Publicación especial 800-181 del NIST
Revisión 1

Marco del personal para la ciberseguridad

(Marco de la iniciativa nacional para la educación en ciberseguridad - NICE)

Rodney Petersen
Danielle Santos
Matthew C. Smith
Karen A. Wetzel
Greg Witte

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.SP.800-181r1es

Document translated courtesy of U.S. Department of State under the Digital Connectivity and Cybersecurity Partnership (DCCP) in partnership with the Organization of American States.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.SP.800-181r1.

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

Publicación especial 800-181 del NIST
Revisión 1

Marco del personal para la ciberseguridad (Marco de la NICE)

Rodney Petersen (Director)
Danielle Santos (Gerente de Comunicaciones y Operaciones)
Karen A. Wetzel (Gerente del Marco de la NICE)
Iniciativa Nacional para la Educación en Ciberseguridad (NICE)
División de seguridad cibernética aplicada
Laboratorio de tecnología de la información

Matthew C. Smith
Greg Witte
Huntington Ingalls Industries
Annapolis Junction, MD

Esta publicación está disponible de forma gratuita en:
https://doi.org/10.6028/NIST.SP.800-181r1es

Noviembre de 2020

Departamento de Comercio de Estados Unidos
Wilbur L. Ross, Jr., Secretario

Instituto Nacional de Normas y Tecnología
Walter Copan, Director del NIST y Subsecretario de Normas y Tecnología del Departamento de Comercio

Autoridad

La presente publicación fue redactada por el Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés) 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, sección 3551 del título 44 del Código de Estados Unidos 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 sobre 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 está de acuerdo 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 a su autoridad estatutaria. Estas directrices tampoco deberán interpretarse como modificaciones o substituciones de las facultades del Secretario de Comercio, Director de la OMB ni 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 revisión 1 del Instituto Nacional de Normas y Tecnología, 31 páginas (noviembre de 2020)
CODEN: NSPUE2

Esta publicación está disponible de forma gratuita en: https://doi.org/10.6028/NIST.SP.800-181r1es

Es posible que en el presente documento se mencionen algunas entidades, equipos o materiales comerciales para describir adecuadamente un procedimiento o concepto experimental. Dicha mención no significa que el NIST los recomienda ni 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 utilizar la información de esta publicación, con inclusión de los conceptos y las metodologías, incluso antes de concluir esas publicaciones complementarias. Por lo tanto, hasta que se finalicen las publicaciones, los requisitos, las directrices y los procedimientos actuales seguirán vigentes donde se hayan establecido. Para 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 presentan para 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 Instituto Nacional de Normas y Tecnología (NIST) promueve la economía y el bienestar público de Estados Unidos por medio de la dirección técnica que aporta 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 el 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 la privacidad, eficaces en función del costo, de la información en los sistemas federales de información que no sea sobre seguridad nacional. La serie 800 de las publicaciones especiales informa acerca de 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

La presente publicación de la Iniciativa Nacional para la Educación en Ciberseguridad (NICE) describe el Marco del Personal para la Ciberseguridad (Marco de la NICE), una referencia fundamental para describir e intercambiar información acerca del trabajo de ciberseguridad. La publicación expresa dicho trabajo como descripción de tarea y presenta la descripción de conocimientos y habilidades, la cual ofrece una base para los alumnos, incluidos los estudiantes, las personas en búsqueda de empleo y los empleados. El uso de estas descripciones ayuda a los estudiantes a desarrollar habilidades, a las personas en búsqueda de empleo a demostrar competencias y a los empleados a realizar sus tareas. Al presentar un léxico común y coherente que categoriza y describe la labor de la ciberseguridad, el Marco de la NICE mejora la comunicación sobre cómo determinar, seleccionar, desarrollar y retener talentos en materia de ciberseguridad. El Marco de la NICE es una fuente de referencia a partir de la cual las organizaciones o los sectores pueden preparar publicaciones y recursos adicionales que satisfagan sus necesidades de definir u ofrecer orientación sobre diferentes aspectos de la educación, la capacitación y el desarrollo del personal en el campo de la seguridad cibernética.

Palabras clave

Competencia, ciberseguridad, ciberespacio, educación, conocimientos, función, seguridad, habilidad, tarea, equipo, capacitación, personal, función laboral.

Aviso de divulgación de patente

AVISO: El Laboratorio de Tecnología de la Información (ITL) solicitó que los titulares de reivindicaciones de patentes cuyo uso pueda ser necesario para cumplir con el asesoramiento o los requisitos de esta publicación divulguen dichas reivindicaciones al Laboratorio de Tecnología de la Información. Sin embargo, los titulares de patentes no están obligados a responder a las solicitudes de patentes del ITL y el ITL no ha emprendido ninguna búsqueda de patentes para determinar aquellas que, de haberlas, se puedan aplicar a esta publicación.

A la fecha de la publicación y posteriormente a las solicitudes para determinar las reivindicaciones de patentes cuyo uso pueda ser obligatorio para el cumplimiento con el asesoramiento o los requisitos de esta publicación, no se ha divulgado al ITL ninguna reivindicación de patentes.

El ITL no formula ni sugiere ninguna declaración acerca de que las licencias no son obligatorias para evitar la infracción de patentes en el uso de esta publicación.

Convenciones del documento

Los términos “debe” y “no debe” indican los requisitos que deben seguirse estrictamente para cumplir con la publicación y de los cuales no se permite ninguna desviación. Los términos "debería" y "no debería" indican que, entre varias posibilidades, se recomienda una como particularmente adecuada, sin mencionar ni excluir otras, o que se prefiere un determinado curso de acción, pero no necesariamente se requiere, o que (en la forma negativa) una cierta posibilidad o línea de acción se desaconseja, pero no se prohíbe. Los términos "podría" y "no necesita" indican un curso de acción permisible dentro de los límites de la publicación. Los términos "puede" y "no puede" indican una posibilidad y capacidad, ya sea material, física o causal.

En el Marco de la NICE, aquellos que realizan trabajos en materia de seguridad cibernética, tales como los alumnos, las personas en búsqueda de empleo y los empleados, se denominan estudiantes. Este apodo destaca que todos los integrantes del personal también siguen un proceso de aprendizaje de por vida.

Agradecimientos

El Marco de la NICE fue creado por un equipo de redacción que incluye representantes de numerosos departamentos y entidades del Gobierno federal de los Estados Unidos. El Instituto Nacional de Normas y Tecnología (NIST) desea reconocer y agradecer a los integrantes del equipo cuya dedicada labor contribuyó de forma importante a la publicación:

William Newhouse, Instituto Nacional de Normas y Tecnología
Pam Frugoli, Departamento de Trabajo
Lisa Dorr, Departamento de Seguridad Nacional
Kenneth Vrooman, Agencia de Seguridad Cibernética y Seguridad de la Infraestructura
Bobbie Sanders, Departamento de Defensa
Patrick Johnson, Departamento de Defensa
Matt Isnor, Departamento de Defensa
Stephanie Shively, Departamento de Defensa
Ryan Farr, Departamento de Defensa

Los autores y el equipo de redacción agradecen y reconocen las importantes contribuciones realizadas por personas y organizaciones de los sectores público y privado, cuyos comentarios reflexivos y constructivos mejoraron la calidad, minuciosidad y utilidad general de la presente publicación. Los autores agradecen especialmente las muchas y útiles respuestas recibidas a la solicitud de comentarios del Marco de la NICE y al borrador de comentarios públicos de esta publicación.

