y hacer recomendaciones que faciliten su corrección inmediata.
- **T0161**: Hacer un análisis de los archivos de registros de diversas fuentes (por ejemplo, registros individuales de hosts, registros de tráfico de redes, registros de firewalls y registros del sistema de detección de intrusiones [IDS]) para identificar posibles amenazas a la seguridad de la red.
- **T0163**: Hacer evaluaciones de incidentes de defensa de la ciberseguridad que incluyan determinación del alcance, urgencia e impacto potencial; identificar la vulnerabilidad específica; y hacer recomendaciones que faciliten su corrección inmediata.
- **T0170**: Hacer una recolección inicial de imágenes de calidad forense apropiada; examinarlas para determinar la posibilidad de mitigación y corrección en los sistemas empresariales.
- **T0175**: Dirigir el manejo de incidentes de defensa de la ciberseguridad en tiempo real (por ejemplo, recolecciones forenses, correlación y seguimiento de intrusiones, análisis de amenazas y corrección directa de sistemas) para ayudar a los equipos desplegables de respuesta a incidentes (IRT).
- **T0214**: Recibir y analizar alertas de red de diversas fuentes dentro de la empresa y determinar las posibles causas de esas alertas.

- **T0233**: Dar seguimiento y documentar los incidentes de defensa de la ciberseguridad desde el momento en que se detectan hasta su resolución final.
- **T0246**: Redactar y publicar técnicas, orientación e informes de defensa de la ciberseguridad sobre los resultados de incidentes para los grupos representados correspondientes.
- **T0262**: Emplear los principios y las prácticas de defensa en profundidad aprobados (por ejemplo, defensa en varios lugares, defensas en capas, solidez de la seguridad).
- **T0278**: Recolectar artefactos de intrusiones (por ejemplo, código fuente, malware, troyanos) y usar los datos descubiertos para facilitar la mitigación de los incidentes potenciales de defensa de la ciberseguridad dentro de la empresa.
- **T0279**: Servir como perito técnico y de enlace con el personal del orden público, y explicar los detalles del incidente según sea necesario.
- **T0312**: Coordinarse con los analistas de inteligencia para correlacionar los datos de las evaluaciones de amenazas.
- **T0164**: Hacer análisis y preparar informes de las tendencias de defensa de la ciberseguridad.
- **T0395**: Escribir y publicar análisis posteriores a una acción.
- **T0503**: Vigilar las fuentes de datos externas (por ejemplo, sitios de proveedores de defensa de la ciberseguridad, equipos de respuesta a emergencias informáticas, grupos de discusión de seguridad) para estar al día de la condición de las amenazas a la defensa de ciberseguridad y determinar los tipos de problemas de seguridad que podrían tener un impacto sobre la empresa.
- **T0510**: Coordinar las funciones de respuesta a incidentes.

Además, el Apéndice B: describe la gran variedad de CHC que podría necesitar una persona cuyo puesto de ciberseguridad incluya esta función laboral.

Una organización que cuente con esta información y que busque lograr el resultado **RS.MI-2** descrito en el Marco de ciberseguridad puede determinar si uno o más de sus empleados actuales posee las habilidades necesarias para llevar a cabo las tareas descritas. Si le falta alguno de los conocimientos, habilidades o capacidades, el empleado que desee desempeñar esa función laboral sabrá las áreas específicas que necesita mejorar y podrá buscar cursos académicos o formación del sector para obtener los conocimientos necesarios. Si no hay ningún empleado con esas cualificaciones, el empleador cuenta con las descripciones de las tareas y los requisitos de CHC específicos que puede usar para anunciar el puesto de trabajo o para buscar personal contratista y aumentar el personal actual.

