DIGITAL SECURITY FOR SENIOR CITIZENS

Seguridad digital para personas de edad avanzada

2020-1-PL01-KA204-082121

Marco de competencias en materia de seguridad digital

Este proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación refleja únicamente la opinión del autor, y la Comisión no se hace responsable del uso que pueda hacerse de la información contenida en ella

Colaboradores

Cuiablue Ltd, Reino Unido

CWEP, Polonia

FyG Consultores, España

eSeniors, Francia

Innovation Hive, Grecia

Índice

Antecedentes

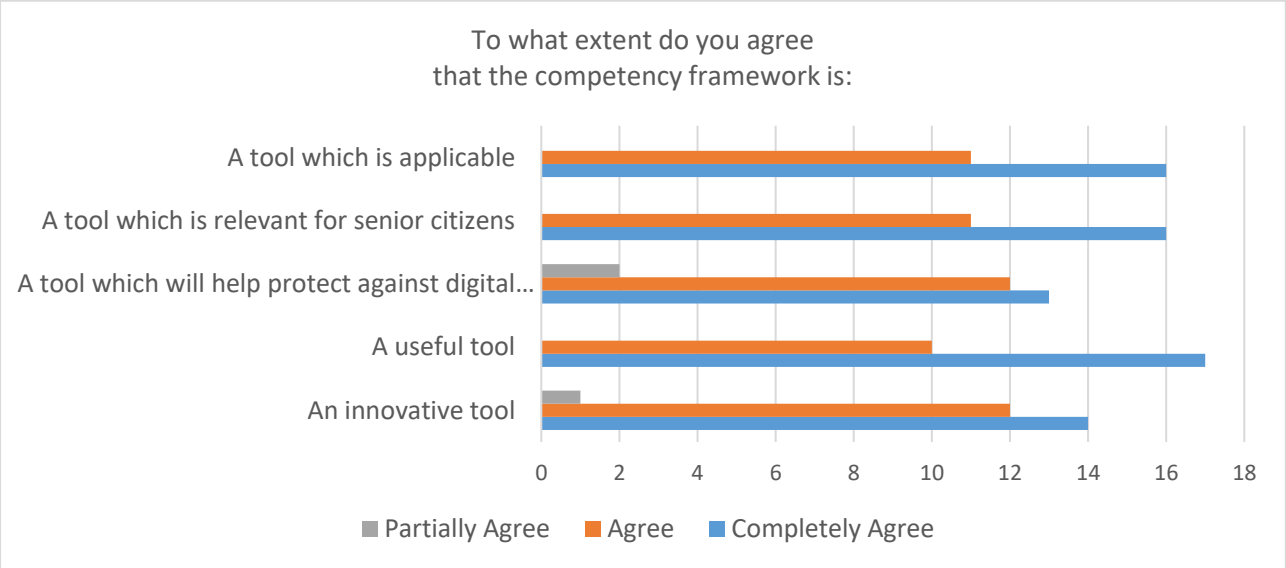
Este marco de competencias se ha desarrollado como parte del Resultado 1 del proyecto DiSC (Seguridad Digital para las Personas de Edad Avanzada). Dentro del ámbito más amplio del proyecto DiSC, este resultado tiene como objetivo respaldar el proyecto en el desarrollo de la capacidad digital de los ciudadanos de edad avanzada para reconocer y adaptarse de forma proactiva a las amenazas y estafas de seguridad digital, así como establecer las bases para la aplicación y adopción de políticas de seguridad digital específicas a nivel europeo. Este marco es un pequeño paso hacia ambos objetivos.

Metodología

El consorcio debatió y acordó el enfoque metodológico para el desarrollo del marco durante la reunión inicial del proyecto que tuvo lugar en diciembre de 2020. En primer lugar, se elaboró un conjunto de cuestionarios para las reuniones de consulta con las partes interesadas y una plantilla para la investigación documental, la cual se ajustó y modificó en consecuencia para que los socios pudieran empezar a recopilar información sobre el estado actual de la información, el asesoramiento, la orientación y la política en materia de seguridad digital a nivel nacional en cada uno de los países representados. Al mismo tiempo que el consorcio llevó a cabo una investigación documental, se desarrolló el borrador inicial del marco. Tras resumir y analizar los resultados de la investigación documental y tener en cuenta los comentarios recibidos en las reuniones de consulta con las partes interesadas, se elaboró la segunda iteración del marco para que el consorcio lo comentara y lo retroalimentara. Una vez incorporados los comentarios y las aportaciones, la versión final del marco se tradujo y se puso a prueba con grupos más amplios de interesados y usuarios finales.