Asimismo, el equipo agradece y reconoce las contribuciones de quienes establecieron las ediciones anteriores de los marcos nacionales para el personal de seguridad cibernética como se describe en la página de la Historia del Centro de Recursos del Marco de la NICE. [1]

Nota al lector

Bienvenido al Marco del Personal para la Ciberseguridad (Marco de la NICE), revisión 1, de la Iniciativa Nacional para la Educación en Ciberseguridad (NICE). El personal de la Oficina del Programa NICE recibió importantes aportes de la comunidad, incluidas muchas respuestas a una reciente solicitud de comentarios generales sobre el Marco de la NICE, así como respuestas al borrador público de esta publicación. En vista de dichos comentarios y del complejo y acelerado ritmo del ecosistema de la seguridad cibernética, el equipo de redacción decidió adoptar y promover atributos de agilidad, flexibilidad, interoperabilidad y modularidad. Estos atributos condujeron a una reestructuración del Marco de la NICE a fin de proporcionar un enfoque simplificado y desarrollar una fuerza laboral que se encargue de los riesgos de la ciberseguridad. A continuación, se presenta un resumen de los cambios:

- La organización de conceptos en la revisión 1 se simplificó a través de la discontinuación de Categorías (por ejemplo, suministrar protección, supervisar y gobernar, proteger y defender, analizar, etc.) y áreas de especialización (por ejemplo, respuesta a incidentes, análisis de riesgos, gestión de la ciberseguridad, etc.). Con el fin de simplificar un enfoque que ofrece agilidad, flexibilidad, interoperabilidad y modularidad para las organizaciones, la revisión 1 presenta un conjunto simplificado de "elementos constitutivos" compuesto por tareas, conocimientos y habilidades. Las organizaciones que encuentran valor en las categorías y áreas de especialización anteriores pueden continuar usándolas o crear equipos en torno a dichos conceptos y ajustarlos a la presente versión del Marco de la NICE (consultar la Sección 3.4).
- La revisión 1 describe varios usos de tareas, conocimientos y habilidades, incluidos los métodos para aplicarlos en la creación de funciones laborales. Los usuarios de las funciones laborales que se describen en el NIST SP 800-181 original pueden seguir utilizándolas. Más adelante, la NICE podría publicar actualizaciones. [2]

La relación entre tareas, conocimientos, habilidades y capacidades ha cambiado. Las descripciones de habilidad y capacidad de la versión anterior se rediseñaron para simplificarlas como descripciones de habilidad, las cuales se centran en la acción del estudiante. Esta revisión presenta métodos para vincular la descripción de conocimientos y habilidades con la descripción de tareas para varios resultados. Las listas de tareas, conocimientos, habilidades y funciones laborales que estaban disponibles anteriormente en los apéndices A y B del Marco de 2017 se eliminaron de la presente versión para simplificar el mantenimiento del Marco de la NICE y facilitar las actualizaciones de esas listas. Las descripciones de tareas, conocimientos y habilidades y las competencias y funciones laborales correspondientes se mantendrán como productos separados y estarán sujetos a revisiones y actualizaciones continuas con un proceso de cambio definido y la indicación de control de versiones para administrar y comunicar los cambios. Hasta que se produzcan esas actualizaciones, las versiones anteriores de estas listas permanecerán disponibles para los usuarios en el centro de recursos del Marco de la NICE. En apoyo a la interoperabilidad y modularidad, las actualizaciones futuras garantizarán que las descripciones coincidan con las definiciones finales de las descripciones de tareas, conocimientos y habilidades mencionados en la presente publicación.

- Para los lectores interesados en asignar estándares, referencias o recursos al Marco de la NICE, la Iniciativa Nacional para la Educación en Ciberseguridad está trabajando con el

Programa Nacional de Referencias Informativa en Línea (OLIR, por sus siglas en inglés) para desarrollar plantillas para dichas asignaciones. El Programa OLIR, administrado por el NIST, ofrece un proceso para hacer concordar referencias con los documentos del NIST. Además, el programa proporciona un catálogo de esas referencias. [3]

Resumen ejecutivo

Cada uno de nosotros, de manera individual o como parte de una organización, realiza un trabajo importante que contribuye a la sociedad. Sin embargo, a medida que la información y la tecnología, incluidos muchos tipos de tecnología operativa en evolución, se vuelven cada vez más complejos e interconectados, puede ser difícil describir claramente la labor que se está realizando o que deseamos lograr en esas áreas en particular. La Iniciativa Nacional para la Educación en Seguridad Cibernética (NICE, por sus siglas en inglés) reconoce que quienes trabajan en el campo de la seguridad cibernética —con inclusión de estudiantes, personas en búsqueda de empleo y empleados— serán alumnos de por vida por medio de su labor de poner de relieve y abordar las repercusiones de la seguridad cibernética en muchos sectores. En el presente documento se hace referencia a ese segmento de personas como «alumnos» y, a veces, como «personal de ciberseguridad», aunque esta última denominación no pretende dar a entender que las funciones laborales y el contenido incluidos en el Marco de la NICE sólo se apliquen a aquellos que estén completamente integrados en el campo de la ciberseguridad. Las tareas que estos alumnos realizan se mencionan más adelante en el presente documento como «trabajo de ciberseguridad», y el Marco aporta un medio que describe ese trabajo con precisión para apoyar la educación y capacitación del alumno, así como en la contratación, la formación y la retención de empleados. El Marco de la NICE fue creado para ayudar a proporcionar una taxonomía de referencia —es decir, un lenguaje común— sobre el trabajo en materia de seguridad cibernética y las personas que realizan ese trabajo. El Marco de la NICE apoya la misión de la NICE de activar, promover y coordinar una comunidad fuerte que trabaje para promover un ecosistema integrado de educación, capacitación y desarrollo del personal para la ciberseguridad. El Marco de la NICE ofrece un conjunto de elementos básicos para describir las tareas, los conocimientos y las habilidades que se necesitan para llevar a cabo el trabajo de seguridad cibernética realizado por individuos y equipos. A través de esos elementos constitutivos el Marco de la NICE permite que las organizaciones desarrollen su fuerza de trabajo para realizar tareas de ciberseguridad y ayuda al alumno a explorar el trabajo en ciberseguridad y participar en actividades de aprendizaje apropiadas para el desarrollo de sus conocimientos y habilidades. Este desarrollo, a su vez, es de utilidad para los empleadores y empleados, dado que les permite determinar trayectorias profesionales que documenten cómo prepararse para el trabajo de seguridad cibernética utilizando los datos de las descripciones de tareas, conocimientos y habilidades (TCH) agrupados en funciones laborales y competencias.

El uso de términos y lenguaje comunes ayuda a organizar y comunicar el trabajo a realizarse y las características de aquellos que están preparados para realizar esa labor. De esta manera, el Marco de la NICE ayuda a simplificar las comunicaciones y a centrarse en las tareas que se están realizando. Por último, el uso del Marco de la NICE mejora la claridad y la coherencia en todos los niveles de la organización, desde un individuo hasta un sistema tecnológico, un programa, una organización, un sector, estado o nación.

Índice

1 Antecedentes

La tecnología continúa evolucionando a un ritmo cada vez mayor. Específicamente, la tecnología que facilita la capacidad de acceder y procesar información de manera rápida y eficiente está cambiando radicalmente. El trabajo necesario para diseñar, construir, asegurar e implementar estos datos, redes y sistemas está aumentando en complejidad. Además, la descripción de ese trabajo y de aquellos que pueden realizarlo sigue siendo un desafío. El problema se agrava ya que las organizaciones utilizan métodos variados y de creación propia para intentar resolver estas dificultades.

