FGSI

ANÁLISIS DEL NICE NIST FRAMEWORK

Diciembre 2020

Ismael Jiménez Castro
Marco Santacroce

Universidad de Alcalá

Máster Universitario en Ciberseguridad

Índice

Índice de figuras

1. Introducción

1.1. Objetivo del Documento

En este documento que hemos elaborado, buscamos que el lector se acerque a entender la finalidad y, sobretodo, el funcionamineto del marco NICE. De está forma, podrá comprender el por qué de su necesidad para ser aplicado en la vida real y su gran utilidad.

En primer lugar, bajo nuestro punto de vista, los roles de trabajo, o work roles, son el elemento más importante de este marco, ya que hace que todos los elementos que lo componen se combinen para definirlos. El documento está centrado en este concepto. Pero para comprender qué es un rol de trabajo y cómo definirlo, primero hay que entender los elementos que conforman el marco y su funcionamiento. A ello le dedicamos el apartado 2.

En segundo lugar, hablaremos de los roles de trabajo, que se ubican en Categorías y áreas de Especialidad (Especialidades) dentro del marco. Estos dos elementos son fundamentales, puesto que son los que componen e identifican los roles. Este contenido viene definido en los apéndices del marco, donde también se habla de herrmientas para mejorar nuestra organización en el ámbito de la ciberseguridad.

Finalmente, acabaremos citando una serie de casos en los que el marco NICE se ha utilizado en la vida real, qué opinan a cerca de éste y cuál ha sido su resultado. También mencionaremos alguna certificación, en la que examina al candidato para comprobar cuál es su nivel de compresión de este framework que hoy en día tan demandado está.

1.2. ¿Qué es el NIST?

El National Institute of Standards and Technology (NIST) Fue fundado en el año 1901 y es parte del departamento de Comercio de Estados Unidos. Se trata del más antiguo de los laboratorios físicos de ciencia. Fue fundado en su momento para hacer competencia a las potencias industriales más importantes del momento (los rivales económicos más directos), que eran Alemania, Reino Unido, etc.

Sus logros van desde la red eléctrica inteligente y los registros electrónicos de salud hasta los relojes atómicos. Los nanomateriales avanzados y los chips de ordenadores, innumerables productos y servicios dependen de alguna manera de la tecnología, las mediciones y las normas proporcionadas por el Instituto Nacional de Normas y Tecnología, el NIST.

Cuando alguien piensa en el NIST, puede caer en la equivocación de pensar que tan solo se trata de un laboratorio cuya misión es simplemente mejorar las medidas establecidas. Sin embargo, su misión principal es potenciar la innovación y competencia industrial en Estados Unidos. Cuesta creer, en un primer lugar, cómo es posible que una agencia de medidas promueva la innovación tanto como lo hace el NIST. La razón es muy simple: sí sabemos medir algo, de cualquier manera, entonces podemos empezar a pensar en cómo diseñarlo, construirlo o mejorarlo. En cierto modo, si nos paramos a pensarlo, todo lo que nos rodea está basado en mediciones qué han sido previamente estandarizadas. En la gran mayoría de ellas, el NIST ha tomado un rol crucial para su creación.

Gracias a estos estándares, podemos hablar todos y cada uno de nosotros el mismo lenguaje en miles de materias distintas.

Figura 1: Logo NIST

1.3. ¿Qué es el NICE framework?

Con el crecimiento y desarrollo de internet tan rápido en los últimos años, los riesgos en la red han aumentado alarmantemente. Es por ello que en el año 2010 el gobierno de Estados Unidos decidió crear una nueva iniciativa dentro del NIST para estandarizar la ciberseguridad. A esta iniciativa se le denominó NICE: National Initiative for Cybersecurity Education. Dicho más formalmente, la Iniciativa Nacional para la Educación en materia de ciberseguridad (NICE) es una asociación entre el gobierno, el mundo académico y el sector privado centrada en el apoyo a la capacidad del país para hacer frente a los problemas actuales y futuros de la educación en materia de ciberseguridad y de la fuerza de trabajo mediante normas y prácticas óptimas. Pese a su creación en el 2010, la primera publicación oficial sobre este marco (framework) se realizó en el año 2017 (su desarrollo tuvo lugar en esos 7 años).

Figura 2: Logo NICE

2. NICE Framework

Como no podía ser de otra forma proviniendo del NIST, el marco NICE es un plan para categorizar, organizar y describir el trabajo de ciberseguridad en categorías, áreas de especialidad, funciones de trabajo, y conocimientos, destrezas y habilidades (KSA). Proporciona un lenguaje común para hablar de las funciones y trabajos cibernéticos y puede ser consultado por quienes deseen definir los requisitos profesionales en materia de ciberseguridad. puedan intercambiar información entre sí. El hecho de que las distintas organizaciones puedan intercambiar información entre sí es crucial para el desarrollo ágil y mejores prácticas en el mundo de la seguridad.

2.1. Organización del Framework

NICE está compuesto por cuatro comités. Cada uno de ellos lleva a cabo una función diferente y todos ellos son de esencial importancia para el desarrollo correcto y prosperidad de este marco.

1. **Consejo de Coordinación Interinstitucional de NICE (NICE Interagency Coordinating Council)**: Convoca a los socios del Gobierno Federal de NICE para la consulta, la comunicación y la coordinación de iniciativas políticas y orientaciones estratégicas relacionadas con la educación, la capacitación y el desarrollo de la fuerza de trabajo en materia de ciberseguridad. Las reuniones proporcionan una oportunidad para la Oficina de Programas de NICE, para comunicar las actualizaciones de los programas con los socios clave del Gobierno Federal para aprender sobre otras actividades del Gobierno Federal en apoyo de NICE. El grupo también identificará y discutirá temas de política y proporcionará información sobre las direcciones estratégicas para NICE.

2. **Consejo de Coordinación de la Comunidad NICE (NICE Community Coordinating Council)**: El Grupo de Trabajo NICE (NICE Working Group) proporciona un mecanismo para que los participantes del sector público y privado desarrollen conceptos, diseñen estrategias y lleven a cabo acciones que fomenten la educación, la

capacitación y el desarrollo de la fuerza laboral en materia de ciberseguridad. Las reuniones proporcionan una oportunidad para la consulta y el intercambio de información entre el gobierno, el mundo académico y el sector privado. El Grupo de Trabajo NICE también identifica nuevas iniciativas que apoyan los objetivos estratégicos de NICE.

3. **Comité del Programa de la Conferencia NICE (NICE Conference Program Committee)**: Este comité sirve como asesores expertos de la oficina del Programa NICE, coordinadores y anfitriones de la Conferencia NICE. El Comité del Programa es responsable de identificar el tema y las pistas de la conferencia, así como de solicitar y seleccionar propuestas de oradores para la conferencia.

4. **Comité de Planificación de la Conferencia de Educación sobre la Ciberseguridad NICE K12 (NICE K12 Cybersecurity Education Conference Planning Committee)**: Asiste y apoya a la oficina del Programa NICE, a los coordinadores y a los anfitriones de la Conferencia de Educación sobre ciberseguridad NICE K12.

2.2. Plan Estratégico de NICE: Objetivos

En 2020, NICE publicó un plan estratégico en una exposición anual (NICE Conference and Expo 2020). El plan establece una visión audaz para preparar, hacer crecer y mantener una personal de ciberseguridad que salvaguarde y promueva la seguridad nacional y la prosperidad económica de los Estados Unidos. Este "personal de ciberseguridadïncluye tanto a aquellos cuyo principal objetivo es la ciberseguridad como a los miembros de la fuerza de trabajo que necesitan conocimientos y aptitudes específicos relacionados con la ciberseguridad para realizar su trabajo de forma que las organizaciones puedan gestionar adecuadamente los riesgos relacionados con la ciberseguridad para la empresa.

Los objetivos estratégicos incluyen

1. Promover el descubrimiento de carreras y vías múltiples en materia de ciberseguridad

2. Transformar el aprendizaje para construir y mantener una fuerza laboral diversa y capacitada

3. Modernizar el proceso de gestión de talentos para hacer frente a las lagunas en materia de ciberseguridad

4. Ampliar el uso del Marco NICE

5. Impulsar la investigación para el desarrollo de prácticas efectivas del marco NICE.

2.3. Las Bases del Marco NICE

2.3.1. Background

La tecnología sigue evolucionando a un ritmo cada vez mayor. Concretamente, la tecnología que facilita la capacidad de acceder y procesar la información de forma rápida y eficiente está cambiando drásticamente. El trabajo requerido para diseñar, construir, asegurar e implementar estos datos, redes y sistemas aumenta en complejidad. Además, describir este trabajo y a quienes pueden realizarlo sigue siendo un desafío. Para agravar este problema, las organizaciones utilizan métodos variados y creados por ellas mismas para tratar de resolverlo.

El Framework NICE ayuda a las organizaciones a superar la barrera de describir su fuerza de trabajo a múltiples interesados presentando un enfoque de **bloques de construcción**. Mediante el uso de bloques de construcción conceptuales, el marco NICE presenta un lenguaje común para que las organizaciones lo utilicen internamente y con otros, tal y como se ha explicado en la introducción. Este enfoque permite a las organizaciones adaptar y aplicar el marco NICE a su contexto operativo único. Además, al crear un lenguaje común, el marco NICE reduce la barrera de entrada para las organizaciones que buscan entrar e interoperar con otras organizaciones.

La figura a continuación muestra una vista de alto nivel de NICE:

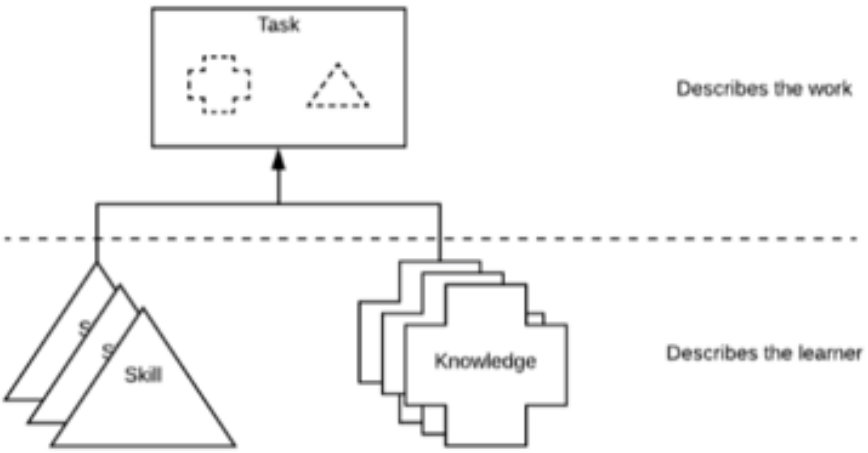

Figura 3: Bloques de Construcción (Alto Nivel)

Los principales bloques de construcción del Framework NICE son las declaraciones de Tareas, Conocimientos y Destrezas (TKS) que se muestran junto a los conceptos que describen: el "trabajo" (work) y el "aprendiz" (learner).