Consulta con las partes interesadas

Como parte del enfoque de cocreación de los resultados del proyecto DiSC, a continuación, se presenta un resumen de las aportaciones pertinentes recogidas por todos los socios del proyecto durante las primeras reuniones de consulta con las partes interesadas a principios de 2021. A continuación, se resumen las declaraciones relativas al marco de competencias, tras lo cual se invitó a las partes interesadas a comentar su decisión o añadir cualquier idea sobre el marco.



A continuación, se pidió a las partes interesadas que complementaran las respuestas cuantitativas respondiendo a la pregunta " ¿Quieres hacer algún comentario o recomendación que nos ayude a mejorar el marco de competencias en materia de seguridad digital?". También se les proporcionó un formulario abierto para que pudieran aportar cualquier comentario, idea o impresión general sobre el concepto.

Las recomendaciones específicas incluían utilizar un vocabulario adecuado para que las personas de edad avanzada lo entendieran y centrarse en los requisitos básicos y alcanzables para garantizar la accesibilidad y la aceptación. Otra recomendación fue proporcionar a los usuarios los medios y los recursos necesarios para desarrollar cada competencia, que apoyan la necesidad de los resultados 1 y 2.

La recomendación más frecuente es que el marco tenga en cuenta tanto los desarrollos tecnológicos más recientes como los problemas de ciberseguridad asociados; por ejemplo, la criptomoneda y los cientos de enfoques creativos y en continua evolución que emplean los hackers para intentar robar dichas divisas. En este contexto, el consorcio DiSC se enfrenta a un gran reto a la hora de concebir el marco: debe ser lo suficientemente exhaustivo como para abarcar el amplio abanico de competencias y conocimientos necesarios, pero también lo suficientemente flexible como para adaptarse a futuras innovaciones.

Investigación documental

La segunda fase emprendida por el consorcio se centró en la recopilación de información, consejos, orientaciones y documentos políticos nacionales pertinentes que ayudaran a enmarcar el contexto en el que se sitúa el marco de competencias de la seguridad digital, tanto a nivel nacional en cada uno de los países asociados, como a nivel europeo. En total, el consorcio ha analizado 10 documentos relevantes, dos de cada país (Polonia, Reino Unido, Grecia, Francia y España). Estos documentos se resumen a continuación. Toda la investigación documental se encuentra en un anexo al final de este documento.

Estrategia Nacional Griega de Ciberseguridad 2020 - 2025: consiste en un plan nacional para el periodo 2020-2025 que incluye los objetivos estratégicos, las prioridades y las medidas políticas y reglamentarias para garantizar un alto nivel de seguridad de los sistemas de comunicación e información digitales a nivel nacional. La campaña de ciberseguridad de la División de Ciberdelincuencia griega sobre el software malicioso para móviles ofrece información e ideas relevantes sobre las formas de amenazas digitales y sobre cómo los hackers podrían acceder a los datos personales de los ciudadanos.

En Francia, los dos documentos examinados fueron la página web de cibervigilancia, publicada en 2021 por el Gobierno francés, y un documento conciso de la CNIL (Comisión Nacional de Informática y Libertades) titulado "10 consejos de la CNIL para mantenerse limpio en la red". Ambos documentos se han publicado con el objetivo de concienciar y capacitar a todos los ciudadanos para hacer frente a las ciberamenazas. Los documentos se diferencian desde el punto de vista del diseño, el nivel y la profundidad de la información que transmiten. No obstante, ambos documentos se ajustan de manera adeucada al proyecto DiSC en cuanto a lo que pretendemos conseguir y al modo en que el consorcio del proyecto DiSC se compromete y presenta la información a los usuarios finales.

En Polonia, la investigación se centró en una guía oficial de ciberseguridad para los ciudadanos, elaborada y publicada por el gobierno polaco con el título "Cómo protegerse de

los ciberataques''. Este documento proporciona unas pautas de lo que podría considerarse un conocimiento esencial sobre el uso de Internet y, especialmente, de los medios sociales y, por lo tanto, podría tenerse en cuenta a la hora de desarrollar el marco e incluirlo en el mismo. El segundo documento es una guía elaborada a través de otro proyecto de la UE. El documento ofrece orientación sobre los conocimientos y la conciencia esenciales que todos los ciudadanos podrían tener a nivel básico, por lo que deberían tenerse en cuenta a la hora de desarrollar el marco e incluirse en el mismo. Ambos documentos incluyen contenidos relevantes para la aplicación del DiSC y se pueden relacionar con muchos contextos individuales y familiares diferentes.

La investigación española condujo a los socios a la Estrategia Nacional de Ciberseguridad 2019 publicada por el Consejo Nacional de Seguridad del Gobierno de España, que marca las directrices dentro de las líneas generales de actuación para afrontar el reto que supone la vulnerabilidad del ciberespacio para el país. El segundo documento se titula "Vive un Internet seguro: Nunca es tarde para disfrutar de un Internet más seguro" y fue publicada por la Organización de Consumidores y Usuarios (OCU). Contiene una serie de guías prácticas para diferentes grupos sociales, como niños, padres, adultos y personas mayores. Para las personas de edad avanzada, la guía ofrece recomendaciones para aprender a disfrutar de todas las ventajas de Internet, sin perjuicio de edad.

La investigación del Reino Unido se centró en la página web de asesoramiento y orientación del Consejo Nacional de Ciberseguridad del Reino Unido. La información proporcionada se enmarca en el objetivo más general de proteger al Reino Unido y, por tanto, está dirigida a todos los ciudadanos, cosa que se refleja en el propio contenido. El segundo documento es la Estrategia Nacional de Ciberseguridad 2016-2021 del Gobierno del Reino Unido, el cual proporciona una visión general de las amenazas estratégicas para el gobierno, las empresas y el público, por lo que, aunque es relevante para el proyecto DiSC, sólo cubre de forma marginal las áreas que aborda este proyecto. La lista completa de tipos de amenazas es muy relevante tanto para el marco como el proyecto en su conjunto.

En resumen, la investigación documental ha servido para elaborar el marco mediante la presentando los problemas de ciberseguridad, las amenazas y la terminología utilizada en cada uno de los contextos nacionales. La presentación y el análisis de las distintas formas de suministro de información utilizadas para los diferentes grupos objetivo también han influido mucho en la orientación del marco de competencias, ya que cierta terminología y la presentación de la información importan mucho a las personas de edad avanzada; y esto se manifiesta de forma similar a nivel nacional. Todos los países socios ofrecen algún tipo de información a los ciudadanos de edad avanzada en el contexto nacional, ya sea de forma específica o dentro de una campaña más amplia de concienciación para los grupos sociales. No obstante, una vez completado, el marco del proyecto será independiente por lo que respecta a la aportación de un conjunto de competencias aplicables necesarias para aumentar la capacidad personal de reducir las ciberamenazas.

Introducción al marco de competencias

Un marco de competencias es un método eficaz para evaluar, mantener y supervisar los conocimientos, las habilidades y las cualidades de los grupos objetivo relacionados con la

concienciación, la reactividad y la proactividad en el ámbito de la ciberseguridad. El proyecto DiSC se diseñó a partir del Marco Europeo de Competencias Digitales Digcomp, el cual no cubre de manera explícita ni la seguridad frente a los ciberataques agresivos, ni el spam ni los trucos de estafa utilizados para robar los datos y la información de las personas en Internet. En términos más generales, estas competencias y habilidades se basan en las secciones 4.1 y 4.2 del marco DigComp 2.1:

4.1 Proteger los dispositivos: proteger los dispositivos y los contenidos digitales, y comprender los riesgos y las amenazas que existen en los entornos digitales. Conocer las medidas de seguridad y tener en cuenta la fiabilidad y la privacidad.

4.2 Proteger los datos personales y la privacidad: proteger los datos personales y la privacidad en los entornos digitales. Entender cómo utilizar y compartir la información de identificación personal, y ser capaz de protegerse a uno mismo y a los demás de los daños. Ser consciente de que los servicios digitales utilizan una "política de privacidad" para informar sobre el uso de los datos personales.

El consorcio del proyecto DiSC ha desglosado el apartado 4.1 (protección de los dispositivos), y el apartado 4.2 (protección de los datos personales y de la privacidad), en cinco subapartados, los cuales se han utilizado para clasificar las competencias de seguridad digital pertinentes:

1. Concienciación sobre las amenazas: concienciación sobre los diferentes tipos de amenazas de la seguridad digital
2. Comprensión de las amenazas: conocimiento de los riesgos asociados a las amenazas de la seguridad digital
3. Plan de mitigación: prepararse para hacer frente a las amenazas y reducirlas
4. Detectar las amenazas: aplicación del pensamiento crítico y analítico a las posibles amenazas de la seguridad digital
5. Contrarrestar las amenazas: resolución de problemas para contrarrestar las amenazas y las infracciones

El establecimiento del marco de competencias sobre la seguridad digital permitirá al proyecto DiSC definir los conocimientos y habilidades de ciberseguridad necesarios para hacer frente a las posibles amenazas, identificar las competencias específicas relativas a la ciberseguridad (a través de una serie de temas), y apoyar el desarrollo y la propuesta de cursos y oportunidades de formación personal y profesional específicos para los grupos objetivo del proyecto.

Los usuarios finales previstos del marco de competencias son las personas mayores de 55 años. También se espera que el marco sea relevante y de interés para los profesores y educadores de TIC (tanto los que se están formando como los que están ejerciendo), y para los profesionales que trabajan en el ámbito del desarrollo de la capacidad tecnológica de las personas de edad avanzada.

El Marco de Competencias de Seguridad Digital tiene como objetivo definir las habilidades, conocimientos y actitudes de las competencias clave que necesitan los ciudadanos de edad avanzada para integrar eficazmente los protocolos de seguridad digital en sus contextos

localizados, así como proporcionar un marco de referencia de la UE para desarrollar y evaluar las competencias de seguridad digital.

Objetivo

Con el fin de definir el ámbito de aplicación del proyecto, los socios han identificado los dispositivos electrónicos, el enfoque y los métodos que se han tenido en cuenta a la hora de aplicar el Marco de Competencia Digital. Esto ayudará a definir otros tipos de actividades delictivas que no están cubiertas por las competencias del marco.

Dispositivos electrónicos: los dispositivos utilizados para contactar con la víctima

- Teléfonos móviles y Smartphones
- Ordenadores y portátiles
- Tabletas

Enfoque: la técnica utilizada para estafar a la víctima

- Fraude electrónico: se trata de un intento fraudulento de obtener información o datos confidenciales, como por ejemplo nombres de usuario, contraseñas y datos de tarjetas de crédito, haciéndose pasar por una entidad de confianza en una comunicación electrónica.
- Llamadas fraudulentas: se trata de un tipo de fraude telefónico delictivo que utiliza la ingeniería social a través del sistema telefónico para acceder a información personal y financiera privada con el fin de obtener una recompensa económica.
- Mensajes fraudulentos: se trata de una actividad que permite a los delincuentes robar el dinero o la identidad de las víctimas, o ambos, a raíz de una respuesta a un mensaje de texto. Los mensajes fraudulentos utilizan los teléfonos móviles (ya sea un smartphone o un teléfono tradicional no conectado a Internet) para manipular a personas inocentes con el fin de que realicen diversas acciones que les lleven a ser estafados.
- Fraudes realizados mediante servicios de software: se trata de una actividad en la que el estafador utiliza un software falso o de imitación (como una aplicación o un programa) para acceder a los datos de un dispositivo digital. Seguidamente, el estafador utiliza el dispositivo para robar el dinero o la identidad de las víctimas.
- Ingeniería social: se trata de un término utilizado para referirse a una amplia gama de actividades maliciosas realizadas a través de las interacciones humanas. Consiste en utilizar la manipulación psicológica para engañar a los usuarios a fin de que cometan errores de seguridad o faciliten información confidencial.
- Método: estafas intencionadas
- Estafas realizadas mediante un correo electrónico
- Estafa del ‘príncipe’ rico
- Estafas con las tarjetas de felicitación
- Préstamos bancarios o estafas con tarjeta de crédito