Esta publicación de la Iniciativa Nacional de Educación para la Ciberseguridad (NICE) describe el Marco del Personal para la Ciberseguridad (Marco de la NICE). El Marco de la NICE ayuda a las organizaciones a superar la barrera de describir su fuerza laboral a múltiples partes interesadas, a través de la presentación de un enfoque de elementos constitutivos. Mediante el uso de estos elementos constitutivos conceptuales, el Marco de la NICE presenta un lenguaje común para que las organizaciones lo utilicen internamente y con otras partes interesadas. Este enfoque permite que las organizaciones adapten e implementen el marco de la NICE a su contexto operativo único. Además, al crear un lenguaje común, el Marco de la NICE reduce la barrera de entrada para las organizaciones que buscan ingresar e interactuar con otras organizaciones.

La figura 1, presentada a continuación, muestra una visión global del Marco de la NICE. Los principales elementos que constituyen el Marco de la NICE son las descripciones de tareas, conocimientos y habilidades (TCH) (explicadas en la Sección 2) que se presentan junto con los conceptos expuestos por las mismas. La figura 1 muestra que se describen dos tipos principales de conceptos: "el trabajo" y "el alumno". En particular, aquellos que están (o estarán) realizando un trabajo (por ejemplo, estudiantes, empleados o personas en búsqueda de empleo) están continuamente aprendiendo y logrando objetivos, y pueden encontrarse en cualquier parte del ciclo de vida del aprendizaje. El Marco de la NICE intenta describir tanto “el trabajo” como “el alumno” en términos genéricos que se pueden aplicar a todas las organizaciones.

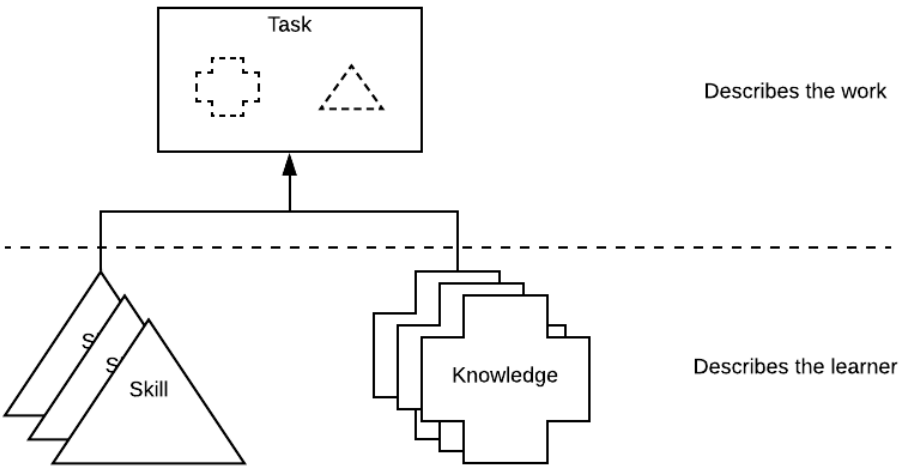


Figura 1 – Enfoque de elementos constitutivos del Marco de la NICE

El "trabajo" es lo que una organización necesita para lograr los objetivos de gestión de riesgos de seguridad cibernética. Cada organización realiza tareas comunes, así como algunas tareas de contexto específico. Por ejemplo, toda organización cuenta con algún tipo de tareas de administración, mientras que solo algunas organizaciones tienen la tarea de "utilizar sistemas de energía en gran escala de forma segura". El Marco de la NICE ofrece a las organizaciones una forma de comunicar su trabajo a través de descripciones de tareas que agrupan descripciones de conocimientos y habilidades.

El "alumno" es la persona que posee conocimientos y habilidades. El término alumno se aplica a todas las personas dentro del ámbito del presente documento. Un alumno puede ser un estudiante, una persona en búsqueda de empleo, un empleado u otra persona dentro del personal. En el contexto de una organización, los alumnos realizan tareas. En un contexto educativo, los alumnos adquieren nuevos conocimientos y habilidades. Todas las personas se consideran alumnos debido a la educación o capacitación que recibieron antes de ingresar a la fuerza de trabajo, capacitación continua, autoaprendizaje o a un plan de carrera profesional.

El Marco de la NICE ofrece a las organizaciones una forma de describir al alumno mediante la asociación de las descripciones de conocimientos y habilidades a un individuo o grupo. Mediante el uso de sus conocimientos y habilidades, los alumnos pueden realizar tareas a fin de lograr los objetivos de la organización. Si bien no todas las organizaciones utilizarán todos los conceptos relacionados con los alumnos, el Marco de la NICE ofrece a las organizaciones un conjunto flexible de elementos constitutivos para usar según sea necesario de acuerdo a su contexto único. El reconocimiento del papel que juega el alumno en el desarrollo de capacidades para realizar el trabajo en ciberseguridad también refuerza la aplicabilidad del Marco de la NICE a los proveedores de educación y formación.

Al describir tanto el trabajo como al alumno, el Marco de la NICE ofrece a las organizaciones un lenguaje común para describir su trabajo y el personal en el campo de la seguridad cibernética. Algunos aspectos del Marco de la NICE describen un contexto de trabajo organizativo (tareas), otros describen un contexto de aprendizaje (conocimientos y habilidades) y, finalmente, el enfoque de elementos constitutivos del Marco de la NICE permite que las organizaciones vinculen los dos contextos.

Además, el Marco de la NICE aporta un mecanismo para comunicarse entre organizaciones a nivel de pares y sectores, así como en los ámbitos estatal, nacional o internacional utilizando los mismos elementos constitutivos. Esta comunicación puede impulsar soluciones innovadoras a desafíos comunes, reducir las barreras de ingreso para nuevas organizaciones e individuos y facilitar la movilidad del personal.

1.1 Atributos del Marco de la NICE

El Marco de la NICE es un recurso de referencia para aquellos que buscan describir el trabajo de su organización en materia de ciberseguridad, las personas que realizarán el trabajo y el proceso de aprendizaje continuo que se necesitará para efectuar esa labor de manera eficaz. La naturaleza del trabajo y, en consecuencia, el personal, se puede describir utilizando los elementos constitutivos de las tareas, los conocimientos y las habilidades que se presentan en las siguientes secciones. Estos elementos constitutivos incorporan los siguientes atributos:

- **Agilidad—** las personas, los procesos y la tecnología maduran, y deben adaptarse al cambio. Por lo tanto, el Marco de la NICE permite que las organizaciones sigan el ritmo de un ecosistema en constante evolución**.**

- **Flexibilidad—**si bien todas las organizaciones enfrentan desafíos similares, no existe una solución única para todos los problemas comunes. Por lo tanto, el Marco de la NICE permite que las organizaciones tengan en cuenta el contexto operativo específico de la organización.

- **Interoperabilidad—** si bien cada solución a los desafíos comunes es única, dichas soluciones deben ponerse de acuerdo en el uso uniforme de los términos. Por lo tanto, el Marco de la NICE permite que las organizaciones intercambien información en materia de personal por medio de un lenguaje común.

- **Modularidad**: si bien el riesgo en materia de seguridad cibernética sigue siendo la base del presente documento, existen otros riesgos que las organizaciones deben manejar dentro de la empresa. Por lo tanto, el Marco de la NICE permite que las organizaciones se comuniquen sobre otros tipos de personal dentro de una empresa y entre organizaciones o sectores (por ejemplo, privacidad, gestión de riesgos, ingeniería/desarrollo de software).