El **trabajo** es lo que necesita una organización para alcanzar los objetivos de gestión de riesgos de la ciberseguridad. El Framework NICE proporciona a las organizaciones una forma de describir su trabajo mediante declaraciones de tareas que agrupan declaraciones de conocimientos y destrezas (y habilidades).

El **aprendiz** es la persona que tiene conocimientos y destrezas, además de habilidades. Puede ser un estudiante, un buscador de empleo, un empleado u otras personas dentro de la fuerza de trabajo. Por lo tanto, todos los individuos son considerados aprendices debido a la educación o capacitación que recibieron antes de ingresar a la fuerza laboral, la capacitación continua, el autoaprendizaje o un plan de progresión de carrera. El Framework NICE proporciona a las organizaciones una forma de describir a los aprendices asociando declaraciones de Conocimientos y Destrezas a un individuo o grupo y, al utilizar sus conocimientos y destrezas, los aprendices pueden completr las tareas para lograr los objetivos de la organización; y al describir tanto el trabajo como el aprendiz, el framework NICE proporciona a las organizaciónes un lenguaje común para describir su trabajo en marteria de ciberseguridad y su fuerza de trabajo.

2.3.1.1 Atributos del Framework NICE

La forma del trabajo, y por consiguiente, la fuerza de trabajo, puede describirse utilizando los bloques de construcción del TKS; estos bloques de construcción incorporan los siguientes atributos:

1. **Agilidad:** la gente, los procesos y la tecnología maduran y deben adaptarse al cambio (NICE permite seguir el ritmo de un ecosistema en constante evolución).

2. **Flexibilidad:** aunque todas las organizaciones se enfrentan a retos similares, no existe una solución única para todos esos retos comunes (NICE permite dar cuenta del contexto operativo único de la organización)..

3. **Interoperabilidad:** aunque cada solución a los retos comunes es única, esas soluciones deben acordar un uso coherente de los términos (NICE permite intercambiar información sobre la fuerza de trabajo utilizando un lenguaje comun).

4. **Modularidad:** aunque el riesgo de ciberseguridad sigue siendo la base de este documento, existen otros riesgos que las organizaciones deben gestionar dentro de la empresa (NICE permite comunicarse acerca de otros tipos de fuerzas de trabajo dentro de una empresa y entre organizaciónes y sectores, como privacidad, gestión de riesgos, etc).

2.3.1.2 Propósito y Aplicabilidad

Pese a que ya hemos hablado del plan estrtégico del marco de NICE, queremos enfacitar brevemente este punto. Las organizaciones gestionan muchas funciones empresariales diferentes (como las operaciones, las finanzas, las cuestiones jurídicas y los recursos humanos) como parte de su empresa general. Cada una de esas funciones comerciales tiene riesgos asociados. A medida que la tecnología se ha convertido en un factor facilitador de la gestión de una empresa, los riesgos asociados a la seguridad cibernética también se han hecho más prominentes. El Framework NICE ayuda a las organizaciones a gestionar los riesgos de la ciberseguridad al proporcionar una forma de examinar el trabajo y los conocimientos asociados a la ciberseguridad.

NICE busca que las organizaciones desarrollen sus propios marcos de seguridad a partir de él según sus necesidades comerciales, proponiendo a través de sí una mejor gestión dentro de la organización.

2.3.1.3 Audiencia: ¿Hacia quién está orientado el marco NICE?

El marco NICE puede considerarse como un **diccionario no prescriptivo** de la fuerza de trabajo de la ciberseguridad. Los usuarios del Framework NICE que se remitan a él deben aplicarlo localmente con diversos fines de desarrollo de la fuerza de trabajo, educación o capacitación.

El marco de NICE está pensado para ser utilizado principalmente por cuatro grupos de personas pertenecientes a la fuerza laboral, que son los **Empleadores** (Employers), los **Aprendices**, que son Trabajadores de la Ciberseguridad actuales y futuros, y otros grupos de trabajadores (Learners), los **Educadores** (Educators/Trainers) y finalmente los **Proveedores de Tecnología** (Tech Providers).

1. **Empleadores**: Utilizando el vocabulario común del Framework NICE, les permite inventariar y desarrollar su fuerza de trabajo en materia de ciberseguridad. El marco NICE puede ser utilizado por los empleadores y los dirigentes de las organizaciones para diversas cosas, como el inventario y el seguimiento de su fuerza de trabajo en materia de ciberseguridad; la determinación de los requisitos de capacitación y calificación para desarrollar los conocimientos, las aptitudes y las habilidades fundamentales para el desempeño de las tareas de ciberseguridad; la mejora de las descripciones de los puestos y de los anuncios de vacantes mediante la selección de los acuerdos y tareas pertinentes una vez que se hayan identificado las funciones y tareas del puesto; la identificación de las funciones más importantes y el desarrollo de vías de carrera para orientar al personal en la adquisición de las aptitudes necesarias para esas funciones; y mucho más.

2. **Trabajadores de la Ciberseguridad actuales y futuros** y los que deseen entrar en el campo de la ciberseguridad, para explorar las tareas dentro de las categorías de la ciberseguridad y las funciones de trabajo. Además, NICE también ayuda a **quienes apoyan a estos trabajadores**, como los especialistas en recursos humanos y los

asesores de orientación, para ayudar a los solicitantes de empleo y a los estudiantes a comprender cuáles son las funciones de los puestos de trabajo de la ciberseguridad y qué conocimientos, aptitudes y habilidades asociados valoran los empleadores para los puestos de trabajo y los puestos de trabajo de la ciberseguridad requeridos.

3. **Educadores:** El NICE proporciona una referencia para el desarrollo de planes de estudio, certificados o programas de licenciatura, programas de capacitación, cursos, seminarios y ejercicios o desafíos que cubren los TKS (o también KSA) (conocimientos, destrezas y habilidades) y las tareas descritas en el Framework NICE.

4. **Proveedores de Tecnología:** NICE permite a un proveedor de tecnología identificar las funciones de trabajo de la ciberseguridad y los TKS (o también KSA) y las tareas asociadas a los productos y servicios de hardware y software que proporcionan.

2.3.2. Bloques de Construcción del marco NICE

El Framework NICE se basa en un conjunto de bloques de construcción discretos que describen el trabajo a realizar (en forma de Tareas) y aquello que se requiere para realizar ese trabajo (a través de Conocimientos y Destrezas).

Estos bloques de construcción son construcciónes organizativas que apoyan la usabilidad y implementación del Framework NICE. Proporciónan un mecanismo por el cual tanto organizaciónes como individuos pueden entender el alcance y el contenido del NICE.

Estos bloques de construcción están destinados a ser directrices que pueden ser utilizadas para mejorar la comprensión en lugar de estructuras rígidas.

2.3.2.1 Task Statements (Declaraciones de Tareas)

Las **Declaraciones de Tareas** describen el trabajo. Deben centrarse en el lenguaje y los patrones de comunicación de la organización que le dan valor.

Se trata de una actividad dirigida al logro de los objetivos tecnológicos o los objetivos de la misión. Las declaraciones de tareas describen el trabajo a realizar de forma fácil de leer y comprender, aunque pueden contener muchos pasos. Una declaración de Tarea comienza siempre con la actividad que se está ejecutando: "*Solucionar problemas de hardware y software del sistema*"

Y no contienen el objetivo de la tarea, puesto que éste puede variar: "*Realizar ejercicios de capacitación interactivo* "

Como se muestra en la figura que se ve en la sección Background, las Tareas están relacionadas con las declaraciones de **Destrezas (S)** y **Conocimientos (K)**, porque un aprendiz demostrará que posee el conocimiento y las destrezas para completar una Tarea

2.3.2.2 Knowledge Statements (Declaraciones de Conocimientos)

Las **Declaraciones de Conocimientos** describen el aprendiz. En general los conocimientos son el conjunto conceptos reversibles dentro de la memoria.

Las declaraciones de conocimiento se relacionan con las declaraciones de la Tarea en que sólo con la comprensión descrita mediante la declaración de conocimiento (Knowledge Statement) podrá el aprendiz completar la Tarea. Se pueden necesitar múltiples declaraciones de Conocimiento para completar una determinada Tarea y, de la misma manera, una declaración de Conocimiento puede ser utilizada para completar muchas Tareas diferentes.

Las declaraciones de conocimiento pueden describir conceptos generals: "*Conocimiento de las amenazas y vulnerabilidades del ciberespacio*" o conceptos específicos: "*Conocimiento de las fuentes de difusión de información sobre vulnerabilidades (por ejemplo, alertas a proveedores, avisos a gobiernos, erratas en la literatura sobre productos y boletines sectoriales)*"

2.3.2.3 Skill Statements (Declaraciones de Destrezas)

Las **Declaraciones de Destrezas** describen el aprendiz. En general, las destrezas se definen como la capacidad de realizar una acción observable.

Se relacionan con las declaraciones de tareas, en el sentido de que un aprendiz está demostrando que posee destrezas para realizarlas. Pueden ser necesarias varias declaraciones de destrezas para completar una tarea determinada y, de la misma manera, el ejercicio de una destreza puede utilizarse para completar más de una tarea.

Las declaraciones de destrezas describen tanto destrezas simples: "*Destrezas para reconocer las alertas de un sistema de detección de intrusos*" como complejas: "*Destrezas para generar una hipótesis de cómo un actor de la amenaza eludió el Sistema de Detección de Intrusos* ".