D.2 Ingeniería de seguridad de sistemas

La Publicación especial 800-160 del NIST, *Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [Ingeniería de seguridad de sistemas: consideraciones para un método multidisciplinario en la ingeniería de

sistemas protegidos y confiables] [14], trata las acciones basadas en ingeniería y necesarias para desarrollar sistemas con más capacidad de defensa y supervivencia, incluidos los componentes de esos sistemas y los servicios que dependen de estos. Esto comienza con un conjunto de normas internacionales bien establecidas para la ingeniería de sistemas y de software, e introduce las técnicas, métodos y prácticas de ingeniería de seguridad de sistemas en esas actividades de ingeniería de sistemas y de software. El objetivo final es solucionar los problemas de seguridad desde la perspectiva de los requisitos y las necesidades de protección de las partes interesadas, y emplear los procesos de ingeniería establecidos para lograr que esos requisitos y necesidades se tengan en cuenta con la fidelidad y rigurosidad apropiadas en todo el ciclo de vida del sistema. Aumentar la confiabilidad de los sistemas es una tarea importante que exige una inversión considerable en requisitos, arquitectura, diseño y desarrollo de sistemas, componentes, aplicaciones y redes, así como un cambio cultural fundamental del concepto actual de "situación normal".

La introducción de un conjunto de actividades y tareas de ingeniería de seguridad de sistemas disciplinado, estructurado y basado en las normas ofrece un punto de partida y una función estricta importantes para iniciar ese cambio necesario. El objetivo final es obtener sistemas seguros y confiables con plena capacidad para ayudar en las misiones críticas y operaciones empresariales protegiendo los recursos de las partes interesadas, y lograrlo con un nivel de seguridad acorde con la tolerancia al riesgo de esas partes interesadas.

La asignación de los componentes del Marco de la NICE a la disciplina de especialización descrita en la Publicación especial 800-160 del NIST validará esos componentes. Es probable que quienes practican la disciplina de especialización en ingeniería de seguridad de sistemas se conviertan en expertos en el tema y puedan justificar la incorporación de más CHC y tareas al Marco de la NICE.

D.3 Códigos federales en materia de ciberseguridad de la Oficina de Administración de Personal de los EE. UU.

El 4 de enero de 2017, la Oficina de Administración de Personal de los EE. UU. (OPM, por sus siglas en inglés) publicó un memorando [15] titulado *Guidance for federal agencies assigning new cybersecurity codes to positions with information technology, cybersecurity, and cyber-related functions* [Guía para los organismos federales que asignan códigos de ciberseguridad nuevos a los puestos con funciones de tecnología de la información, ciberseguridad y funciones relacionadas con la cibernética]. El memorando señala que la Ley federal sobre la evaluación del personal de ciberseguridad de 2015 [16] obliga a la OPM a establecer procedimientos para implementar la estructura de codificación de la NICE y determinar todos los puestos civiles federales que exigen el desempeño de funciones de tecnología de la información, ciberseguridad u otras funciones relacionadas con la ciberseguridad. En la Tabla 9, se muestra la asignación de las identificaciones de funciones laborales del Marco de la NICE, las cuales representan la naturaleza interdisciplinaria del trabajo de ciberseguridad, a los códigos de ciberseguridad de la OPM, que sean compatibles con el Sistema de integración de recursos humanos empresarial de la OPM.

Tabla 9: Correspondencia entre las identificaciones de las funciones laborales y los códigos de ciberseguridad de la OPM

Id. de la función laboral	Código de la OPM	Id. de la función laboral	Código de la OPM	Id. de la función laboral	Código de la OPM
SP-RSK-001	611	OV-LGA-001	731	AN-TWA-001	141
SP-RSK-002	612	OV-LGA-002	732	AN-EXP-001	121
SP-DEV-001	621	OV-TEA-001	711	AN-ASA-001	111
SP-DEV-002	622	OV-TEA-002	712	AN-ASA-002	112
SP-ARC-001	651	OV-MGT-001	722	AN-TGT-001	131
SP-ARC-002	652	OV-MGT-002	723	AN-TGT-002	132
SP-TRD-001	661	OV-SPP-001	751	AN-LNG-001	151
SP-SRP-001	641	OV-SPP-002	752	CO-CLO-001	311
SP-TST-001	671	OV-EXL-001	901	CO-CLO-002	312
SP-SYS-001	631	OV-PMA-001	801	CO-OPL-001	331
SP-SYS-002	632	OV-PMA-002	802	CO-OPL-002	332
OM-DTA-001	421	OV-PMA-003	803	CO-OPL-003	333
OM-DTA-002	422	OV-PMA-004	804	CO-OPS-001	321
OM-KMG-001	431	OV-PMA-005	805	IN-INV-001	221
OM-STS-001	411	PR-CDA-001	511	IN-FOR-001	211
OM-NET-001	441	PR-INF-001	521	IN-FOR-002	212
OM-ADM-001	451	PR-CIR-001	531		
OM-ANA-001	461	PR-VAM-001	541		