1.2 Obejtivo y aplicabilidad

Las organizaciones se encargan de administrar muchas funciones comerciales diferentes (tales como operaciones, finanzas, aspectos jurídicos y recursos humanos) como parte de su empresa en general. Cada una de estas funciones comerciales conlleva riesgos. A medida que la tecnología se convierte en un factor facilitador de la gestión empresarial, los riesgos relacionados con la seguridad cibernética también se vuelven más prominentes. El Marco de la NICE ayuda a las organizaciones a gestionar los riesgos de la seguridad cibernética al ofrecer una forma de examinar el trabajo y los alumnos relacionados con la ciberseguridad. Los riesgos en materia de ciberseguridad representan una importante contribución para las decisiones de riesgo empresarial, como se describe en el informe de NIST: Informe interinstitucional 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. [Integración de la ciberseguridad y la gestión de riesgos empresariales] [4]

El presente documento constituye una posible guía para otras funciones comerciales que están considerando la creación de marcos de personal. Las organizaciones pueden elevar su eficiencia utilizando los mismos elementos constitutivos en varias funciones comerciales. Por lo tanto, el presente documento puede ser útil para cualquier organización.

1.3 Público

El tema sobre la administración del personal de ciberseguridad abarca muchos puestos de naturaleza diferente, así como diferentes tipos de organizaciones. El público de este documento incluye organismos del sector público, organizaciones privadas y sin fines de lucro, instituciones educativas y de capacitación, diseñadores de programas de estudio, proveedores de credenciales, profesionales de recursos humanos, gerentes de contrataciones, supervisores, planificadores de personal, funcionarios encargados de contrataciones y todos los alumnos.

1.4 Organización de esta publicación

El resto de esta publicación especial se organiza de la siguiente manera:

- Sección 2, Elementos constitutivos del Marco de la NICE: se definen los elementos constitutivos de las tareas, los conocimientos y las habilidades (TCH) del Marco de la NICE
- Sección 3, Uso del Marco de la NICE: describe enfoques comunes para el uso del Marco de la NICE
- Sección 4, Conclusión
- Referencias: una lista de publicaciones relacionadas con el tema a las que se hace referencia en el documento.
- Apéndice A: siglas: se presenta una lista de siglas y abreviaturas utilizadas en este documento.

2 Elementos constitutivos del Marco de la NICE

El Marco del personal para la ciberseguridad (Marco de la NICE) se basa en un conjunto de elementos constitutivos específicos que describen el trabajo a realizarse (en forma de tareas) y lo que se requiere para realizar ese trabajo (a través de conocimientos y habilidades). Dichos elementos constitutivos son estructuras organizativas que respaldan el uso y la implementación del Marco de la NICE. Ofrecen un mecanismo mediante el cual, tanto organizaciones como personas, pueden comprender el alcance y el contenido del Marco de la NICE. Estos elementos básicos están concebidos como pautas que se pueden utilizar para mejorar la comprensión en lugar de estructuras rígidas.

2.1 Descripción de tareas

Tarea
Una actividad que está dirigida al logro de los objetivos de la organización.

Descripción de la tarea
- Fácil de leer y entender
- Comienza con la actividad que se realiza
- No contiene el objetivo de la tarea

Como se muestra en la figura 1, la descripción de tareas detalla el trabajo, mientras que la descripción de conocimientos y habilidades (C y H) define al alumno. La descripción de una tarea debe centrarse en el lenguaje organizativo y en los modelos de comunicación que aportan valor a la organización. Esta descripción está destinada a detallar el trabajo a realizarse y debe estar de acuerdo con el contexto de la organización.

La tarea describe el trabajo que se debe llevar a cabo. La tarea se puede definir como una actividad dirigida al logro de los objetivos de la organización, incluidos los objetivos comerciales, objetivos tecnológicos u objetivos de misión. La descripción de una tarea debe ser sencilla. Si bien el trabajo incluido en una descripción de tarea puede contar con muchos pasos, como en el siguiente ejemplo, la descripción en sí es fácil de leer y comprender.

Una descripción de tarea comienza con la actividad que debe ejecutarse.

Ejemplo: **resolver problemas** de hardware y software del sistema

La descripción de la tarea no contiene el objetivo, ya que los objetivos pueden variar según los impulsores de la misión y las necesidades de la organización.

Ejemplo: realizar ejercicios de capacitación interactivos

En el ejemplo anterior, el propósito de los ejercicios puede ser crear un entorno de aprendizaje eficaz, pero ese objetivo no se incluye en la descripción de tarea.

Como se observa en la figura 1, las tareas están relacionadas con las descripciones de conocimientos y habilidades. Un alumno demostrará que posee el conocimiento y las habilidades para realizar la tarea (o deberá adquirir el conocimiento y aprender la habilidad para preparar la tarea). La complejidad dentro de una tarea se explica en las descripciones de conocimientos y habilidades relacionadas con la misma. En el ejemplo anterior sobre resolución de problemas, para resolver cualquier problema en alguna pieza de software o hardware, el alumno debe estar

familiarizado y entender la descripción de conocimientos que se relacionan con el tema. Lo mismo puede decirse de la descripción de habilidades.

2.2 Descripción de conocimientos

Conocimiento
Un conjunto de conceptos recuperables dentro de la memoria.

Descripción de conocimientos
- Describir conocimientos fundamentales o específicos
- Es posible que se necesiten varias descripciones para realizar una tarea
- Se puede usar una sola descripción para realizar muchas tareas diferentes.

La descripción de conocimientos está relacionada con la descripción de tareas en el sentido de que solo al comprender lo que se expone en la descripción de conocimientos el alumno podrá realizar la tarea. El conocimiento se define como un conjunto recuperable de conceptos dentro de la memoria. Las descripciones de conocimientos pueden referirse a conceptos fundamentales o específicos. Es posible que se necesiten varias descripciones de conocimientos para llevar a cabo una tarea determinada. Del mismo modo, una descripción de conocimientos se puede utilizar para realizar muchas tareas diferentes.

La descripción de conocimientos puede ser de naturaleza fundamental.

> Ejemplo: conocimiento sobre las amenazas y vulnerabilidades del espacio cibernético

La descripción de conocimientos puede ser específica.

> Ejemplo: Conocimiento las fuentes de difusión sobre información de vulnerabilidades (por ejemplo, alertas de proveedores, avisos de los Gobiernos, erratas en la documentación sobre productos y boletines sectoriales).

Las organizaciones que realizan descripciones de conocimientos deben considerar los diferentes niveles de conocimiento y experiencia del alumno. En la taxonomía revisada de Bloom, la cual utiliza un lenguaje que facilita la observación y la evaluación del alumno, se describe un ejemplo de estos diversos niveles. [5]

2.3 Descripción de habilidades

La descripción de habilidades está relacionada con la descripción de tareas en cuanto a que el alumno demuestra habilidades para realizar tareas. Un alumno que no pueda demostrar la habilidad descrita no podrá realizar la tarea que depende de esa habilidad. Una habilidad se define como la capacidad de realizar una acción observable. Las descripciones de habilidades pueden presentar habilidades sencillas o complejas. Es posible que se necesiten varias descripciones de habilidades para llevar a cabo una tarea determinada. Del mismo modo, el ejercicio de una habilidad se puede utilizar para llevar a cabo más de una tarea.

La descripción de una habilidad puede ser simple.

> Ejemplo: habilidad para reconocer alertas del sistema de detección de intrusiones

La descripción de una habilidad puede ser compleja.

> Ejemplo: habilidad para generar una hipótesis sobre cómo un actor malintencionado elude el sistema de detección de intrusiones.

Habilidad
La capacidad de realizar una acción observable.

Descripción de habilidades
• Describir habilidades sencillas o complejas
• Es posible que se necesiten varias descripciones de habilidades para realizar una tarea.
• Puede utilizarse una sola descripción de habilidad para llevar a cabo más de una tarea.

Como se presenta en la figura 1, la descripción de habilidades se refiere a lo que el alumno puede hacer y la descripción de tareas se refiere al trabajo que se debe realizar. Por lo tanto, es importante separar el lenguaje utilizado entre descripción de habilidades y descripción de tareas, y utilizar términos que faciliten la observación y la evaluación del alumno.