2.3.2.4 Conocimiento, Destrezas y Habilidades (KSAs)

Cuando hablamos de funciones de trabajo, los conocimientos, destrezas y habilidades (KSA) son los atributos necesarios para desempeñar las funciones de trabajo y generalmente se demuestran a través de la experiencia, la educación o la capacitación pertinentes.

En este caso, la **Habilidad** es la competencia para realizar un comportamiento observable o un comportamiento que resulte en un producto observable. En la versión anterior a noviembre de 2020, las habilidades eran ampliamente utilizadas y se emplean en multitud de empresas que utilizan el framework de NICE.

2.3.3. Utilización de los componentes del marco NICE

El objetivo del uso del Framework es no tener una estructura rígida en cuanto a los bloques de construcción. De hecho, siempre debemos tratar de promover la flexibilidad en la aplicación de NICE para el lenguaje común, porque esto es ventajoso en un contexto comercial.

En particular, se pueden utilizar los bloques de **TKS existentes**, como por ejemplo en el área de las habilidades de rastreo para determinar un ascenso, o los conocimientos necesarios para completar un curso o una lista de tareas mensuales a realizar;

De lo contrario, puede utilizar una estructura **TKS creada** por la propia empresa (por lo tanto, única), también porque es interesante crear nuevas declaraciones de Tareas, Conocimientos o Destrezas para la mejora de la empresa, ¡pero se debe recordar que NUNCA se deben modificar las existentes!

Ahora se van a proceder a identificar las diferentes aplicaciones de éstos bloques.

2.3.3.1 Competencias

Las Competencias son un mecanismo de evaluación necesario para los learners (aprendices). Se definen mediante un enfoque dirigido por el empleador y permiten a los aprendices cumplir los requisitos, por lo que son esenciales.

Las competencias se componen de cuatro dominios:

1. El nombre de la competencia

2. Una descripción de la competencia

3. Un método de evaluación

4. Las declaraciones respectivas de la TKS

Ofrecen flexibilidad para necesidades amplias, abiertas al cambio. Puede utilizar competencias ya definidas o crear otras nuevas en función de las necesidades de la organización.

Hay varias maneras de utilizar las competencias, mediante Declaraciones de Tareas o mediante Declaraciones de Destrezas y Conocimientos.

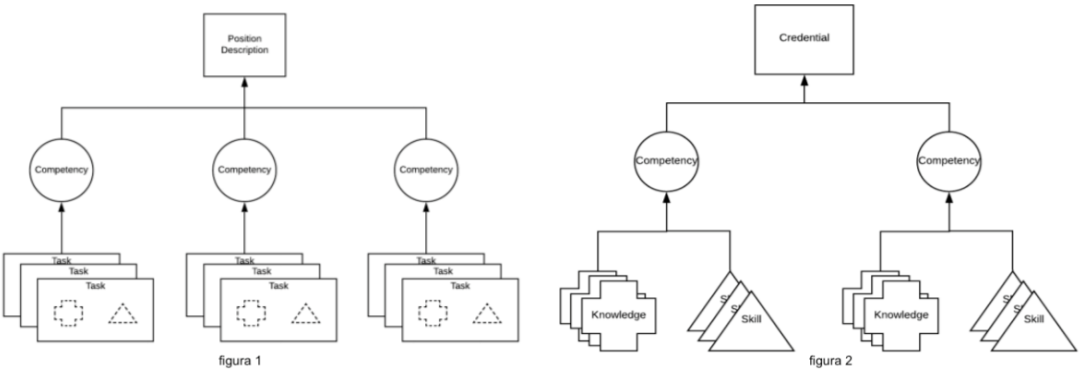

Figura 4: Competencias de NICE

2.3.3.2 Roles de Trabajo (Work Roles) y Título de Trabajo (Job Title)

El **Rol de Trabajo** es piedra angular de NICE. Pese a que se le dedican más contenido más adelante, vamos a hablar brevemente de qué son.

Los Roles de Trabajo son una forma de describir una agrupación de trabajo de la que alguien es responsable.

El Framework NICE fomenta un enfoque ágil a través de las Tareas, que incluyen declaraciones asociadas de Conocimientos y Destrezas que representan el potencial de los aprendices para llevar a cabo esas Tareas. Este enfoque transitivo, ilustrado en la figura 3, apoya la flexibilidad y simplifica la comunicación. Pero debemos tener cuidado de no confundirlo con un título de trabajo, pues no siempre son lo mismo.

El **Título de Trabajo** es una descripción de la posición o puesto de trabajo en una organización. Algunos puestos de trabajo pueden coincidir con el título del puesto, dependiendo del uso que haga la organización de estos. Una solo rolo de trabajo (por ejemplo, desarrollador de software) puede aplicarse a quienes tienen muchos títulos de trabajo diferentes (por ejemplo, ingeniero de software, codificador, desarrollador de aplicaciones). A la inversa, se pueden combinar múltiples roles para crear un trabajo en particular. Este enfoque aditivo permite mejorar la modularidad e ilustra el hecho de que todos los alumnos de la fuerza de trabajo realizan numerosas tareas en diversas funciones, independientemente de su cargo. Puedes usar un rol de trabajo existente o crear el tuyo propio.

Ahora que entendemos qué es un Rol de Trabajo y comprendemos en qué difiere de los títulos de trabajo, mostraremos una imagen para para observar visualmente cómo se compone un rol de trabajo en el NICE.

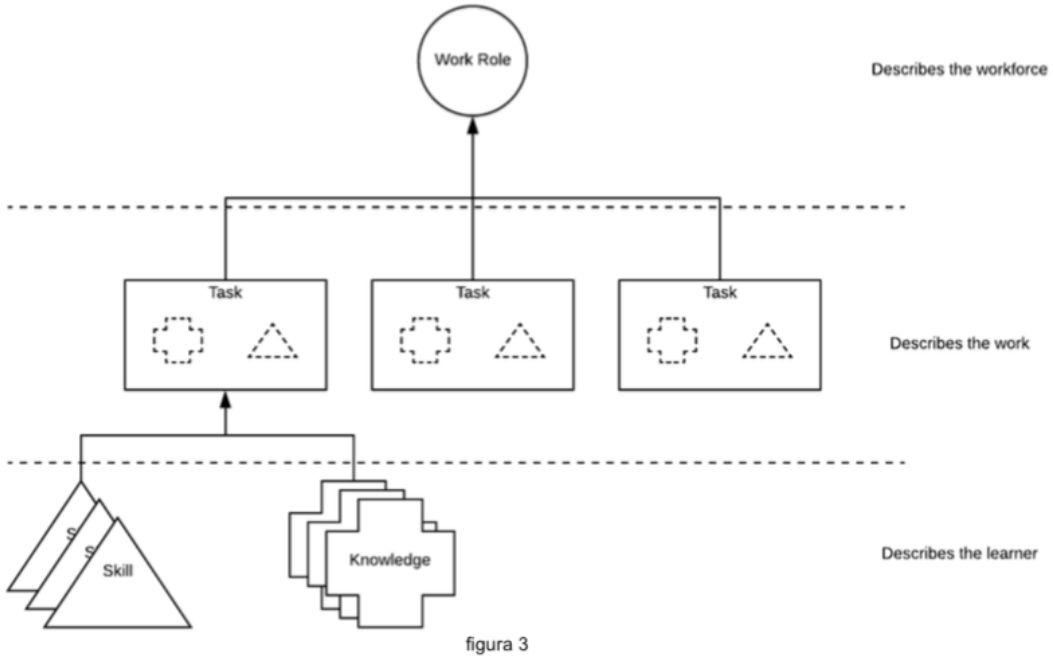

Figura 5: Roles de Trabajo de NICE

2.3.3.3 Equipos (Teams)

Muchas organizaciones utilizan equipos para abordar colectivamente desafíos complejos reuniendo a individuos con habilidades y experiencia complementarias. Al utilizar diferentes recursos y perspectivas, los **equipos** permiten a las organizaciones gestionar los riesgos de manera holística. Los equipos aprovechan la especialización de los conocimientos y los procesos de cada miembro para distribuir el trabajo con eficacia. **Los equipos pueden definirse utilizando Roles de Trabajo o Competencias**.

1. Un enfoque de la creación de equipos centrado en el **rol de trabajo** permite a las organizaciones definir qué tipos de funciones laborales son necesarias para alcanzar los objetivos definidos. Dado que los Roles de Trabajo se componen a su vez de Competencias, este enfoque para la construcción de equipos comienza con el trabajo a realizar. Este enfoque puede considerarse "de arriba hacia abajo". La siguiente tabla muestra una forma de crear un equipo de desarrollo de software seguro.

2. Los equipos también pueden construirse utilizando las **competencias**. Este enfoque para construir equipos reconoce que las Tareas individuales pueden ser desconocidas, pero los tipos de Competencias necesarias para resolver el desafío son conocidos. Este enfoque puede considerarse "de abajo hacia arriba". Por lo tanto, los equipos construidos de esta manera pueden ayudar a identificar a los alumnos que pueden participar en el trabajo del equipo en el futuro. Por ejemplo, un equipo defensivo de ciberseguridad que utiliza sus destrezas para imitar las técnicas de ataque de los adversarios (es decir, un .Equipo Rojo") puede estar compuesto por las siguientes Competencias teóricas:

    - Planificación del compromiso
    - Reglas de combate
    - Prueba de la pluma
    - Recopilación de datos
    - Explotación de la vulnerabilidad

3. Aplicabilidad en el mundo real: Apéndices

3.1. Apéndice A: Listado de los Elementos de NICE

3.1.1. Categorías del Framework NICE

Una vez concocemos los componentes básicos del framework, podemos adentrarnos más profundamente en sus funcionalidades. Comenzamos hablando por las categorías, que conforman una agrupación de alto nivel de funciones comunes de ciberseguridad. Cada una de las categorías viene definida por un nombre junto con una abreviación de dos caracteres que nos ayudará a identificar la categoría de forma más fácil y a agilizar la creación de los roles de trabajo definidos por el framework. Aunque bien es cierto que esto se publicó en el año 2017, lleva habiendo borradores desde el año 2010. Podemos decir pues, que el resultado ha sido altamente meditado por los mejores expertos de ciberseguridad que componen el NIST.