- Estafas con la lotería
- Estafas de extorsión
- Estafas realizadas en páginas de citas
- Antivirus falsos
- Suplantación de identidad en Facebook/estafa de perfiles pirateados
- Estafas de '¡Gana dinero rápido!'
- Estafas con viajes
- Estafas con criptomonedas
    - Intercambios falsos de Bitcoin
    - Esquemas Ponzi
    - Intentos de estafa diarios
    - Software maliciosos
- Estafas con noticias falsas
- Tiendas online fraudulentas
- Estafas en las ofertas de empleo
- Mensajes fraudulentos
- Estafas de sobrepago online
- Estafas de soporte técnico online

Nota: las amenazas digitales están en constante cambio y evolución y, por su naturaleza, es imposible elaborar una lista exhaustiva. Para estar al día de las amenazas, DiSC recomienda suscribirse a una organización o red de ciberseguridad, como Heimdal Security, por ejemplo, la cual publica actualizaciones frecuentes sobre temas, enfoques y métodos de ciberseguridad, o la página de Europol sobre actividades delictivas.

El marco de competencias

Competencias fundamentales	Niveles de competencia		
Descripción	Básico El individuo entiende el concepto básico, las habilidades y los requisitos de conocimiento de la seguridad digital, y está preparado para	Intermedio El individuo muestra un pensamiento crítico relacionado con la seguridad digital, puede diferenciar las amenazas digitales en todos los dispositivos y	Avanzado El individuo muestra un pensamiento analítico hacia la seguridad digital y puede responder a las amenazas en tiempo real evaluando y

	alcanzar el nivel más alto posible de competencia.	es capaz de planificar de forma independiente y llevar a cabo con éxito acciones de mitigación para protegerse de ellas.	eligiendo la respuesta más eficaz en una situación de alta presión.

1. Concienciación sobre las amenazas

Concienciación sobre las amenazas	Básico	Intermedio	Avanzado
Concienciación sobre las amenazas específicas dirigidas a los dispositivos digitales.	Soy consciente de los enfoques comunes utilizados por las amenazas de seguridad digital.	Soy consciente de los enfoques menos comunes utilizados por las amenazas de seguridad digital.	Me mantengo al día con los nuevos enfoques de seguridad digital.
	Soy consciente de los métodos habituales utilizados por las amenazas de seguridad digital.	Soy consciente de los enfoques menos comunes utilizados por las amenazas de seguridad digital.	Me mantengo al día con los nuevos enfoques de seguridad digital.
	Soy consciente de las actividades básicas de ingeniería social en el contexto de la seguridad digital.	Conozco las técnicas de ingeniería social más complejas.	Conozco diferentes combinaciones de técnicas, enfoques y métodos de ingeniería social.

2. Comprensión de las amenazas

Comprensión de las amenazas	Básico	Intermedio	Avanzado
Conocimiento de las características y funciones de cada una de las amenazas. Evaluar las amenazas digitales y su nivel de riesgo.	Conozco las principales características y funciones de las amenazas de seguridad digital más comunes.	Conozco las principales características y funciones de las amenazas de seguridad digital más inusuales.	Actualizo activamente mis conocimientos sobre las amenazas digitales a través de fuentes de información de seguridad fiables, actualizadas y precisas.
	Comprendo el nivel de riesgo y las posibles consecuencias asociadas a las simples	Soy consciente del nivel de riesgo y de las posibles consecuencias asociadas a las	Soy consciente del nivel de riesgo y de las posibles consecuencias asociadas a las

Comprender la naturaleza cambiante de las amenazas digitales. Ser consciente de la importancia de contar con fuentes de información de seguridad fiables, actualizadas y precisas.	amenazas de seguridad digital.	múltiples amenazas de seguridad digital.	complejas amenazas de seguridad digital.

3. Mitigación

Mitigación	Básico	Intermedio	Avanzado
Conocimientos y experiencia que permiten tomar decisiones informadas sobre la protección contra las amenazas digitales. Conocimiento y comprensión de las diferentes herramientas y recursos de protección contra las amenazas.	Soy capaz de identificar las herramientas de protección digital adecuadas para mitigar las amenazas a la seguridad digital.	Soy capaz de utilizar mis experiencias y habilidades pasadas para fundamentar mis decisiones sobre la protección de las amenazas a la seguridad digital.	Soy capaz de utilizar mi experiencia y mis conocimientos para analizar las posibles repercusiones de los distintos riesgos y elegir las estrategias de protección adecuadas.
	Soy capaz de seguir instrucciones básicas de seguridad digital para mitigar las amenazas a la seguridad digital.	Soy capaz de decidir cuáles son las herramientas básicas de seguridad digital más adecuadas para mitigar las amenazas a la seguridad digital.	Soy capaz de analizar y evaluar las amenazas a la seguridad digital y adaptar mi estrategia de protección en función de la amenaza a la seguridad digital.
	Sé cómo configurar un dispositivo digital para garantizar la protección contra las amenazas básicas de seguridad digital.	Sé cómo comprobar y actualizar un dispositivo digital para garantizar una protección adecuada contra las amenazas de seguridad.	Sé cómo instalar herramientas y software de protección en los dispositivos digitales para mitigar las amenazas digitales.

4. Detección de las amenazas

Deteción de las amenazas	Básico	Intermedio	Avanzado
Capacidad para reconocer las amenazas digitales y los riesgos específicos que se plantean Capacidad para clasificar las amenazas digitales por nivel de riesgo	Soy capaz de reconocer e identificar las amenazas de seguridad digital más comunes para mis datos e información personales.	Soy capaz de reconocer e identificar las amenazas de seguridad digital más raras e inusuales para mis datos e información personales.	Me mantengo activamente al tanto de las amenazas a la seguridad digital a través de fuentes de información de seguridad fiables, actualizadas y precisas.
	Puedo reconocer riesgos y amenazas claros y evidentes en entornos digitales.	Soy capaz de reconocer amenazas oscuras de seguridad digital.	Puedo reconocer riesgos y amenazas complejas en entornos digitales.
	Soy capaz de utilizar mis conocimientos para evaluar posibles amenazas de seguridad y decidir si son sospechosas.	Soy capaz de utilizar mi enfoque analítico de la seguridad digital para detectar las amenazas digitales.	Soy capaz de utilizar mis habilidades de pensamiento crítico para analizar, comparar y evaluar el alcance de una amenaza digital y el nivel de riesgo asociado.

5. Contrarrestar las amenazas

Contrarrestar las amenazas	Básico	Intermedio	Avanzado
Tomar decisiones positivas y eficaces manteniendo la calma en situaciones de presión. Fuerza mental para afrontar la	Soy flexible y estoy bien preparado para afrontar las amenazas de seguridad digital.	Utilizo la adaptabilidad para contrarrestar las amenazas a la seguridad digital.	Anticipo activamente las amenazas de seguridad digital y sus riesgos y practico la adaptación para contrarrestarlas.
	Me mantengo positivo cuando me enfrento a amenazas o violaciones de la seguridad digital.	Soy capaz de utilizar mis propias experiencias para abordar con optimismo y confianza las posibles amenazas e infracciones.	Soy capaz de explicar cómo han contribuido a mi seguridad digital la actitud, los comportamientos y las acciones positivas.

incertidumbre, el estrés y las situaciones difíciles.	Soy capaz de reflexionar sobre las amenazas digitales del pasado para aprender de ellas.	Soy capaz de reflexionar sobre experiencias pasadas y cambiar mi comportamiento y actitud ante las amenazas digitales para enfrentarme mejor a ellas.	Soy capaz de reflexionar sobre las experiencias pasadas de amenazas digitales y cambiar mi comportamiento y actitud en la vida para convertirme en una persona más fuerte.