3 Uso del Marco de la NICE

Si bien el Marco del Personal para la Ciberseguridad (Marco de la NICE) está dirigido a ofrecer un conjunto de elementos constitutivos comunes que muchos pueden utilizar, algunas organizaciones deberán adaptar el modelo para ajustarlo más estrechamente a su contexto concreto. Por ejemplo, un fabricante puede tener tareas que son específicas para un sector u organización, las cuales no están descritas en el Marco de la NICE. Otros pueden encontrar que las tareas se pueden aplicar, pero deben ajustarse o deben formular una descripción específica de conocimientos y habilidades para aumentar la probabilidad de que las tareas puedan llevarse a cabo de acuerdo a lo que su contexto específico requiere. Por lo tanto, estos elementos constitutivos no deben ser rígidos, sino que deben proporcionar un lenguaje común para que las organizaciones y los sectores los utilicen de manera que sean de utilidad para un contexto determinado.

Por último, los ejemplos de usos de los elementos constitutivos del Marco de la NICE que se presentan a continuación son de naturaleza teórica o conceptual. Una organización puede utilizar los elementos constitutivos de diferentes formas para satisfacer mejor las necesidades locales. Estos ejemplos se presentan con el propósito de ilustrar posibles enfoques prácticos del Marco de la NICE que han demostrado que pueden ayudar a lograr objetivos organizativos comunes. Brindan orientación a organizaciones o sectores que buscan un lugar para comenzar en vez de una forma singular de utilizar el Marco de la NICE.

3.1 Uso de las descripciones de tareas, conocimientos y habilidades existentes

Los usuarios del Marco de la NICE hacen referencia a una o más descripciones de tareas, conocimientos y habilidades (descripciones TCH), como se señala en la sección 2, para referirse tanto al trabajo como al alumno. La descripción de tareas se utiliza para detallar el trabajo. La descripción de tarea contiene las descripciones de conocimientos y habilidades que se relacionan con la tarea. Aunque la descripción de la tarea puede contar con un conjunto recomendado de descripciones de conocimientos y habilidades, los usuarios pueden incluir otras descripciones de conocimientos y habilidades ya establecidas para adaptar las tareas a su contexto específico. La descripción de conocimientos y habilidades se utiliza para describir al alumno. La descripción de conocimientos y habilidades se pueden utilizar de muchas formas para administrar el personal de ciberseguridad. Pueden utilizarse en parte, todas juntas o no usarse en absoluto, según el contexto específico del organismo de ejecución. Los ejemplos teóricos de uso que se presentan a continuación muestran las áreas en las cuales la descripción de tareas, conocimientos y habilidades pueden implementarse:

- Programa de seguimiento de habilidades del empleado para determinar los títulos y méritos para su promoción
- Conocimientos necesarios para realizar un curso
- Lista de tareas semanales que se deben llevar a cabo en una organización

La descripción y los ejemplos de tareas, conocimientos y habilidades se pueden encontrar en el centro de recursos del Marco de la NICE y se actualizarán, según sea necesario, para mantenerse al día con los cambios que surjan de la evolución de la misión de las empresas, los riesgos o las tecnologías emergentes. [1]

3.2 Creación de nuevas descripciones de tareas, conocimientos y habilidades

Se advierte a los usuarios que no modifiquen el texto de las descripciones de tareas, conocimientos y habilidades ya existentes del Marco de la NICE. Las descripciones tienen el propósito de respaldar la interoperabilidad; por lo tanto, cambiar su contenido puede causar un desajuste posterior al usar fuentes externas. Si se necesita una redacción diferente para una descripción de tarea, conocimientos y habilidades que respalde el contexto específico de un usuario, se puede crear una nueva descripción.

Los usuarios también pueden crear descripciones de tareas, conocimientos o habilidades completamente nuevas para ayudar a adaptar el uso del Marco de la NICE para el uso local dentro de un contexto específico. Estas descripciones adicionales ayudarán a respaldar un análisis interno claro y coherente con respecto a los alumnos y sus actividades laborales.

3.3 Competencias

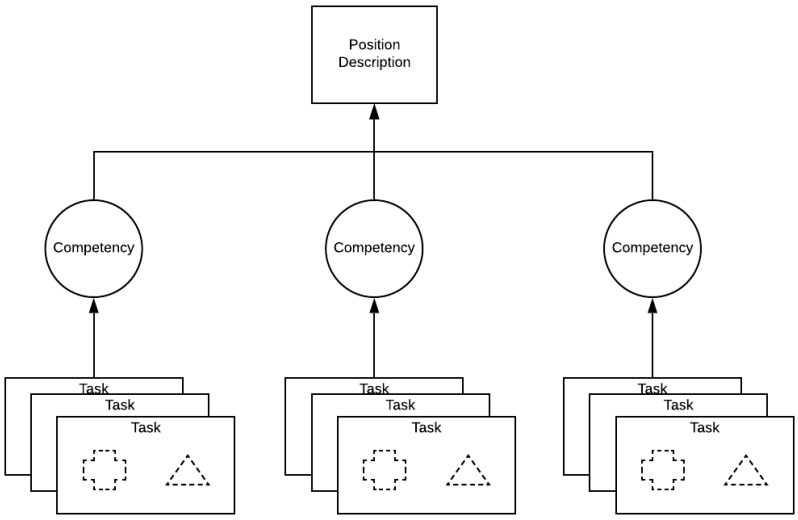
Las competencias ofrecen un mecanismo para que las organizaciones evalúen al alumno. Las competencias se definen a través de un enfoque motivado por el empleador que aporta información sobre el contexto específico de una organización. Además, las competencias permiten que los proveedores de educación y capacitación respondan a las necesidades del empleador o del sector mediante la formulación de experiencias de aprendizaje que ayuden al alumno a desarrollar y demostrar las competencias. Las competencias constan de un nombre, la descripción de la competencia, el método de evaluación, así como de un grupo de descripciones de tareas, conocimientos o habilidades relacionados.

Las competencias ofrecen flexibilidad al permitir que las organizaciones agrupen varias descripciones de TCH en una categoría general que define una necesidad amplia. Si bien una tarea específica y la descripción de conocimientos y habilidades relacionados pueden no cambiar, la competencia definida de manera más amplia puede introducir nuevas tareas, así como conocimientos y habilidades particulares, o eliminar algunos de los existentes, en respuesta a necesidades que pueden variar en un ecosistema de ciberseguridad cambiante.

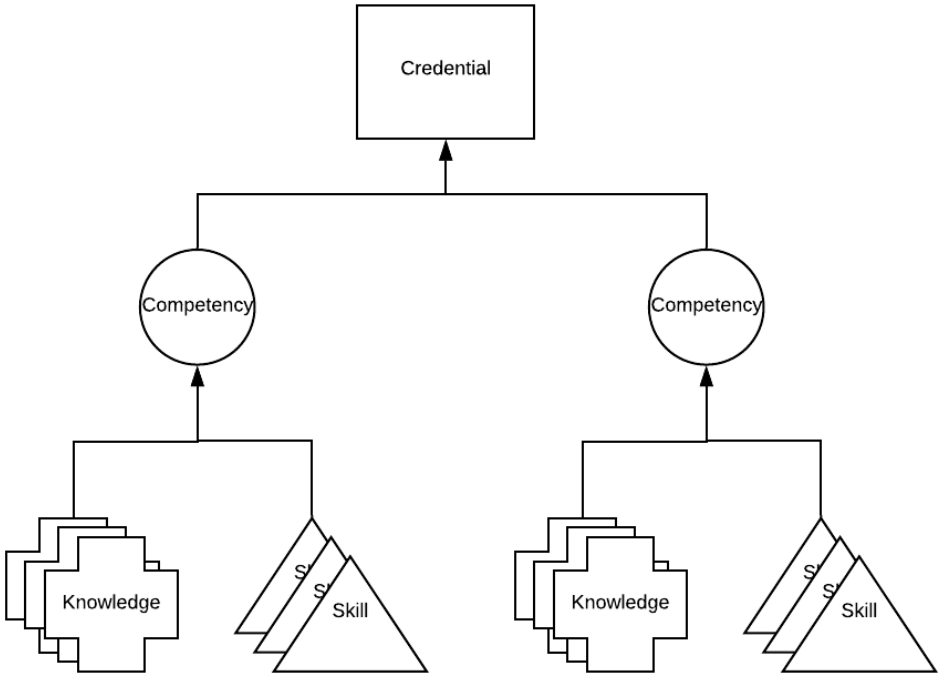
Competencia
Mecanismo de las organizaciones para evaluar a los alumnos.