En total existen **7 categrorías** de las que se hablarán a continuación:

Figura 6: Categorías de NICE

3.1.1.1 Analyze (AN)

Esta es la categoría que se encarga de realizar un examen y evaluación altamente especializados de la información de ciberseguridad entrante para determinar su utilidad para la inteligencia. Gracias a este categoría, podemos tener un conocimiento más amplio sobre el contenido de información relacionado con este tema que desconozcamos.

3.1.1.2 Collect And Operate (CO)

Esta es la categoría en la que se proporciona operaciones especializadas de denegación de servicio y engaño o estafa y la recolección de información de ciberseguridad que puede ser utilizada para desarrollar inteligencia.

3.1.1.3 Investigate (IN)

Investiga eventos de ciberseguridad o delitos relacionados con sistemas de tecnología de la información (TI), redes y pruebas digitales. Como no puede ser de otra manera, al tratarse de una investigación según su definición, esta categroría queda definida como una que opera tras haber sucedido el evento o delito (siempre después).

3.1.1.4 Operate and Maintain (OM)

Aquí se nos proporciona el apoyo, la administración y el mantenimiento necesarios para garantizar el rendimiento y la seguridad de los sistemas de tecnología de la información (TI).

3.1.1.5 Oversee and Govern (OV)

Esta es la categoría que proporciona liderazgo, gestión, dirección o desarrollo y promoción para que la organización pueda llevar a cabo eficazmente la labor de ciberseguridad. A mejor organización y gobierno haya dentro de nuestra empresa (cuanto mejor gestionada esté), mejor será la productividad.

3.1.1.6 Protect and Defend (PR)

Categoría en la que se identifican, analizan y mitigan las amenazas a los sistemas y/o redes internas de tecnología de la información (TI). Es la categoría que se define básicamente

como la defensa frente a ataques a nuestro sistema.

3.1.1.7 Securely Provision (SP)

Aquí se conceptualizan, diseñan, procuran y/o construyen sistemas de tecnología de la información (TI) seguros, con responsabilidad sobre aspectos del desarrollo de sistemas y/o redes. Es otra de las categorías que se basa meramente en dotar a nuestro sistema de la seguridad necesaria en todo momento desde el inicio de su ciclo de vida.

3.1.2. Especialidades del Framework NICE

Las áreas de especialidades conforman distintas áreas de la ciberseguridad que componen las características de las que hemos hablado en la sección anterior. Por lo tanto, cabe recalcar que la definición de cada una de las categorías es la base de la que parten sus respectivas especialidades. Se utilizan también para definir de una forma más especifica los roles de trabajo y vienen descritas por un nombre junto con tres caracteres en lugar de dos (como pasaba en las categorías) para hacer una referencia mucho más ágil a éstas.

En total existen **33 especialidades**, que son las siguientes:

3.1.2.1 Especialidades en Analyze

- **Threat Analysis/Análisis de amenazas (TWA)**: Identifica y evalúa las capacidades y actividades de los delincuentes/piratas informáticos o entidades de inteligencia extranjeras. Adicionalmente, produce conclusiones para ayudar a iniciar o apoyar la ley investigaciones o actividades de represión y contrainteligencia.

- **Exploitation Analysis/Análisis de explotación (EXP)**: Analiza la información que ha sido reunida para identificar las vulnerabilidades y las posibilidades de explotación a nuestro sistema/s.

- **All-Source Analysis/Análisis de todas las fuentes (ASA)**: Analiza la información sobre amenazas de múltiples fuentes, disciplinas y agencias de la Comunidad de Inteligencia. Sintetiza y sitúa la información de inteligencia en su contexto; extrae información sobre las posibles implicaciones.

- **Targets/Objetivos (TGT)**: Aplica los conocimientos actuales de una o más regiones, países, entidades no estatales y sus respectivas tecnologías.
- **Language Analysis/Análisis del lenguaje (LNG)**: Aplica los conocimientos lingüísticos, culturales y técnicos para apoyar la recolección y el análisis de información y otras actividades de ciberseguridad.

3.1.2.2 Especialidades en Collect And Operate

- **Collection Operations/Operaciones de Recolección (CLO)** : Ejecuta la recolección utilizando estrategias apropiadas y dentro de las prioridades establecidas a través del proceso de gestión de la recolección que se tiene definido.
- **Cyber Operational Planning/Planificación Operativa Cibernética (OPL)**: Lleva a cabo un proceso de planificación de la ciberseguridad y de los objetivos conjuntos detenida y laboriosamente. Reúne información y desarrolla planes operativos detallados y órdenes de apoyo a las necesidades. También lleva a cabo una planificación estratégica y operacional de operaciones de información integrada y operaciones en el ciberespacio.
- **Cyber Operations/Operaciones Cibernéticas (OPS)**: Realiza actividades para reunir pruebas sobre entidades delictivas o de inteligencia extranjeras a fin de mitigar amenazas posibles o en tiempo real, protegerse contra el espionaje o las amenazas internas, el sabotaje extranjero, las actividades terroristas internacionales o para apoyar otras actividades de inteligencia.

3.1.2.3 Especialidades en Investigate

- **Cyber Investigation/Investigación Cibernética (INV)**: Aplica tácticas, técnicas y procedimientos para una amplia gama de herramientas de investigación y procesos que incluyen, pero no se limitan a la entrevista y el interrogatorio, técnicas, vigilancia, contravigilancia y detección de vigilancia. Como función adicional, también equilibra adecuadamente los beneficios del enjuiciamiento con los de la recopilación de inteligencia.

- **Digital Forensics/Forense Digital (FOR)**: Recoge, procesa, preserva, analiza y presenta pruebas relacionadas con la informática en apoyo de la mitigación de la vulnerabilidad de la red y/o el fraude criminal, contrainteligencia, o investigaciones de aplicación de la ley

3.1.2.4 Especialidades en Operate and Maintain

- **Data Administration/Administración de datos (DTA)**: Desarrolla y administra bases de datos y/o sistemas de gestión de datos que permiten el almacenamiento, la consulta, la protección y la utilización de los datos.
- **Knowledge Management/Gestión del conocimiento (KMG)**: Gestiona y administra procesos e instrumentos que permiten a la organización identificar, documentar y acceder al capital intelectual (la suma de todos los activos de la organización) y al contenido de la información.
- **Customer Service and Technical Support/Servicio de Atención al Cliente y Apoyo Técnico(STS)**: Aborda los problemas e instala, configura, soluciona los problemas y proporciona mantenimiento y capacitación en respuesta a las necesidades o consultas de los clientes. Normalmente proporciona información base sobre el incidente a la Especialidad de Respuesta a Incidentes (RI).
- **Network Services/Servicios de Red (NET)**: Instala, configura, prueba, opera, mantiene y gestiona redes y sus cortafuegos, incluidos los equipos y programas informáticos que permiten compartir y transmitir todas las transmisiones de información del espectro para apoyar la seguridad de la información y los sistemas de información.
- **Systems Administration/Administración de Sistemas (ADM)**: Instala, configura, soluciona problemas y mantiene las configuraciones de los servidores (hardware y software) para asegurar su confidencialidad, integridad y disponibilidad. También administra cuentas, cortafuegos y parches. Responsable del control de acceso, contraseñas y creación y administración de cuentas.
- **Systems Analysis/Análisis de Sistemas (ANA)**: Estudia los sistemas y procedimientos informáticos actuales de una organización y diseña soluciones de sistemas de

información para ayudar a la organización a funcionar de manera más segura, eficiente y eficaz. Reúne a las empresas y a la tecnología de la información (TI) comprendiendo las necesidades y limitaciones de ambas.

3.1.2.5 Especialidades en Oversee and Govern

- **Legal Advice and Advocacy/Asesoramiento y Promoción Jurídica (LGA)**: Proporciona asesoramiento y recomendaciones jurídicamente sólidas a la dirección y al personal sobre un variedad de temas relevantes dentro del dominio temático pertinente. Aboga por la legalidad y cambios de política, y hace un caso en nombre del cliente a través de productos de trabajo escritos y orales, como pueden ser los escritos y las actuaciones judiciales. Para esta especialización tendremos expertos en el ámbito legal.

- **Training, Education, and Awareness/Capacitación, Educación y Concienciación (TEA)**: Lleva a cabo la capacitación del personal dentro del dominio de la materia pertinente. Al fin y al cabo, son los humanos el componente de un sistema de cualquier tipo aquellos más prominentes a fallar. Desarrolla, planea, coordina, imparte y/o evalúa cursos de capacitación, métodos y técnicas como sea apropiado.

- **Cybersecurity Management/Gestión de la Ciberseguridad (MGT)**: Supervisa el programa de ciberseguridad de un sistema, incluyendo la gestión de las implicaciones de la seguridad de la información dentro de la organización, programa específico, u otra área de responsabilidad, para incluir personal estratégico, infraestructura, requisitos, aplicación de políticas, planificación de emergencias, seguridad la conciencia, y otros recursos.

- **Strategic Planning and Policy/Planificación Estratégica y Política (SPP)**: Desarrolla políticas y planes y/o aboga por cambios en la política que apoyen iniciativas organizativas en el ciberespacio o los cambios/mejoras necesarios.

- **Executive Cyber Leadership/Liderazgo Cibernético Ejecutivo (EXL)**: Supervisa, dirige y/o lidera el trabajo y los trabajadores que realizan ciber y relacionados con la cibernética y/o el trabajo de operaciones cibernéticas.

- **Program and Project Management and Acquisition/Gestión de Programas y Proyectos y Adquisición (PMA)**: Aplica el conocimiento de los datos, la información, los procesos, las interacciones organizativas, y experiencia analítica, así como sistemas, redes y capacidades de intercambio de información para gestionar **programas de adquisición** (término definido por el Departamento de defensa de EEUU como *un esfuerzo dirigido y financiado destinado a proporcionar una capacidad nueva, mejorada o automatizada del sistema de información (SIA) en respuesta a una necesidad operacional válida*).

  Ejecuta las tareas que rigen el hardware, el software y los programas de adquisición de sistemas de información y otras políticas de gestión de programas. Proporciona apoyo directo a las adquisiciones que utilizar la tecnología de la información (TI) (incluidos los sistemas de seguridad nacional), aplicando leyes y políticas relacionadas con la TI, y proporciona orientación relacionada con la TI en todo el ciclo de vida de adquisición total.