Apéndice E: Siglas

Se definen a continuación las siglas y abreviaturas seleccionadas que se usan en este documento.

API	Application programming interface [interfaz de programación de aplicaciones]
CDM	Continuous Diagnostics and Mitigation [diagnóstico y mitigación continuos]
CDS	Cross-Domain Solutions [soluciones entre dominios]
CIO	Chief Information Officer [director de sistemas de información]
CKMS	Crypto Key Management System [sistema de gestión de claves criptográficas]
CMMI	Capability Maturity Model Integration [Integración de modelos de madurez de capacidades]
CMS	Content Management System [sistema de gestión de contenidos]
CNSSI	Committee on National Security Systems Instruction [instrucción del Comité de Sistemas de Seguridad Nacional]
COMSEC	Communications Security [seguridad de las comunicaciones]
COTR	Contracting Officer's Technical Representative [representante técnico del funcionario de contrataciones]
DNS	Domain Name System [sistema de nombres de dominio]
EISA	Enterprise Information Security Architecture [arquitectura de seguridad de la información empresarial]
FISMA	Federal Information Security Modernization Act [Ley federal de modernización de la seguridad de la información]
FOIA	Freedom of Information Act [Ley de libertad de información]
HR	Human Resource [recursos humanos (RR. HH.)]
IDS	Intrusion detection system [sistema de detección de intrusiones]
IP	Internet Protocol [protocolo de internet]
IPS	Intrusion Prevention System [sistema de prevención de intrusiones]
IR	Incident Response [respuesta a incidentes]
IRT	Incident Response Teams [equipos de respuesta a incidentes]
ISD	Instructional System Design [diseño de sistemas didácticos]
ITL	Information Technology Laboratory [Laboratorio de tecnología de la información]
KSA	Knowledge, Skills, and Abilities [conocimientos, habilidades y capacidades (CHC)]
LAN	Local area network [red de área local]
NICE	National Initiative for Cybersecurity Education [Iniciativa nacional para la educación en ciberseguridad]
OLA	Operating-Level Agreement [acuerdo de nivel de operación]
OMB	Office of Management and Budget [Oficina de Administración y Presupuesto]
OPM	Office of Personnel Management [Oficina de Administración de Personal]
OS	Operating system [sistema operativo]
OSI	Open System Interconnection [interconexión de sistemas abiertos]
P.L.	Public Law [Ley pública]
PCI	Payment Card Industry [industria de tarjetas de pago]
PHI	Personal Health Information [información personal de salud]
PIA	Privacy Impact Assessments [evaluaciones del impacto en la privacidad]
PII	Personally Identifiable Information [información de identificación personal]

PKI	Public key infrastructure [infraestructura de clave pública]
R&D	Research and Design [investigación y desarrollo]
RFID	Radio Frequency Identification [identificación por radiofrecuencia]
RMF	Risk Management Framework [Marco de gestión de riesgos]
SA&A	Security Assessment and Authorization [evaluación y autorización de la seguridad]
SDLC	System Development Life Cycle [ciclo de vida de desarrollo de sistemas]
SLA	Service-Level Agreements [acuerdos de nivel de servicio]
SOP	Standard operating procedures [procedimientos operativos estándar]
SQL	Structured query language [lenguaje de consulta estructurado]
TCP	Transmission Control Protocol [protocolo de control de transmisión]
TTP	Tactics, techniques, and procedures [tácticas, técnicas y procedimientos]
URL	Uniform Resource Locator [localizador uniforme de recursos]
VPN	Virtual Private Network [red privada virtual]
WAN	Wide Area Network [red de área extensa]