Las competencias:
- Se definen a través de un enfoque motivado por el empleador
- Se centran en el alumno
- Son observables y medibles

Hay varias formas de utilizar las competencias. Por ejemplo, como se muestra en la figura 2, una organización podría usar las competencias como parte del proceso de contratación dirigido a cumplir con metas específicas de la organización. En este caso, las competencias podrían definirse como un grupo de descripciones de tareas relacionadas. Luego, la organización podría usar estas competencias para evaluar si un candidato puede realizar esas tareas. Esta evaluación podría tomar la forma de una entrevista, una prueba previa al empleo o la observación del aprendizaje en el trabajo.



Otras organizaciones podrían utilizar las competencias para determinar si un alumno ha alcanzado un conjunto definido de habilidades y conocimientos. Estas organizaciones podrían, como se muestra en la figura 3, optar por utilizar las competencias como grupos de descripciones de conocimientos y habilidades. Estas organizaciones podrían entonces evaluar a los alumnos con respecto a dichas descripciones de conocimientos y habilidades. Las evaluaciones pueden tomar la forma de pruebas, demostraciones de laboratorio o evaluaciones orales.



Los ejemplos anteriores pretenden ser hipotéticos. Pueden usarse en parte, todos juntos o no usarse en absoluto, según el contexto único del organismo de ejecución.

3.3.1 Uso de competencias existentes

El uso de las competencias del Marco de la NICE es una forma de que las organizaciones se ajusten al Marco de la NICE como visión global, sin profundizar en los detalles de las descripciones de tareas, conocimientos y habilidades (TCH). Las competencias son una forma de describir la evaluación de un alumno. Al posibilitar grupos de descripciones de TCH definidos por la organización, las competencias permiten que las organizaciones se comuniquen de manera sucinta y organicen su trabajo en materia de ciberseguridad de manera efectiva para brindar una visión optimizada del personal. Otros posibles usos de las competencias incluyen:

- Describir los tipos de tareas dentro de un puesto determinado
- Dar seguimiento a las capacidades del personal
- Describir los requisitos del equipo
- Demostrar las capacidades del alumno.

Aunque la competencia cuenta con un conjunto recomendado de descripciones de tareas, conocimientos y habilidades asociadas, los usuarios pueden agregar otra descripción o eliminar descripciones existentes para adaptar las competencias a su contexto específico. Sin embargo, se advierte a los usuarios que no modifiquen el título ni la descripción de una competencia ya establecida en el Marco de la NICE. Las competencias tienen el propósito de respaldar la interoperabilidad, por lo que cambiar su contenido puede derivar en un desajuste posterior cuando

se utilizan fuentes externas. Si se necesita una redacción diferente en una competencia para respaldar el contexto único de un usuario, se puede crear una nueva competencia como se describe a continuación (consultar la Sección 3.3.2).

3.3.2 Creación de nuevas competencias

Algunas organizaciones pueden necesitar la descripción de una competencia para el contexto específico de su trabajo en ciberseguridad. El Marco de la NICE, desarrollado con el principio de agilidad, permite que las organizaciones describan una competencia para responder a un ecosistema de ciberseguridad cambiante. Esto se puede lograr al modificar una competencia ya establecida para satisfacer las necesidades locales o creando una competencia completamente nueva.

A continuación, se presentan dos ejemplos teóricos para explicar los posibles procesos para el uso de las competencias. Los dos ejemplos se centran en el análisis de datos para mostrar que se puede utilizar la misma competencia mediante enfoques diferentes. Además, estos ejemplos explican las figuras 2 y 3 en más detalle para brindar al lector una buena base de conocimientos sobre una posible implementación. Estos ejemplos utilizan una estructura de tabla para comunicar la competencia. Este enfoque tabular es uno de los muchos que podría utilizar una organización que busque implementar competencias.

Ejemplo 1 de análisis de datos

El cuadro 1 presentado a continuación es informativo y ofrece un punto de partida para la formulación de una competencia. La competencia de análisis de datos del ejemplo 1 tiene un nombre y una descripción que le permite a la organización detectar rápidamente una competencia como una competencia que tiene valor para su estructura organizativa y su contexto. Por medio del método de evaluación de "demostración de laboratorio", la organización evalúa a un alumno al proporcionar un entorno de trabajo simulado para llevar a cabo las tareas que cumplen con sus objetivos comerciales. (Tener en cuenta que el cuadro 1 utiliza tareas de la versión 2017 del Marco de la NICE. [2])

Cuadro 1 – Ejemplo sobre la creación de una nueva competencia sobre análisis de datos con las tareas actuales del Marco de la NICE de 2017

Nombre de la competencia: Ejemplo 1 de Análisis de datos
Descripción de la competencia: recopilación, síntesis o análisis cualitativo y cuantitativo de una variedad de fuentes para tomar una decisión, formular una recomendación y/o recopilar informes, sesiones informativas, resúmenes ejecutivos y otra correspondencia.
Método de evaluación: demostración de laboratorio
Descripción de las tareas
T0007 | Analizar y definir los requisitos y las especificaciones de datos.

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).

En el ejemplo presentado en el cuadro 1, una organización puede entregar a un alumno una computadora cargada con un conjunto de datos específicos y conectada a la red de laboratorio. Luego, el alumno tiene un tiempo para demostrar su capacidad de utilizar lenguajes de código abierto para aplicar técnicas cuantitativas a los datos. Un aspecto clave de esta evaluación puede ser analizar el conjunto de datos para garantizar que los datos cumplan con una especificación de datos concreta antes de finalizar el análisis. A través de esta evaluación, el estudiante demuestra la competencia del "Ejemplo 1 de análisis de datos" según lo define el empleador.

La descripción de una competencia de análisis de datos completamente detallada podría ser mucho más larga. Al enumerar las descripciones de tareas dentro de la competencia, la organización puede especificar el alcance deseado de la competencia. Para facilitar su uso, se hace referencia a las tareas con el Id. de la tarea de acuerdo al Marco de la NICE de 2017.

Ejemplo 2 sobre análisis de datos

El siguiente cuadro 2 presenta otro punto de partida para crear una competencia. El ejemplo es informativo; la descripción es la misma del cuadro 1. Sin embargo, este ejemplo utiliza conocimientos y habilidades para crear la competencia.

Cuadro 2 – Ejemplo de creación de una nueva competencia de análisis de datos con tareas adicionales

Nombre de la competencia: Ejemplo 2 de análisis de datos
Descripción de competencia: recopilación, síntesis o análisis cualitativo y cuantitativo de una variedad de fuentes para tomar una decisión, formular una recomendación y/o recopilar informes, sesiones informativas, resúmenes ejecutivos y otra correspondencia.
Método de evaluación: prueba
Descripciones de conocimientos y habilidades
S0013 | Habilidad para llevar a cabo consultas y diseñar algoritmos a fin de analizar estructuras de datos.
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)
S0091 | Habilidad para analizar datos volátiles.
K0020 | Conocimiento de políticas sobre administración y normalización de datos.
K0338 | Conocimiento de técnicas de extracción de datos.

En este ejemplo, el cuadro 2 representa una competencia de análisis de datos. Esta competencia podría ser creada por un organismo de certificación que proporcione una prueba para evaluar a los alumnos. La prueba se puede realizar en papel o en formato informático. Al pasar exitosamente la prueba, el alumno demuestra la competencia del "Ejemplo 2 de análisis de datos" según lo define el organismo de certificación.

(Tenga en cuenta que el cuadro 2 utiliza los conocimientos y habilidades establecidos en la versión de 2017 del Marco de la NICE. [2])

3.4 Funciones laborales

Las funciones laborales son un caso de uso común del Marco de la NICE. Las funciones laborales son una forma de describir un conjunto de trabajos del cual alguien está encargado o por el cual alguien es responsable.

Si bien los marcos de personal anteriores también vinculaban las funciones laborales con las especificaciones de conocimientos, habilidades y aptitudes, el Marco de la NICE promueve un enfoque más ágil a través de las tareas. Las funciones laborales están compuestas por tareas que constituyen el trabajo que debe realizarse. Las tareas incluyen descripciones de conocimientos y habilidades relacionadas a ellas, las cuales representan el potencial del alumno de realizar esas tareas. El enfoque de transición que se presenta en la figura 3, respalda la flexibilidad y simplifica la comunicación.

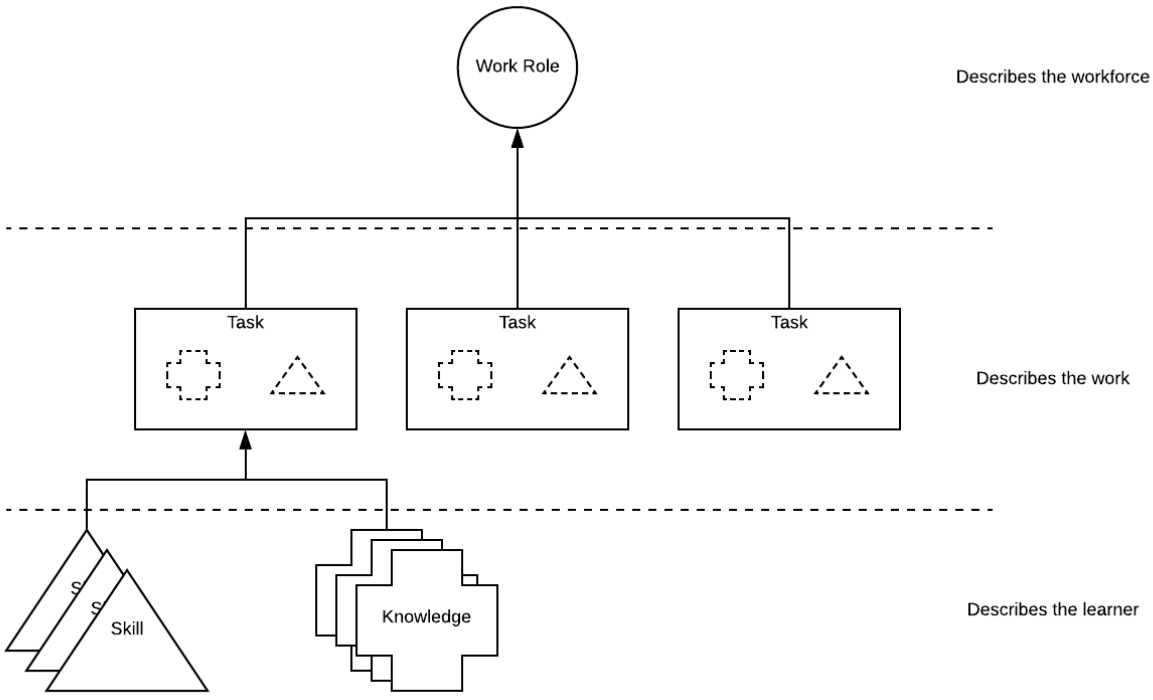


Figura 4 – Relación entre las funciones laborales y los elementos constitutivos

Los nombres de las funciones laborales no son sinónimos de los nombres que reciben los puestos de trabajo. Algunas funciones laborales pueden coincidir con el nombre del puesto de trabajo, según el uso que haga una organización de los puestos. Además, las funciones laborales no son sinónimos de ocupaciones.

Para aquellos con muchos nombres de puestos diferentes (por ejemplo, ingeniero de software, codificador, desarrollador de aplicaciones), podría aplicarse solamente una única función laboral (por ejemplo, desarrollador de software). Por el contrario, se pueden combinar muchas funciones laborales para crear un puesto de trabajo específico. Este enfoque aditivo respalda mejor modularidad e ilustra el hecho de que todos los alumnos en el personal realizan numerosas tareas en varias funciones laborales, independientemente de sus puestos de trabajo. Asimismo, el Marco de la NICE no define niveles de competencia (por ejemplo, básico, intermedio, avanzado). Dichos atributos y los relacionados con pericia con la que un alumno realiza las tareas, se dejan para otros modelos o recursos.

3.4.1 Uso de las funciones laborales existentes

Cada una de las funciones laborales tiene el propósito de respaldar el logro de objetivos a través de tareas. Aunque una función laboral puede contar con un conjunto de tareas predeterminadas, los usuarios pueden incluir otras tareas ya establecidas para adaptar las funciones laborales a su contexto único. Asimismo, un usuario podría utilizar alguna de las funciones laborales alistadas o agregar otras para respaldar objetivos adicionales. El conjunto actual de componentes del Marco de la NICE está disponible en el Centro de Recursos del Marco de la NICE. [1]

Se advierte a los usuarios que no deben modificar internamente el nombre ni la descripción de una función laboral existente. Las funciones laborales tienen el propósito de respaldar la interoperabilidad, por lo que cambiar su contenido puede causar un desajuste posterior. Si se necesita una redacción diferente, se puede crear una nueva función laboral como se describe a continuación.

3.4.2 Creación de una nueva función laboral

Los usuarios también pueden crear nuevas funciones laborales para ayudar a adaptar el uso del Marco de la NICE a su contexto específico. Dichas funciones laborales adicionales ayudarán a respaldar discusiones internas con claridad y coherencia con respecto al trabajo de ciberseguridad.

3.5 Equipos

Muchas organizaciones utilizan equipos para abordar colectivamente desafíos complejos, reuniendo a personas con habilidades y experiencia complementarias. Al utilizar diferentes recursos y perspectivas, los equipos permiten que las organizaciones administren los riesgos de manera integral. Los equipos aprovechan la especialización de conocimientos y procesos de cada integrante para distribuir el trabajo de manera efectiva. Los equipos se pueden definir por medio de las funciones laborales o las competencias.

3.5.1 Creación de equipos con funciones laborales

El enfoque centrado en la función laboral para la formación de equipos permite que las organizaciones definan el tipo de funciones laborales que se necesitan para lograr objetivos determinados. Dado que las funciones laborales están formadas por competencias, este enfoque de creación de equipos comienza con el trabajo que se debe realizar. Este enfoque puede considerarse "de arriba abajo".

Cuadro 3 – Ejemplo de un equipo de desarrollo de software seguro que utiliza las funciones laborales del Marco de la NICE de 2017

Fase del ciclo de vida	Función laboral
Diseñar	SP-ARC-002 | Arquitecto de seguridad
Construir	SP-DEV-001 | Desarrollador de software
Deploy	OM-NET-001 | Especialista en operaciones de red
Operar	OM-STS-001 | Especialista en soporte técnico
Mantener	OM-DTA-001 | Administrador de base de datos
Eliminar	OV-LGA-001 | Asesor de derecho informático

El cuadro 3 anterior presenta una forma de crear un equipo para desarrollar un software seguro. Se hace referencia a las funciones laborales mediante la versión 2017 para determinar las funciones laborales del Marco de la NICE. Los equipos construidos de esta manera comienzan con la determinación del trabajo que debe realizarse. En el ejemplo presentado, el equipo de desarrollo de software seguro está organizado por fase de ciclo de vida. La primera fila muestra que el equipo consideraría los objetivos de la fase de diseño, incluida la planificación, y por lo tanto necesitaría un arquitecto de seguridad. El cuadro 3 es un ejemplo informativo y no cubre todas las funciones laborales que pueden estar presentes o ser necesarias para un equipo determinado. Para obtener más información, consulte el *Marco de Desarrollo de Software Seguro del NIST*. [6]

Cuadro 4 – Ejemplo de creación de un equipo de ciberseguridad por medio del uso de las funciones laborales del Marco de la NICE de 2017 y nuevas funciones laborales

Función del marco de ciberseguridad	Función laboral
Identificar	Nueva función laboral 1 | Gestor de riesgos
Proteger	SP-RSK-002 | Asesor de control de seguridad
Detectar	PR-CDA-001 | Analista de ciberdefensa
Responder	PR-CIR-001|Respuesta a incidentes de defensa cibernética
Recuperar	Nueva función laboral 2 | Especialista en comunicaciones

El cuadro 4 describe un ejemplo de equipo de ciberseguridad. Semejante al equipo de desarrollo de software seguro, el equipo del ejemplo se construye con un enfoque centrado en el trabajo. Al utilizar el Núcleo del *"Marco para la mejora de la seguridad cibernética en infraestructuras críticas (Marco de ciberseguridad)"*, se seleccionan los objetivos de la seguridad cibernética, se determinan las tareas para lograr esos objetivos y se seleccionan las funciones laborales para

determinar las funciones necesarias para respaldar esos objetivos. [7] El cuadro 4 es un ejemplo informativo y no cubre todas las funciones laborales que pueden estar presentes o requerirse para un equipo determinado. Se agregan dos funciones laborales nuevas para mostrar un enfoque mixto del uso de las funciones laborales existentes (sección 3.4.1) y la creación de nuevas funciones laborales (sección 3.4.2). Al crearse nuevas funciones laborales, el ejemplo demuestra un enfoque flexible y ágil para adaptar el Marco de la NICE.

3.5.2 Creación de equipos con competencias

Los equipos también se pueden construir utilizando competencias. Este enfoque de creación de equipos reconoce que las tareas específicas pueden ser desconocidas, pero se conoce el tipo de competencias necesarias para resolver el problema. Este enfoque puede considerarse "de abajo arriba". Por lo tanto, los equipos creados de esta manera pueden ayudar a los alumnos que pueden participar en el trabajo del equipo en el futuro. Estos alumnos pueden o no estar asociados con una función laboral y simplemente poseer las competencias necesarias para ayudar a alcanzar los objetivos de la organización.

Por ejemplo, el equipo defensivo de seguridad cibernética que utiliza sus habilidades para imitar las técnicas de ataque de los adversarios (es decir, el "Equipo Rojo") puede estar formado por las siguientes competencias teóricas:

- Planificación del enfrentamiento
- Reglas de enfrentamiento
- Prueba de penetración [*pen testing*]
- Recopilación de datos
- Explotación de vulnerabilidades

Al crear equipos u otras agrupaciones de tareas, conocimientos y habilidades, cada organización puede adaptar el Marco de la NICE de la mejor manera que ayude a aplicar y comunicarse sobre los alumnos (y el trabajo que realizarán los alumnos) para permitir el logro de los objetivos de la misión.

4 Conclusión

Mediante la aplicación del enfoque de elementos constitutivos presentado por el Marco de la NICE, los usuarios pueden beneficiarse con un método uniforme para organizar y comunicar el trabajo a realizarse a través de las descripciones de tareas, así como a través de los conocimientos y las habilidades de los alumnos que desempeñan ese trabajo. El Marco de la NICE ayuda a orientar la labor de los empleadores para describir el trabajo de seguridad cibernética, de las instituciones educativas y de capacitación para preparar a los trabajadores de la seguridad cibernética y de los alumnos para que demuestren su capacidad de realizar el trabajo en materia ciberseguridad.

La capacidad de describir tareas, conocimientos y habilidades es importante para garantizar una comprensión integral del trabajo y el personal. El Marco de la NICE ofrece un recurso de referencia extensible que puede ser aplicado y utilizado por varias organizaciones o grupos para describir el trabajo a realizarse en muchas áreas. Los beneficios para estas organizaciones respaldan la misión de la NICE de dinamizar, promover y coordinar una comunidad fuerte que trabaja en conjunto para promover un ecosistema integrado de educación, capacitación y desarrollo de la fuerza laboral en ciberseguridad.

Referencias

[1] National Initiative for Cybersecurity Education [Iniciativa nacional para la educación en ciberseguridad], (2020) *NICE Framework Resource Center*. Disponible en: https://www.nist.gov/nice/framework

[2] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [Iniciativa nacional para la educación en ciberseguridad del Marco del personal para la ciberseguridad]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. https://doi.org/10.6028/NIST.SP.800-181

[3] National Institute of Standards and Technology [Instituto Nacional de Normas y Tecnología] (2020) *National Online Informative References Program*. Disponible en: https://csrc.nist.gov/projects/olir

[4] Stine K, Quinn S, Witte G, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM) [Integrar la ciberseguridad y la gestion del riesgo empresarial]. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[5] Krathwohl, D. R. (2002). A revision of Bloom's taxonomy: An overview. *Theory Into Practice*, [Una revisión de la taxonomía de Bloom: una visión general. De la teoría a la práctica] 41(4), 212-218. Disponible en https://www.depauw.edu/files/resources/krathwohl.pdf

[6] Dodson DF, Souppaya MP, Scarfone KA (2020) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.04232020

[7] National Institute of Standards and Technology [Instituto Nacional de Normas y Tecnología] (2018) Framework for Improving Critical Infrastructure Cybersecurity [Marco para la mejora de la ciberseguridad en infraestructuras críticas] Versión 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

Apéndice A - Siglas

A continuación, se presentan las siglas y abreviaturas utilizadas en el presente documento.

ERM	Enterprise Risk Management [Gestión del riesgo 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]
ITL	NIST Information Technology Laboratory y [Laboratorio de tecnología de la información]
K&S	Knowledge and Skill statement(s) [Descripciones de conocimientos y habilidades (CH)]
NICE	National Initiative for Cybersecurity Education [Iniciativa nacional para la educación en ciberseguridad]
NIST	National Institute of Standards and Technology [Instituto Nacional de Normas y Tecnología]
OLIR	Online Informative Reference [Recurso informativo en línea]
OMB	Office of Management and Budget [Oficina de Administración y Presupuesto]
SSDF	Secure Software Development Framework [Marco de Desarrollo Seguro de software]
TKS	Task, Knowledge, and Skill statements [Descripciones de tareas, conocimientos y habilidades]

Apéndice B - Glosario

Para obtener el glosario completo, sírvase visitar la página https://csrc.nist.gov/glossary.

Competencia Un mecanismo mediante el cual las organizaciones pueden evaluar al estudiante.

Conocimientos Conjunto de conceptos recuperables dentro de la memoria.

Habilidad La capacidad de realizar una acción observable.

Tarea Una actividad dirigida hacia el logro de los objetivos de la organización.