3.1.2.6 Especialidades en Protect and Defend

- **Cyber Defense Analysis/Análisis de Ciberdefensa (CDA)**: Utiliza medidas defensivas e información recopilada de diversas fuentes para identificar, analizar e informar de los acontecimientos que ocurren o podrían ocurrir dentro de la red para proteger la información, los sistemas de información y las redes contra las amenazas. Se trata de una especie de anticipación

- **Cyber Defense Infrastructure Support/Apoyo a la Infraestructura de Ciberdefensa (INF)**: Prueba (realizada constantemente), implementa, despliega, mantiene, revisa y administra el hardware y software de infraestructura que se requieren para administrar eficazmente la red de proveedores de servicios de defensa de la red de equipos y los recursos. Monitorea la red para remediar activamente las actividades no autorizadas.

- **Incident Response/Respuesta a Incidentes (CIR)**: Responde a las crisis o situaciones urgentes en el ámbito pertinente para mitigar amenazas inmediatas y potenciales. Utiliza enfoques de mitigación, preparación y respuesta y recuperación, según

sea necesario, para maximizar la supervivencia de la vida, la preservación de los bienes y la seguridad de la información. Investiga y analiza todos los aspectos relevantes actividades de respuesta.La investigación y análisis dentro de esta especialización es fundamental para proporcionar una respuesta robusta: está directamente relacionada con otras especialidades.

- **Vulnerability Assessment and Management/Evaluación y Gestión de las Vulnerabilidades (VAM)**: Realiza evaluaciones de las amenazas y vulnerabilidades; determina las desviaciones de las configuraciones aceptables, la empresa o la política local; evalúa el nivel de riesgo; y desarrolla y/o recomienda las contramedidas de mitigación apropiadas en situaciones operacionales y no operacionales.

3.1.2.7 Especialidades en Securely Provision

- **Risk Management/Gestión de Riesgos (RSK)**: Supervisa, evalúa y apoya la documentación, validación, evaluación y procesos de autorización necesarios para asegurar que la información existente y la que viene nueva los sistemas de tecnología de la información (TI) satisfacen los requisitos de la ciberseguridad y el riesgo de la organización. Asegura el tratamiento/gestión apropiado del riesgo, el cumplimiento y la garantía desde perspectivas internas y externas, pieza angular para cualquier organización cuando se produce algún ataque.

- **Software Development/Desarrollo del Software (DEV)**: Desarrolla y escribe o codifica aplicaciones informáticas, software o programas de utilidades especializadas siguiendo las mejores prácticas de aseguramiento de software. Todo este material puede ser nuevo o ya existentes.

- **Systems Architecture/Arquitectura de Sistemas(ARC)**: Desarrolla los conceptos de sistemas y trabaja en las fases de capacidad del ciclo de vida de desarrollo de sistemas; se encarga de transformar la tecnología y las condiciones ambientales (como puede ser la ley y la reglamentación o una normativa concreta) en diseños y procesos de sistemas y de seguridad.

- **Technology R&D/Tecnología R&D (TRD)**: Realiza la evaluación de la tecnología y los procesos de integración y evalúa su utilidad.
- **Systems Requirements Planning/Requerimentos de Planificación del Sistema (SRP)**: Consulta con los clientes para reunir y evaluar los requisitos funcionales y traduce estos requisitos en soluciones técnicas. Proporciona orientación a los clientes sobre la aplicabilidad de los sistemas de información para satisfacer las necesidades comerciales. Hoy en día, los enfoques de desarrollo ágil involucran al cliente dentro del proceso de planificación, a diferencia de los enfoques tradicionales, donde esto era inpensable.
- **Test and Evaluation/Probar y Evaluar (TST)**: Desarrolla y realiza pruebas de sistemas para evaluar el cumplimiento de las especificaciones y requisitos aplicando principios y métodos para la planificación rentable, evaluando, verificando y validando las características técnicas, funcionales y de rendimiento de los sistemas que incorporan la TI. La interoperabilidad de los sistemas es fundamental.
- **Systems Development/Desarrollo de Sistemas (SYS)**: Trabaja en las fases de desarrollo del ciclo de vida del desarrollo de sistemas

Figura 7: Visualización de Categorías y Especialidades

3.1.3. Roles de Trabajo del Framework NICE

Una vez hemos descrito las categorías y sus respectivas especializades, vamos a proceder a definir los diferentes roles de trabajo que aparecen en el NICE. Podría considerarse la pieza angular en la que está basada este framework de seguridad. Pese a que ya hemos hablado de los "work roles.º roles de trabajo, citaremos una breve frase como recordatorio del concepto. Los roles de trabajo son los agrupamientos más detallados de la ciberseguridad, que comprenden una serie de conocimientos, destrezas y habilidades (knowledge, skill and agility, KSA) necesarios para realizar una tarea específica (task).

El framework de NICE define un total de 52 roles de trabajo cada uno de ellos identificado a su vez por una respectiva especialidad dentro de una categoría. Para facilitarle la comprensión al lector, hemos creado una imagen para observar cómo podría verse esta relación de conceptos abstractos de forma más sencilla.

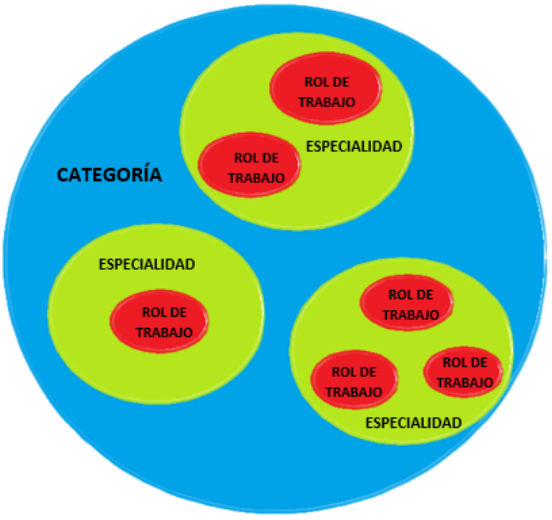

Figura 8: Relación Categoría-Especialidad-Work Role

Un rol de trabajo queda identificado por su respectivo nombre y un id (Work Role ID), que está compuesto en primer lugar por los caracteres de la categoría, seguido de los caracteres de la respectiva especialidad y finalmente por el número de rol de trabajo que le corresponda dentro de una especialidad. A estos roles de trabajo les acompaña una descripción, que a menudo echan mano de documentación externa para ser definidos, aunque en la mayoría de los casos no es así. Debido a la amplia gama de roles de trabajo que hay, haremos una breve

mención de cada uno de ellos correspondiéndose con su respectiva categoría y especialidad.

3.1.3.1 Work Roles dentro de la Categoría Analyze (AN)

- **Work Roles dentro de Análisis de Amenazas (TWA)**

  1. Analista de Alerta de Amenazas (Threat Warning Analyst): AN-TWA-002

- **Work Roles dentro de Análisis de Explotación (EXP)**

  1. Analista de Explotación (Exploitation Analyst): AN-EXP-001

- **Work Roles dentro de Análisis All-Source (ASA)**

  1. Analista All-Source (All-Source Analyst): AN-ASA-001
  2. Especialista de evaluación de misiones (Mission Assessment Specialist): AN-ASA-002

- **Work Roles dentro de Objetivos (TGT)**

  1. Desarrollador de Objetivos (Target Developer): AN-TGT-001
  2. Analista de la Red de Objetivos (Target Network Developer): AN-TGT-002

- **Work Roles dentro de Análisis de lenguaje (LNG)**

  1. Analista de Lenguaje Multidisciplinario (Multi-Disciplined Language Analyst): AN-LNG-001

3.1.3.2 Work Roles dentro de la Categoría Recolección y Operación (CO)

- **Work Roles dentro de Operaciones de Recolección (CLO)**

  1. Manager de Recolección All-Source (All Source-Collection Manager): CO-CLO-001
  2. Manager de Requerimientos de Recolección All-Source (All Source-Collection Requirements Manager): CO-CLO-002

- **Work Roles dentro de Planning Ciberoperacional (OPL)**

1. Planificador de Ciberinteligencia (Cyber Intel Planner): CO-OPL-001
2. Planificador de Ciberoperaciones (Cyber Ops Planner): CO-OPL-002
3. Planificador de Integración de Socios (Planificador de integración de socios): CO-OPL-003

- **Work Roles dentro de Ciberoperaciones (OPS)**

1. Ciberoperador (Cyber Operator): CO-OPS-001

3.1.3.3 Work Roles dentro de la Categoría Investigación (IN)

- **Work Roles dentro de Ciberinvestigación (INV)**

1. Investigador de Cibercrímenes (Cyber Crime Investigator): IN-INV-001

- **Work Roles dentro de Forense Digital (FOR)**

1. Analista Forense de Aplicación de la Ley/Contrainteligencia (Law Enforcement/Counterintelli Forensics Analyst): IN-FOR-001
2. Analista Forense de Ciberdefensa (Cyber Defense Forensics Analyst): IN-FOR-002

3.1.3.4 Work Roles dentro de la Categoría Operativa y Mantenimiento (OM)

- **Work Roles dentro de Administración de Base de Datos (DTA)**

1. Administrador de Base de Datos (Database Administrator): OM-DTA-001
2. Analizador de Datos (Data Analyst): OM-DTA-002

- **Work Roles dentro de Gestión del Conocimientos (KMG)**

1. Gestor de Conocimientos (Knowledge Manager): OM-KMG-001

- **Work Roles dentro de Servicio de Atención al Cliente y Apoyo Técnico (STS)**

1. Especialista en Apoyo Técnico (Technical Support Specialist): OM-STS-001

- **Work Roles dentro de Servicios de Red (NET)**

    1. Especialista en Operaciones de Red (Network Operations Specialist): OM-NET-001

- **Work Roles dentro de Administración de Sistemas (ADM)**

    1. Administrador de Sistemas (System Administrator): OM-ADM-001

- **Work Roles dentro de Análisis de Sistemas (ANA)**

    1. Analista de Sistemas de Seguridad (Systems Security Analyst): OM-ANA-001

3.1.3.5 Work Roles dentro de la Categoría de Supervisión y Gobierno (OV)

- **Work Roles dentro de Asesoramiento y defensa legal (LGA)**

    1. Asesor Jurídico Cibernético (Cyber Legal Advisor): OV-LGA-001
    2. Oficial de Privacidad/Gerente de Cumplimiento de la Privacidad (Privacy Officer/Privacy Compliance Manager): OV-LGA-002

- **Work Roles dentro de Capacitación, Educación y Concienciación (TEA)**

    1. Desarrollador de Currículum de Instrucción Cibernética (Cyber Instructional Curriculum Developer): OV-TEA-001
    2. Instructor Cibernético (Cyber Intructor): OV-TEA-002

- **Work Roles dentro de Gestión de la Ciberseguridad (MGT)**

    1. Manager de Seguridad de Sistemas de Información (Information Systems Security Manager): OV-MGT-001
    2. Manager de Seguridad de las Comunicaciones (COMSEC): OV-MGT-002

- **Work Roles dentro de Planificación Estratégica y Politicas (SPP)**

    1. Desarrollador y Manager de la fuerza de trabajo (workforce) de Seguridad (Cyber Workforce Developer and Manager): OV-SPP-001

2. Planificador de Políticas y Estrategias cibernéticas (Cyber Policy and Strategy Planner): OV-SPP-002

- **Work Roles dentro de Liderazgo Cibernético Ejecutivo (EXL)**

1. Liderazgo Cibernético Ejecutivo (Executive Cyber Leadership): OV-EXL-001

- **Work Roles dentro de Gestión de Programas y Proyectos y Adquisición (PMA)**

1. Gestor de Programas (Program Manager): OV-PMA-001
2. Director de Proyector de la TI (IT Project Manager): OV-PMA-002
3. Gestor de Soporte de Productos (Product Support Manager): OV-PMA-003
4. Gestor de Inversiones/Cartera de la TI (IT Investment/Portfolio Manager): OV-PMA-004
5. Auditor de Programas de la TI (IT Program Auditor): OV-PMA-005

3.1.3.6 Work Roles dentro de la Categoría de Protección y Defensa (PR)

- **Work Roles dentro de Análisis de Ciberdefensa (CDA)**

1. Analista de Ciberdefesa (Cyber Defense Analyst): PR-CDA-001

- **Work Roles dentro de Apoyo a la Estructura de Ciberdefensa (INF)**

1. Especialista en Apoyo a la Estructura de Ciberdefensa (Cyber Defense Infrastructure Support Specialist): PR-INF-001

- **Work Roles dentro de Respuesta a Incidentes (CIR)**

1. Respondedor de Incidentes de Ciberdefensa (Cyber Defense Incident Responder): PR-CIR-001

- **Work Roles dentro de Evaluación y Gestión de Vulnerabilidades (VAM)**

1. Analista de Evaluación de la Vulnerabilidad (Vulnerability Assessment Analyst): PR-VAM-001

3.1.3.7 Work Roles dentro de la Categoría Provisión de la Seguridad (SP)

- **Work Roles dentro de Gestión de Riesgos (RSK)**

  1. Oficial autorizador/Representante Designador (Authorizing Official/Designating Representative): SP-RSK-001
  2. Asesor de Control de Seguridad (Security Control Assessor): SP-RSK-002

- **Work Roles dentro de Desarrollo de Software (DEV)**

  1. Desarrollador de Software (Software Developer): SP-DEV-001
  2. Asesor de Software Seguro (Secure Software Assessor): SP-DEV-002

- **Work Roles dentro de Arquitectura de Sistemas (ARC)**

  1. Arquitecto de Empresa (Enterprise Architect): SP-ARC-001
  2. Arquitecto de Seguridad (Security Architect): SP-ARC-002

- **Work Roles dentro de Tecnología R&D (TRD)**

  1. Especialista en Investigación y Desarrollo (Research & Development Specialist): SP-TRD-001

- **Work Roles dentro de Planificación de Requerimientos de Sistemas (SRP)**

  1. Planificador de los Requerimientos del Sistema (Systems Requirements Planner): SP-SRP-001

- **Work Roles dentro de Test y Evaluación (TST)**

  1. Especislista en Pruebas y Evaluación del Sistema (System Testing and Evaluation Specialist): SP-TST-001

- **Work Roles dentro de Desarrollo de Sistemas (SYS)**

  1. Desarrollador de Seguridad de Sistemas de la Información (Information Systems Security Developer): SP-SYS-001
  2. Desarrollador de Sistemas (Systems Developer): SP-SYS-002

3.1.4. Tareas, Conocimientos, Destrezas y Habilidades

Las siguientes secciones de este apéndice (desde la 4 hasta la 7) conforman un listado de tareas, conocimientos y destrezas en secciones separadas. El framework de NICE proporciona una enorme lista de cada de ellas

1. Una lista de **1007 Tareas**, definidas en una tabla con dos columnas. Estas Tareas vienen identificadas con una letra, la **T** (Task) junto con su correspondiente identificador. A la derecha la definición de la Tarea que será utilizada para definir una determinada competencia o rol de trabajo (Apéndice B).

2. Una lista de **630 Conocimientos**, definidos en una tabla con dos columnas. Estos Conocimientos vienen identificados con una letra, la **K** (Knowledge) junto con su correspondiente identificador. A la derecha la definición del Conocimiento que podrá ser utilizado para definir una determinada competencia o rol de trabajo (Apéndice B).

3. Una lista de **374 Destrezas**, definidas en una tabla con dos columnas. Estas Destrezas vienen identificadas con una letra, la **S** (Skill) junto con su correspondiente identificador. A la derecha la definición de la Destrezas que será utilizada para definir una determinada competencia o rol de trabajo (Apéndice B).

4. Una lista de **176 Habilidades**, definidas en una tabla con dos columnas. Estas Habilidades vienen identificadas con una letra, la **A** (Ability) junto con su correspondiente identificador. A la derecha la definición de la Habilidades que será utilizada para definir una determinada competencia o rol de trabajo (Apéndice B).

3.2. Apéndice B: Listado de Roles de Trabajo

Como puede deducir por el título, en este apéndice se describen de forma más íntegra los roles de trabajo se los que se habla en el su respectiva sección del Apéndice A. Se relacionan, en forma de tabla, todos los conceptos de los hablados en el apéndice anterior en el orden descrito a continuación y de la siguiente manera:

1. El nombre del rol de trabajo.

2. Una identificación única de la función de trabajo del marco NICE, basada en las abreviaturas del NICE Categoría marco y área de especialidad a la que pertenece ese rol de trabajo.

3. El área de especialidad en la que reside el rol de trabajo.

4. El área de especialidad en la que reside el rol de trabajo.

5. La Categoría en la que reside el rol de trabajo.

6. Una descripción del rol de trabajo.

7. Una lista de las tareas (Tasks) del marco NICE que una persona en un puesto de ciberseguridad que incluye el rol de trabajo que se podría esperar que desempeñara.

8. Una lista de las áreas de conocimiento (Knowledge) del marco NICE que una persona en un puesto de ciberseguridad que incluye el rol de trabajo que se podría esperar que se exhibiera.

9. Una lista de las destrezas (Skills) del marco NICE que una persona en un puesto de ciberseguridad que incluye el rol de trabajo que se podría esperar que tuviera.

10. Una lista de las habilidades (Abilities) del marco NICE que una persona en una posición de ciberseguridad que incluye el rol de trabajo que se espera que demuestre.

Una vez conocemos la estructura, se definen las tablas conteniendo cada uno de los roles de trabajo (52). Para facilitar la comprensión del lector, tomaremos un par de ejemplos que aparecen en el documento oficial publicado por el NIST 800-181, en el que aparecen las tablas modelo.

En la primera de las imágenes podemos observar que nos encontramos ante el rol de trabajo de Analista Forense de Ciberdefensa identificado ocn IN-FOR-002. Está ubicado dentro del área de especialidad de Forense Digital (FOR), que pertenece a su vez a la categoría de Investigación (IN). Justo debajo viene la descripción del rol, que como puede un imaginarse, es realizar investigaciones en profundidad sobre delitos informáticos estableciendo pruebas documentales o físicas, para incluir medios digitales y registros asociados a incidentes de ciberintrusiones. Seguida de ésta, vienen las respectivas tareas, conocimientos, destrezas y

habilidades que el aprendiz debe cumplir.

Work Role Name	**Cyber Defense Forensics Analyst**
Work Role ID	**IN-FOR-002**
Specialty Area	**Digital Forensics (FOR)**
Category	**Investigate (IN)**
Work Role Description	Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.
Tasks	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
Knowledge	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
Skills	S0032, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093, S0131, S0132, S0133, S0156
Abilities	A0005, A0043

Figura 9: Rol de Trabajo Analista Forense de Ciberdefensa

En la segunda de las imágenes podemos observar que nos encontramos ante el rol de trabajo de Respondedor a Incidentes de Ciberdefensa identificado con PR-CIR-001. Está ubicado dentro del área de especialidad de Respuesta a Incidentes (CIR), que pertenece a su vez a la categoría de Protección y Defensa (PR). Justo debajo viene la descripción del rol, que consiste en investigar, analizar y responder a ciberincidentes dentro del entorno o enclave de la red. Seguida de ésta, aparecen las respectivas tareas, conocimientos, destrezas y habilidades que el aprendiz debe cumplir.

Work Role Name	**Cyber Defense Incident Responder**
Work Role ID	**PR-CIR-001**
Specialty Area	**Incident Response (CIR)**
Category	**Protect and Defend (PR)**
Work Role Description	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
Tasks	T0041, T0047, T0161, T0163, T0164, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0395, T0503, T0510
Knowledge	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
Skills	S0003, S0047, S0077, S0078, S0079, S0080, S0173, S0365
Abilities	A0121, A0128

Figura 10: Rol de Trabajo Respondedor a Incidentes de Ciberdefensa

Como hemos comentado previamente, existen otros 50 roles de trabajo, que no vamos a escribir para no hacer hacer este documento redundante. Todas siguen la misma estructura y pueden pertenecer a 7 Categorías diferentes y a 33 áreas de Especialidad diferentes.

3.3. Apéndice C: Listado de Herramientas

El apéndice C es ciertamente útil para diversas organizaciones, ya que en él se examinan los instrumentos de desarrollo de la fuerza de trabajo; concretamente, en este apéndice se hace referencia a **tres** tipos de instrumentos (o conjunto de instrumentos) que pueden ser de gran ayuda para las organizaciones en la esfera de la ciberseguridad y en otros ámbitos:

1. El Conjunto de herramientas para Desarrollo de la Fuerza de Trabajo de Ciberseguridad del DHS (DHS Cybersecurity Workforce Development Toolkit, CWDT).

2. La Herramienta de Construcción de Excelencia en Ciberseguridad de Baldrige (Baldrige Cybersecurity Excellence Builder Tool).

3. La Herramienta de Redacción de Descripción de Puestos (Position Description Drafting Tool: PushbuttonPD).

3.3.1. Conjunto de herramientas para Desarrollo de la Fuerza de Trabajo de Ciberseguridad del DHS: CWDT

El **Conjunto de herramientas de desarrollo de la fuerza de trabajo en materia de ciberseguridad del Departamento de Seguridad Nacional (DHS)**, ayuda a cualquier organización a comprender las necesidades de ciberseguridad de su fuerza laboral y de su personal para proteger la información, los clientes y las redes (por lo que es útil no sólo para el negocio, sino también para los clientes que lo utilizan). Este conjunto de herramientas (en este caso estamos describiendo un conjunto de herramientas) incluye plantillas de trayectorias profesionales en materia de ciberseguridad y recursos de contratación para reclutar y retener a los mejores talentos en materia de ciberseguridad, lo cual es fundamental porque de este modo se mantienen altos niveles de personal y se dispone de una fuerza de trabajo altamente cualificada.

Por consiguiente, el **CWDT** (Cybersecurity Workforce Development Toolkit) proporciona un conjunto de herramientas que ayudan a comprender los riesgos del personal de ciberseguridad de una organización y a hacer un inventario del personal de una organización. Estas herramientas aprovechan las áreas de especialización y los Conocimientos, Destrezas y Habilidades (KSA) y las Tareas (Tasks) del Framework NICE. El CWDT comienza ilustrando

que el primer paso para preparar una fuerza de trabajo para la ciberseguridad es una visión compartida para organizar su fuerza de trabajo en materia de ciberseguridad; esto se debe a que el hecho de tener una visión compartida apoya a los líderes a responder a los entornos cambiantes, al tiempo que proporciona datos para ajustar mejor los recursos, ver las pautas de trabajo y destacar las áreas de riesgo potencial.

El CWDT, en su conjunto de herramientas, incluye un Modelo de Madurez de la Capacidad de Planificación de la Fuerza de Trabajo en materia de ciberseguridad (CMM), una herramienta de autoevaluación para ayudar a una organización a evaluar la madurez de su capacidad de planificación de la fuerza de trabajo en materia de ciberseguridad.

El CWDT también ofrece perfiles como guía para centrarse en la retención del personal a todos los niveles, entendiendo por todos los niveles ya sean profesionales de la ciberseguridad, principiantes, personas a mitad de carrera o expertos en la materia.

Cuando hablamos de CWDT, es importante mirar con atención los niveles de habilidad y las trayectorias profesionales. Esto se debe a que el desarrollo y el intercambio de trayectorias profesionales con los empleados les ayudará a identificar sus niveles de aptitudes y a avanzar en las trayectorias profesionales de la ciberseguridad, por lo que es muy importante para la educación y las nuevas aptitudes que un empleado de una organización puede aprender durante su carrera laboral.

De hecho, el CWDT incluye un proceso de tres pasos para desarrollar las trayectorias profesionales de la ciberseguridad para su organización. Estos pasos son los siguientes:

1. Familiarizarse con los niveles de habilidad y revisar ejemplos de trayectorias profesionales (por lo tanto, un enfoque inicial y una visión general).

2. Utilizar una plantilla de CWDT para crear trayectorias profesionales específicas de ciberseguridad para su organización rellenando “Experiencia y credenciales recomendadas”, “Destrezas y competencias de muestra/KSA” y “Actividades de formación y desarrollo recomendadas”.

3. Compartir las trayectorias profesionales con los directores y el personal de ciberseguridad.

3.3.2. Herramienta de Construcción de Excelencia en Ciberseguridad de Baldrige

Una vez que una organización ha determinado sus requisitos de ciberseguridad (por ejemplo, mediante una auditoría de ciberseguridad o una autoevaluación interna), puede remitirse al Framework NICE para identificar las funciones y tareas del trabajo que ayudarán a cumplir esos requisitos. Si bien históricamente se han utilizado términos generales, como "profesionales de la tecnología de la información", para medir las necesidades, la especificidad que ofrece el Marco NICE proporciona un mejor enfoque para describir las docenas de funciones laborales discretas que se requieren. Al determinar las aptitudes necesarias y disponibles, y al identificar las lagunas entre las aptitudes necesarias y las disponibles, una organización puede determinar las necesidades críticas. El Framework NICE ayuda a una organización a responder a las siguientes preguntas, extraídas de la segunda herramienta de este apéndice, **la Herramienta de Construcción de Excelencia en Ciberseguridad de Baldrige**, relacionadas con el mantenimiento de un entorno de trabajo eficaz y de apoyo para alcanzar sus objetivos de ciberseguridad. Estas preguntas son:

1. ¿Cómo evalúa las capacidades y necesidades de su personal en relación con la ciberseguridad?.

2. ¿Cómo organiza y gestiona su personal de ciberseguridad para establecer funciones y responsabilidades?.

3. ¿Cómo prepara a su fuerza de trabajo para cambiar las capacidades de ciberseguridad y las necesidades de capacidad?.

A medida que más organizaciones evalúan su personal de ciberseguridad, el léxico común del Framework NICE permite la evaluación de las capacidades y necesidades de capacidad a través de múltiples organizaciones, sectores industriales y regiones.

3.3.3. Herramienta de Redacción de Descripción de Puestos

La tercera herramienta de este apéndice es la herramienta **PushbuttonPD** de la Iniciativa de Apoyo a la Gestión de Ciberdestrezas del DHS, que permite a los gerentes, supervisores

y especialistas en recursos humanos redactar rápidamente la descripción de un puesto de empleado federal (PD) sin necesidad de una amplia capacitación o de un conocimiento previo de la clasificación del puesto. Está diseñado para presentar un lenguaje de múltiples fuentes autorizadas y normas de misión crítica para los deberes, las Tareas y las KSA para captar rápidamente los requisitos del funcionario contratante y presentarlos en un paquete de contratación robusto que pueda integrarse fácilmente en los procesos de recursos humanos existentes del organismo. Cualquier organización puede experimentar con la herramienta PushbuttonPD para ver cómo el material del NICE Framework encaja en la descripción del trabajo.

4. Casos de Uso del Framework de NICE

Ahora conocemos al completo el funcionamiento del marco NICE: componentes, distribución, aplicabilidad, destinatarios, etc. No es ningún secreto que la organización de NICE es fantástica y una gran idea a aplicar en muchas organizaciones. Sin embargo, en ningún momento hemos hablado de ejemplos reales en los cuales una compañía u organización decide aplicar este marco para su funcionamiento Y para ello destinamos esta sección.

Como hemos comentado en la introducción del documento, aunque no nos demos cuenta, el NIST está presente en gran parte de las organizaciones hoy día. Su incidencia es increíble. Como no podía ser de otra forma, las implementaciones qué propone NICE no iban a ser una excepción.

El 18 de marzo de 2020, el NICE organizó una conferencia online (no presencial, ya que era en época de pandemia) en la que fueron invitadas dos organizaciones que habían implantado el marco para su funcionamiento básico. Uno de los pilares de este framework, como venimos diciendo desde el principio, es la flexibilidad. en esta conferencia (webminar) las empresas invitadas hablaron de su experiencia, sus mejoras/cambios respecto al marco NICE Y su experiencia con su uso.

El seminario estaba dirigido por el director del NICE, Rodney Petersen, en la que también intervenía Danielle Santos (Manager del Programa) Para dar unas nociones básicas de casos de uso a los asistentes a la charla y más adelante tomaban la voz las dos organizaciones invitadas: el CEO de **IQ4** (Frank Cicio) y la CEO de **CyberVista** (Simone Petrella) y su Jefe de Producción (Jung Lee). Ambas son dos workforces (fuerza laboral) que se han desarrollado utilizando NICE como base.

4.1. Empleabilidad/Uso de NICE (según Danielle Santos)

"NICE categoriza, organiza y describe el trabajo de la ciberseguridad"

La Program Manager de NICE aporta una serie de sectores es para los que puede ser utilizado el marco:

- Empleadores del sector público y privado
- Proveedores de educación

- Desarrolladores de tecnología
- Trabajadores de la ciberseguridad actuales y futuros
- Proveedores de capacitación y certificación
- Responsables de la formulación de políticas

Como no podía ser de otra forma, los casos de uso de los que hablaremos aplican el marco para los sectores mecionados.

4.2. IQ4: Transforming the learning economy

IQ4 es un workforce o fuerza laboral fundado en el año 2007 por Frank Cicio. Según las propias palabras del CEO de la compañía, IQ4 vio en el marco el base para orientar su tecnología hacia algo que hoy en día desafortunadamente escasea en el mercado: Ayudar a los aprendices a retener sus destrezas, identificar donde fallan o hay fallos, ayudarles a alcanzar sus metas el mundo de la tecnología y hacerles capaces de ayudar a organizaciones tanto internamente como externamente. El objetivo de IQ4 es encontrar y alimentar el talento y crecimiento mediante la transformación de la economía del aprendizaje mediante:

1. La optimización de la inversión en la búsqueda, desarrollo y retención del talento.
2. La interrupción del statu quo de la compra de un sistema de talento construyendo una a escala, usando nuestras herramientas, modelos y contenido
3. El potencial de nuestra empresa, los compromisos académicos y estudiantiles.
4. La solución de la brecha de habilidades que existe internamente en la empresa, el sector público y las escuelas está en el centro de nuestra empresa y los mercados sociales.

Los pilares de esta organización se fundamentan en tres declaraciones basadas en la aplicación del marco NICE:

1. Para que una empresa sepa qué tiene, primero debe saber qué necesita. Por ello, IQ4 comenzó definiendo los roles de trabajo y KSA (Knowledge, Skills y Abilities) como perfiles para la compañía para poder identificar cuáles son sus necesidades, y también

para las competencias del objetivo, añadiendo esta propia compañía este apartado por su cuenta. Para la organización, es importante tener en cuenta además de las destrezas los sueldos del aprendiz para saber hasta qué punto se le puede exigir una serie de competencias o no (principiante o junior, senior, etc.). A mayor grado, más madurez. Como inciso, con la revisión de noviembre de 2020 y que estará lista para noviembre de 2021, ahora NICE sí que contará con una amplia gama de competencias.

2. La formación del aprendiz es siempre una pieza clave para la organización. por ello es necesario que éste se forme siguiendo una serie de "caminos en el aprendizaje". Para ello se echarán mano de cursos que son recomendados por la IQ4 según el trabajo realizado y nivel de destreza del que se disponga. en un principio, era el propio aprendiz el que se evaluaba, pero los resultados con las recomendaciones son mucho mejores.

3. Al segundo punto está muy ligado este: una vez hemos adquirido estas destrezas, debemos conseguir que el aprendiz las retenga. También tenemos que hacerle saber hasta dónde puede llegar poseyéndolas y cuáles son los fallos que se tienen y se deben corregir/mejorar. Se decidió construir un entorno basado en el framework de NICE para que los usuarios tengan muy claro estos conceptos.

IQ4 presume de ser una organización muy ambiciosa que ha conseguido que el 25 % de las personas que se han formado con ellos han conseguido trabajo en ciberseguridad, que el 45 % de los usuarios son mujeres y que han conseguido un total de 4 millones de puestos de trabajo. Además, justifican su facilidad de uso afirmando que un 98 % de sus usuarios nunca antes había realizado un curso de ciberseguridad.

La organización tiene además clientes de un amplio renombre. Su adaptación al framwork NICE ha sido crucial para tener clientes de gran importancia nacional (en USA) como internacional.

Dentro de su clientela destacan:

1. En el entorno de la Industria y Educación: Virtual Apprentice Challenge

2. En el entorno empresarial, JPM Chase (el banco más grande de EEUU).

3. En el entorno estudiantil, National Student Clearinghouse

Además, recientemente Costa Rica ha contratado a esta empresa para mejorar su fuerza laboral.

Figura 11: Logo IQ4

4.3. CyberVista: Workforce Transformation

CyberVista es una organización fundada en el año 2016 por Graham Holgings Company que potencia el desarrollo de la ciberseguridad dentro una empresa. Se centran meramente en el desarrollo del currículum y en implementar evaluaciones basadas en destrezas y entrenamiento/enseñanza para que los usuarios aprendan.

Según las palabras de la CEO Simone, la misión de CyberVista es construir y fortalecer las organizaciones proporcionando a los profesionales de la ciberseguridad los conocimientos, habilidades y destrezas necesarias para impulsar el crecimiento y la defensa.

La taxonomía de la compañía está puramente basada en el marco de NICE. Sin embargo, el cometido de está compañía es (como es lógico) particular a un área: desarrollo de currículum y evaluaciones. Gracias a la flexibilidad que proporciona el marco NICE, la organización pudo orientar sus fundamentos tomando aquellas áreas de NICE que quería utilizar y dejando las que no.

Jung Lee, el jefe de producción de la organización, explica cuáles son los beneficios que NICE le aportaba y cuáles las limitaciones:

- Las ventajas: El diseño es muy robusto. Cuenta en total con alrededor de 2000 declaraciones de tareas, conocimientos, destrezas y habilidades y más de 50 roles de trabajo (52 más concretamente). También destaca que NICE es fantástico para definir posiciones de trabajo y roles de inventario.

- Las desventajas: Es imposible de manejar, Precisamente porque cuenta con 2000 declaraciones y 52 roles. También es un gran inconveniente que el framework no proporciona una manera efectiva de medir el aprendizaje dinámico de los usuarios, no se puede medir continuamente lo que se va aprendiendo. algunas de las declaraciones de tareas, conocimientos, destrezas y habilidades no están bien definidas; son abstractas.

Conociendo esto, la compañía decidió desarrollar su taxonomía añadiéndole algunos elementos nuevos como son el Asunto (Subject), los Prerrequisitos o las Dependencias (Prerequisite/Dependency) y el Nivel del que disponemos (Level). Enfatizan como clave la creación de objetivos de aprendizaje y motivan constantemente a contrastar las cualidades del producto desarrollado por su taxonomía con los TKSA de NICE.

La organización funciona siguiendo una metodología basada en 3 pasos muy sencillos:

1. La primera es definir las metas que se persiguen, los objetivos a conseguir.

2. La segunda es realizar cursos, entrenamiento y evaluaciones para lograr cumplir los objetivos que se han definido en el primer apartado. El objetivo como no puede ser de otra forma, es cubrir las brechas que existen en las destrezas que un usuario posee y formarlo en aquellas que sean necesarias.

3. El tercero es mantener lo aprendido: hacer que el aprendizaje haya sido efectivo. Nunca dejar de aprender.

Figura 12: Logo Cybervista

Gracias a la implementación del modelo del NICE en esta organización, Cybervista ha conseguido reclutar a clientes de un gran renombre internacionaly nacional (en EEUU) como son Microsoft, el Ejército Estadounidense, Allstate, TRIMEDX, paloalto, etc.

4.4. Examinaciones NICE: Entrenamiento SANS y certificaciones GIAC

El Instituto SANS (SANS institute) es una compañía privada de Estados Unidos fundada en el año 1989 que está especializada en la seguridad de la información, entrenamiento en el ámbito de ciberseguridad y venta de certificados. Global Information Assurance Certification (GIAC) Es una compañía de certificaciones de la seguridad de la información que está especializada en certificaciones técnicas y prácticas. Ambas compañías están ligadas de tal forma que los cursos de formación de SANS permiten formarse para las certificaciones GIAC.

Desde hace más de 35 años ambas compañías han sido socias del National Security Workforce. Hoy en día existe una certificación que nos permite examinarnos sobre el contenido del framework NICE para comprobar si comprendemos un funcionamiento. Estos exámenes están orientados a las diferentes categorías del NICE, es decir, podemos elegir sobre cuál o cuáles de las 7 categorías queremos examinarnos. en la página web aparece un mapa interactivo en el cual podemos ver las diferentes certificaciones que se nos propone de acuerdo con la/s categoría/s en la/s que estamos interesados . Existen 4 niveles de exámenes:

- **Básico**: El entrenamiento se relaciona con muchas declaraciones de conocimiento, habilidades más simples y tareas que son requisitos previos para que un empleado sea efectivo en este rol de trabajo.

- **Intermedio**: El entrenamiento se relaciona con muchos conocimientos, habilidades, destrezas y tareas de nivel medio. El empleado puede ser razonablemente efectivo en este rol de trabajo después de recibir entrenamiento.

- **Avanzado**: La capacitación se dirige a conocimientos, habilidades, destrezas y tareas de nivel superior. El empleado debe ser muy efectivo en esta área funcional después de recibir entrenamiento. Sin embargo, algunos conocimientos de nivel inferior, requisito previo, pueden no estar cubiertos por estos cursos.

- **Experto**: Hace un mapa de unos pocos KSAs muy específicos o tareas en un área altamente enfocada. Este entrenamiento asume que alguien ya está bien entrenado y

es efectivo en este rol de trabajo en general. Se centra en la experiencia en un área muy específica y estrecha

Figura 13: Logo SANS-GIAG

5. Conclusiones y Trabajos Futuros

Este documento está basado en el documento oficial publicado por el NICE en el año 2017 y el documento de la revisión temporal publicado en noviembre del año 2020 en el que se profundiza en el término de las competencias (según el NICE se está produciendo una modernización que requiere su uso) y se suprimen las habilidades. Como la publicación es temporal, el contenido es escueto y por lo tanto, seguiremos considerando las habilidades como bloque de construcción. La publicación final de está revisión se espera para noviembre del año 2021. En él, se redefinirán además los apéndices donde aparecen los roles de trabajo (basados en categorías y especialidades), puesto que la tecnología es cambiante y NICE debe modernizarse y adaptarse a estos cambios.

Como experiencia personal, recalcar que este marco está estructurado y divido de forma muy clara y su compresión es bastante sencilla. Su empleo nos parece una idea fantástica y sin duda, lo recomendamos para su uso en cualquier organización. El simple hecho de pensar que se pueda intercambiar información de forma ágil es algo fundamental para optimizar el funcionamiento de los sistemas y potencial el desarrollo. Hace tiempo, en los esquemas de desarrollo tradicionales, apenas había intercambios de información y eso implicaba procesos más longevos.

No podemos tampoco despedir este proyecto sin destacar lo que hace tan fácil implementar este framework: la flexibilidad. Como hemos podido observar en los dos casos de las empresas (IQ4 y CiberVista) que basaban sus fundamentos en el NICE, ambos tenían resultados diferentes. Sus organizaciones funcionaban de forma distinta y sus objetivos no eran los mismos. Sin embargo, ambas partían de la misma base y es por la flexibilidad de este marco que se motiva el cambio y la mejoría (añadir declaraciones, quitarlas, etc) lo que hace que las empresas puedan obtener resultados óptimos hablando del mismo lenguaje.

Bibliografía

[1] Nice cybersecurity workforce framework. [Online]. Available: https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

[2] Nice cybersecurity workforce framework. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

[3] Workforce framework for cybersecurity (nice framework). [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

[4] National initiative for cybersecurity education. [Online]. Available: https://en.wikipedia.org/wiki/National_Initiative_for_Cybersecurity_Education

[5] Nice webinar: Nice cybersecurity workforce framework use cases and success stories. [Online]. Available: https://www.nist.gov/news-events/events/2020/03/nice-webinar-nice-cybersecurity-workforce-framework-use-cases-and-success

[6] Nice webinar series slides. [Online]. Available: https://www.nist.gov/system/files/documents/2020/03/19/NICE%20FW%20Use%20Cases%20Success%20Stories.pdf

[7] Iq4 transforming the learning economy. [Online]. Available: https://www.iq4.com/

[8] Cybervista. [Online]. Available: https://www.cybervista.net

[9] Sans-giag nice certs. [Online]. Available: https://www.sans.org/niceframework