Apéndice F: Referencias

[1] Página web de revisiones del Marco de la NICE. *Institute of Standards and Technology* [Instituto Nacional de Normas y Tecnología] [sitio web]. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-revisions

[2] *National Initiative for Cybersecurity Education* [Iniciativa nacional para la educación en ciberseguridad], *National Cybersecurity Workforce Framework* [Marco nacional para el personal de ciberseguridad], versión 1.0. https://www.nist.gov/file/359276

[3] *National Initiative for Cybersecurity Education* [Iniciativa nacional para la educación en ciberseguridad], *National Cybersecurity Workforce Framework* [Marco nacional para el personal de ciberseguridad], versión 2.0. https://www.nist.gov/file/359261

[4] Hoja de cálculo de referencia para la Publicación especial 800-181 del NIST. https://www.nist.gov/file/372581

[5] Marco de la NICE, *National Institute of Standards and Technology* [Instituto Nacional de Normas y Tecnología] [sitio web]. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

[6] *U.S. Department of Labor, Employment and Training Administration (ETA)* [Administración de Empleo y Capacitación (ETA, por sus siglas en inglés) del Departamento del Trabajo de los EE. UU.] [sitio web]. https://www.doleta.gov

[7] *Competency Model Clearinghouse, Cybersecurity Competency Model*. [Modelo de competencias para la ciberseguridad del Centro de intercambio de información sobre modelos de competencias]. https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

[8] *Cybersecurity Workforce Development Toolkit (CWDT)* [Conjunto de herramientas para la formación del personal de ciberseguridad] del Departamento de Seguridad Nacional de los EE. UU. https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit

[9] *Baldrige Cybersecurity Excellence Program* [programa Baldrige para la excelencia en la ciberseguridad] del Instituto Nacional de Normas y Tecnología [sitio web]. https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative

[10] Sitio web de la herramienta PushButtonPD™ de la *CyberSkills Management Support Initiative* (CMSI, por sus siglas en inglés) [Iniciativa de ayuda a la gestión de habilidades cibernéticas] del Departamento de Seguridad Nacional de los EE. UU. https://niccs.us-cert.gov/workforce-development/dhs-cmsi-pushbuttonpd-tool

[11] *Framework for Improving Critical Infrastructure Cybersecurity* [Marco para la mejora de la ciberseguridad en infraestructuras críticas], versión 1.0. Instituto Nacional de Normas y Tecnología, 12 de febrero de 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[12] Orden ejecutiva 13636, *Improving Critical Infrastructure Cybersecurity* [Mejora de la ciberseguridad en infraestructuras críticas]. DCPD-201300091, 12 de febrero de 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[13] *NIST Roadmap for Improving Critical Infrastructure Cybersecurity* [Hoja de ruta del NIST para mejorar la ciberseguridad en infraestructuras críticas]. Instituto Nacional de Normas y Tecnología, 12 de febrero de 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

[14] Publicación especial 800-160 del NIST, *Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [Ingeniería de seguridad de sistemas: consideraciones para un método multidisciplinario en la ingeniería de sistemas protegidos y confiables]. Instituto Nacional de Normas y Tecnología, noviembre de 2016. https://doi.org/10.6028/NIST.SP.800-160

[15] Memorando *Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions* [Guía para la asignación de códigos de ciberseguridad nuevos a los puestos con funciones de tecnología de la información, ciberseguridad y funciones relacionadas con la cibernética], enero de 2017. https://www.chcoc.gov/content/guidance-assigning-new-cybersecurity-codes-positions-information-technology-cybersecurity

[16] Cámara de Representantes H.R.2029, *Consolidated Appropriations Act, 2016* [Ley de asignaciones consolidadas de 2016] que incluye la ley *Division N- Cybersecurity Act of 2015* [Ley de ciberseguridad de 2015, División N]. https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf.