BA/T Valida tus competencias digitales

CERTIFICACIÓN AREA COMPETENCIAL: SEGURIDAD

La certificación de esta área competencial aborda las siguientes competencias digitales basadas en el marco de referencia DigComp:

- **Protección de dispositivos:** Proteger los dispositivos y los contenidos digitales, y comprender los riesgos y las amenazas en los entornos digitales. Conocer las medidas de seguridad y tener en cuenta la fiabilidad y la privacidad.
- **Protección de datos personales y privacidad:** Proteger los datos personales y la privacidad en los entornos digitales. Entender cómo utilizar y compartir la información personal identificable, siendo capaz de protegerse a sí mismo y a los demás de los daños. Entender que los servicios digitales utilizan una "política de privacidad" para informar sobre el uso de los datos personales.
- **Protección de la salud y del bienestar:** Capacidades a la hora de evitar riesgos para la salud tanto física como mental en el uso de las tecnologías digitales. Capacidad a la hora de protegerse uno mismo y a otros ante los riesgos de los entornos digitales (por ejemplo: cyber-bullying).
- **Protección medioambiental:** Ser consciente del impacto de las tecnologías digitales y su uso.

Objetivos de aprendizaje evaluados

A continuación, en la siguiente tabla se muestran los objetivos de aprendizaje evaluados para cada una de las competencias digitales y los 3 niveles de competencia considerados (básico, medio y avanzado).

básico	medio	avanzado
Protección de dispositivos		
Conocer maneras sencillas de proteger los dispositivos y el contenido digital, por ejemplo, configurando políticas de seguridad y privacidad. Dimensiones clave a considerar: 1. **Conocimiento de conceptos básicos de seguridad digital:** evaluar si el usuario comprende conceptos fundamentales relacionados con la protección de dispositivos y contenido digital, como contraseñas seguras, políticas de seguridad, privacidad en línea, malware, phishing, entre otros. 2. **Aplicación de medidas de seguridad básicas**: evaluar la capacidad del usuario para aplicar medidas de seguridad simples pero	Proteger sus dispositivos y contenido digital, aplicando medidas de seguridad más avanzadas. Dimensiones clave a considerar: 1. **Comprensión de medidas avanzadas de seguridad digital**: Esta dimensión evaluaría la comprensión del usuario sobre las medidas de seguridad más avanzadas disponibles para proteger dispositivos y contenido digital. Incluiría conocimientos sobre cifrado, autenticación multifactor, VPN, firewalls avanzados, entre otros. 2. **Aplicación de técnicas de protección avanzadas**: Aquí se evaluaría la capacidad del usuario para aplicar de manera efectiva las	Conocer y aplicar medidas de seguridad para proteger los dispositivos y controlar incidentes maliciosos que pueden afectar al funcionamiento de los equipos. Dimensiones clave a considerar: 1. **Conocimiento avanzado de medidas de seguridad:** Comprender en profundidad los conceptos de seguridad informática, incluyendo tipos de malware, técnicas de prevención, cifrado de datos, autenticación y control de acceso. 2. **Aplicación efectiva de medidas de seguridad:** Ser capaz de implementar y configurar adecuadamente herramientas y medidas de seguridad en

efectivas en la protección de dispositivos y contenido digital. Esto incluiría acciones como actualizar software, configurar privacidad en redes sociales, utilizar software antivirus, realizar copias de seguridad, entre otros. 3. **Reconocimiento de riesgos y buenas prácticas:** evaluar la capacidad del usuario para identificar posibles riesgos en línea y reconocer buenas prácticas de seguridad digital. Esto implicaría comprender los peligros del phishing, la importancia de descargar archivos de fuentes confiables, la necesidad de mantener actualizados los dispositivos y software, entre otros aspectos.	técnicas y herramientas de seguridad más avanzadas en situaciones reales. Esto podría incluir la configuración de firewalls, la implementación de políticas de seguridad, la utilización de herramientas de cifrado, entre otros. 3. **Análisis de amenazas y vulnerabilidades**: Esta dimensión evaluaría la habilidad del usuario para identificar y analizar amenazas y vulnerabilidades específicas en entornos digitales, así como para proponer soluciones o contramedidas adecuadas. Incluiría la capacidad de evaluar riesgos, detectar ataques potenciales y tomar medidas preventivas o correctivas.	diferentes dispositivos y entornos, demostrando habilidades prácticas para proteger eficazmente contra amenazas maliciosas. 3. **Gestión de incidentes y respuesta ante ataques:** Estar preparado para identificar y responder de manera adecuada ante incidentes de seguridad, incluyendo procedimientos de detección, análisis de vulnerabilidades, mitigación de riesgos y recuperación de sistemas afectados.
Diferenciar riesgos y amenazas simples en entornos digitales, así como riesgos asociados con el uso de tecnologías. Dimensiones clave a considerar: 1. **Identificación de riesgos digitales simples**: evaluar la capacidad del usuario para reconocer y diferenciar entre diferentes tipos de riesgos y amenazas simples en entornos digitales. Esto incluiría comprender conceptos básicos como phishing, malware, contraseñas débiles, entre otros. 2. **Comprensión de riesgos asociados con el uso de tecnologías**: evaluar la capacidad del usuario para comprender los riesgos específicos asociados con el uso de tecnologías digitales, como la seguridad de la información, la privacidad en línea y la protección de datos personales. 3. **Aplicación de medidas de protección básicas**: evaluar la capacidad del usuario para aplicar medidas básicas de protección contra los riesgos identificados, como utilizar contraseñas seguras, mantener el software actualizado, evitar la descarga de archivos de sitios web no seguros, entre otras acciones preventivas.	Diferenciar riesgos y amenazas en entornos digitales. Dimensiones clave a considerar: 1. **Conocimiento de amenazas digitales:** Evaluar la comprensión de los diferentes tipos de riesgos y amenazas en entornos digitales, como malware, phishing, suplantación de identidad, entre otros. Esto incluiría conocer cómo se originan estas amenazas, cómo se propagan y cuáles son sus efectos potenciales en los dispositivos y la seguridad digital en general. 2. **Identificación de medidas de protección:** Evaluar la capacidad de reconocer y entender las medidas de protección y seguridad digital disponibles para mitigar los riesgos y amenazas identificados. Esto implica conocer y comprender conceptos como el uso de software antivirus, la configuración de contraseñas seguras, la autenticación de dos factores, el uso de conexiones VPN, entre otros. 3. **Aplicación de prácticas seguras:** Evaluar la habilidad para aplicar prácticas seguras en entornos digitales para proteger dispositivos y datos personales. Esto incluiría la capacidad de tomar decisiones informadas sobre el uso de contraseñas seguras, la descarga de software desde fuentes confiables, la navegación segura en línea, la gestión adecuada de la privacidad en redes sociales y la protección de la información confidencial al trabajar en entornos digitales compartidos.	Discriminar los riesgos y las amenazas en los entornos digitales. Dimensiones clave a considerar: 1. **Conocimiento avanzado de riesgos y amenazas digitales:** Comprender en profundidad los diferentes tipos de riesgos y amenazas en entornos digitales, incluyendo malware, phishing, ingeniería social, ataques de denegación de servicio (DDoS), entre otros. 2. **Análisis crítico y evaluación de riesgos:** Ser capaz de analizar críticamente situaciones y escenarios digitales para identificar y evaluar los riesgos y amenazas potenciales, considerando su impacto y probabilidad de ocurrencia. 3. **Estrategias de mitigación y prevención:** Desarrollar habilidades para diseñar e implementar estrategias efectivas de mitigación y prevención de riesgos y amenazas en entornos digitales, incluyendo medidas de seguridad técnicas y prácticas de comportamiento seguro en línea.
	Aplicar y ser capaz de explicar distintas políticas de seguridad y privacidad. Dimensiones clave a considerar: 1. Conocimiento de Políticas de Seguridad y Privacidad: ¿El usuario puede identificar y explicar	Evaluar las formas más adecuadas para tener en cuenta la fiabilidad y la privacidad. Dimensiones clave a considerar: 1. **Análisis crítico de la fiabilidad de la información en línea:** Capacidad

	diferentes políticas de seguridad y privacidad utilizadas en entornos digitales? ¿Puede describir cómo estas políticas ayudan a proteger la información y los dispositivos? 2. **Aplicación Práctica de Políticas de Seguridad y Privacidad:** ¿El usuario puede aplicar eficazmente las políticas de seguridad y privacidad en situaciones prácticas? ¿Puede demostrar cómo implementar estas políticas en la configuración y uso diario de dispositivos digitales? 3. **Comprensión de Implicaciones y Buenas Prácticas:** ¿El usuario comprende las implicaciones de no seguir las políticas de seguridad y privacidad? ¿Puede identificar y explicar buenas prácticas para mantener la seguridad y privacidad en entornos digitales?	para evaluar la credibilidad de las fuentes de información en línea y discernir entre información confiable y desinformación. 2. **Gestión efectiva de la privacidad en entornos digitales:** Habilidad para comprender y aplicar prácticas de privacidad adecuadas al utilizar servicios en línea, proteger la información personal y gestionar la configuración de privacidad en diversas plataformas. 3. **Toma de decisiones informadas sobre seguridad y privacidad:** Habilidad para tomar decisiones fundamentadas sobre cómo proteger la privacidad y la seguridad en entornos digitales, considerando los riesgos y las mejores prácticas disponibles.
Protección de datos personales y privacidad		
Seleccionar formas sencillas de proteger mis datos personales y mi privacidad en entornos digitales. Dimensiones clave a considerar: 1. **Conocimiento básico de riesgos y amenazas:** Identificar las principales amenazas para la privacidad en línea, como el phishing, la divulgación de información personal en redes sociales, contraseñas débiles, etc. Reconocer los riesgos asociados con el uso de redes Wi-Fi públicas y la transmisión de datos no cifrados. 2. **Habilidades para adoptar prácticas de seguridad básicas:** Seleccionar y aplicar medidas básicas de protección de datos, como el uso de contraseñas seguras, la configuración de la privacidad en redes sociales, y la instalación de actualizaciones de software. Conocer y utilizar herramientas básicas de seguridad, como conexiones VPN para redes Wi-Fi públicas. 3. **Conciencia sobre la importancia de la seguridad digital:** Comprender la importancia de proteger la información personal y la privacidad en línea. Reconocer las posibles consecuencias de no proteger adecuadamente los datos personales en entornos digitales, como el robo de identidad, el fraude financiero, etc.	Respetar la privacidad e intimidad, las opiniones, la propiedad intelectual e industrial de los demás y proteger nuestros datos personales sensibles y la información relevante de los demás. (Valorar lo qué ocurre con sus datos personales en Internet.) Dimensiones clave a considerar: 1. **Conciencia y comprensión de la importancia de la privacidad y protección de datos:** ¿El usuario comprende la importancia de proteger la privacidad y los datos personales en línea? ¿Es consciente de los riesgos asociados con la divulgación de información personal en Internet? ¿Entiende la necesidad de proteger la propiedad intelectual e industrial de los demás? 2. **Conocimiento y aplicación de buenas prácticas de seguridad digital:** ¿El usuario conoce y puede aplicar medidas de seguridad básicas en línea, como contraseñas seguras y actualización de software? ¿Es capaz de identificar y evitar prácticas riesgosas, como el phishing y el compartir información confidencial en redes sociales? ¿Puede utilizar herramientas y configuraciones de privacidad en línea para proteger su información personal y la de los demás? 3. **Actitudes y valores hacia la privacidad y la protección de datos:** ¿El usuario demuestra actitudes responsables hacia la privacidad y la protección de datos en línea? ¿Muestra respeto por la privacidad y la propiedad intelectual de los demás? ¿Está comprometido con la protección de su propia información personal	Proteger los datos personales y la privacidad en los entornos digitales, tanto los propios como los de otras personas. Evaluar y gestionar el rastro y datos que se dejan en la red cuando se comparte información, se visitan páginas web o se utilizan aplicaciones web. Dimensiones clave a considerar: 1. **Conocimiento Profundo de las Amenazas y Vulnerabilidades en Línea:** evaluar la comprensión del usuario sobre las diversas amenazas y vulnerabilidades que existen en línea, como el phishing, el malware, la ingeniería social, entre otros. También incluiría el conocimiento detallado sobre cómo estas amenazas pueden comprometer la privacidad y los datos personales. 2. **Gestión Avanzada de la Privacidad y la Seguridad en Línea:** se centra en la capacidad del usuario para aplicar medidas avanzadas de protección de datos y privacidad en entornos digitales. Incluiría la habilidad para configurar de manera efectiva la configuración de privacidad en diversos servicios en línea, así como la implementación de herramientas de seguridad avanzadas, como redes privadas virtuales (VPN) y sistemas de cifrado. 3. **Análisis Crítico y Toma de Decisiones en Escenarios Complejos:** evaluar la capacidad del usuario para analizar críticamente situaciones complejas relacionadas con la privacidad y la seguridad en línea, así como para tomar decisiones informadas y estratégicas para proteger los datos personales. Incluiría la

	y la de los demás en entornos digitales?	capacidad para evaluar el impacto de diferentes acciones en la privacidad y la seguridad en línea y tomar medidas adecuadas en consecuencia.
Identificar formas sencillas de utilizar y compartir la información personal identificable, protegiéndome a mí y a los demás de los daños. Dimensiones clave a considerar: 1. **Conocimiento básico de prácticas seguras de manejo de información:** Identificar qué tipo de información personal identificable se debe proteger. Reconocer formas seguras de utilizar y compartir la información personal en línea. 2. **Habilidades básicas de protección de la privacidad:** Aplicar medidas básicas de protección de datos personales en entornos digitales. Comprender la importancia de proteger tanto la propia privacidad como la de los demás al manejar información personal. 3. **Conciencia sobre las amenazas y riesgos asociados:** Reconocer posibles amenazas y riesgos para la seguridad de la información personal en línea. Comprender las consecuencias potenciales de la exposición indebida de información personal identificable en entornos digitales.	Conocer pautas y buenas prácticas de ciberseguridad y privacidad. (Conocer los mecanismos de defensa existentes y sus derechos.) Dimensiones clave a considerar: 1. **Conciencia de Riesgos y Amenazas en Línea:** evaluar la comprensión del usuario sobre los riesgos y amenazas a la seguridad y privacidad en línea, así como su capacidad para identificar posibles peligros y comportamientos inseguros. 2. **Conocimiento de Buenas Prácticas de Ciberseguridad:** evaluar el conocimiento del usuario sobre las prácticas recomendadas de ciberseguridad y privacidad, incluyendo el uso de contraseñas seguras, la importancia de las actualizaciones de software, el reconocimiento de correos electrónicos fraudulentos, entre otros. 3. **Comprensión de Derechos y Mecanismos de Defensa:** se centra en la comprensión de los derechos individuales en línea, como el derecho a la privacidad y la protección de datos personales, así como en la comprensión de los mecanismos de defensa disponibles, como la autenticación de dos factores y el cifrado de datos.	Utilizar herramientas de cifrado de mensajes de correo electrónico para para evitar el acceso no autorizado y mejorar la privacidad. Dimensiones clave a considerar: 1. **Conocimiento Profundo de las Herramientas de Cifrado de Mensajes:** evaluar el conocimiento detallado sobre las herramientas de cifrado de mensajes de correo electrónico, incluyendo cómo funcionan, qué tecnologías utilizan y cómo se implementan en entornos digitales. 2. **Habilidades Avanzadas de Configuración y Gestión de Privacidad:** se enfoca en evaluar la capacidad del usuario para configurar y gestionar adecuadamente las herramientas de cifrado de mensajes de correo electrónico para mejorar la privacidad y evitar el acceso no autorizado. 3. **Análisis Crítico y Toma de Decisiones en Escenarios Complejos de Seguridad Digital:** evaluar la capacidad del usuario para analizar situaciones complejas relacionadas con la seguridad digital y tomar decisiones informadas sobre el uso de herramientas de cifrado de mensajes de correo electrónico para proteger la privacidad y los datos personales.
Identificar declaraciones encillas de política de privacidad sobre el uso de los datos personales en los servicios digitales. Dimensiones clave a considerar: 1. **Conocimiento básico de políticas de privacidad:** Comprender la función y el propósito de una política de privacidad en un servicio digital. Identificar las partes clave de una política de privacidad, como la información sobre la recopilación y el uso de datos personales. 2. **Habilidades básicas de comprensión de políticas de privacidad:** Interpretar declaraciones sencillas de política de privacidad para entender cómo se manejan los datos personales. Reconocer las responsabilidades del usuario al leer y entender una política de privacidad. 3. **Conciencia sobre la importancia de leer y comprender las políticas de privacidad:** Reconocer la importancia de leer y comprender las políticas de privacidad para	Indicar las declaraciones de política de privacidad sobre el uso de los datos personales en los servicios digitales. Dimensiones clave a considerar: 1. **Comprensión de las Políticas de Privacidad:** evaluar la capacidad del usuario para comprender el propósito y el contenido de las políticas de privacidad de los servicios digitales, incluyendo la capacidad de identificar y explicar los elementos clave de estas políticas. 2. **Conciencia de los Derechos del Usuario:** evaluar la comprensión del usuario sobre los derechos que tienen los usuarios en relación con sus datos personales, incluyendo el derecho a la privacidad, el consentimiento informado y el acceso a la información sobre cómo se utilizan sus datos. 3. **Capacidad de Interpretación y Aplicación:** se centra en la capacidad del usuario para interpretar y aplicar las políticas de privacidad en situaciones prácticas, incluyendo la capacidad	Comprender y aplicar las regulaciones de privacidad de datos más recientes. Dimensiones clave a considerar: 1. **Comprensión Profunda de las Regulaciones de Privacidad:** evaluar la capacidad del usuario para comprender en detalle las regulaciones de privacidad de datos más recientes, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, incluyendo sus principios, requisitos y repercusiones. 2. Aplicación Práctica de las Regulaciones: se centra en la habilidad del usuario para aplicar las regulaciones de privacidad de datos en situaciones prácticas, como la redacción de políticas de privacidad, la gestión de consentimientos de los usuarios y la implementación de medidas de seguridad adecuadas para garantizar el cumplimiento de las regulaciones. 3. **Análisis Crítico de Escenarios Legales y Éticos:** evaluar la capacidad del usuario para analizar

proteger la privacidad en línea. Comprender las implicaciones de no entender una política de privacidad en cuanto a la seguridad de los datos personales.	de reconocer y resolver problemas relacionados con la privacidad de los datos en entornos digitales.	críticamente situaciones legales y éticas relacionadas con la privacidad de datos, como casos de incumplimiento de las regulaciones, disputas sobre el consentimiento del usuario y conflictos entre la privacidad y otros derechos.
		Seguridad de la información sensible: Implementar medidas de seguridad para proteger la confidencialidad de la información sensible, como contraseñas y datos financieros. Desarrollar habilidades para identificar y responder a incidentes de seguridad que puedan comprometer la integridad de la información personal. Dimensiones clave a considerar: 1. **Implementación de medidas de seguridad:** evaluar la capacidad del usuario para aplicar medidas concretas destinadas a proteger la confidencialidad de la información sensible, como contraseñas y datos financieros. Incluiría el conocimiento y la aplicación de técnicas de cifrado, autenticación de dos factores, gestión de contraseñas seguras, entre otras medidas. 2. **Identificación y respuesta a incidentes de seguridad:** se centra en la capacidad del usuario para identificar y responder eficazmente a incidentes de seguridad que puedan comprometer la integridad de la información personal. Incluiría la capacidad de reconocer signos de posibles ataques o brechas de seguridad, así como la habilidad para tomar medidas correctivas rápidas y efectivas en caso de incidentes. 3. **Desarrollo de habilidades de concienciación y prevención:** evaluar la capacidad del usuario para desarrollar habilidades de concienciación y prevención en materia de seguridad de la información. Incluiría la capacidad de educar a otros usuarios sobre buenas prácticas de seguridad, identificar posibles vulnerabilidades en sistemas o procesos y tomar medidas proactivas para prevenir incidentes de seguridad.
Protección de la salud y del bienestar		
Conocer los riesgos que puede correr mi salud física y psicológica al utilizar de forma incorrecta la tecnología. Dimensiones clave a considerar: **1. Conocimiento de los riesgos para la salud física relacionados con el uso de la tecnología.**	Explicar y seleccionar formas concretas y rutinarias sobre cómo evitar riesgos y amenazas para la salud física y mental en el uso de las tecnologías digitales. Dimensiones clave a considerar: 1. **Conocimiento de los riesgos:** Evaluar la comprensión de los diferentes riesgos para la salud	Discriminar las formas más apropiadas de evitar los riesgos para la salud y las amenazas para el bienestar físico y psicológico durante el uso de las tecnologías digitales. Dimensiones clave a considerar: 1. **Conocimiento Profundo de las Amenazas y Riesgos Digitales:**

2. Conciencia de los riesgos para la salud mental asociados con el uso inapropiado de la tecnología. 3. **Comprensión de la importancia de establecer límites y prácticas saludables al utilizar la tecnología.**	física y mental asociados con el uso de tecnologías digitales, como el sedentarismo, la fatiga visual, el estrés digital, entre otros. 2. **Identificación de prácticas saludables:** Evaluar la capacidad para reconocer y seleccionar prácticas saludables que ayuden a mitigar los riesgos identificados, como establecer límites de tiempo en el uso de dispositivos, mantener una postura adecuada, realizar descansos periódicos, entre otros. 3. **Aplicación de estrategias de prevención:** Evaluar la habilidad para aplicar activamente las estrategias y prácticas saludables identificadas en situaciones concretas de uso de tecnología digital, tomando decisiones informadas para proteger la salud física y mental.	Comprender en detalle los diversos riesgos para la salud física y mental asociados con el uso de tecnologías digitales. Reconocer las amenazas específicas para la salud y el bienestar físico y mental que pueden surgir del uso inadecuado de la tecnología. Identificar las últimas tendencias y problemas emergentes en el ámbito de la salud digital y el bienestar. 2. **Habilidades de Evaluación y Análisis:** Analizar críticamente diferentes estrategias y enfoques para mitigar los riesgos para la salud asociados con la tecnología digital. Evaluar la efectividad de diversas medidas preventivas y de protección para abordar los riesgos para la salud y el bienestar digital. Identificar y discriminar entre soluciones apropiadas y no apropiadas para proteger la salud física y mental durante el uso de la tecnología. 3. **Capacidad de Aplicación Práctica:** Aplicar de manera efectiva las estrategias y medidas de protección para minimizar los riesgos y amenazas para la salud física y mental relacionados con la tecnología digital. Demostrar habilidades avanzadas para adaptar y personalizar las medidas de seguridad y protección de acuerdo con las necesidades individuales y las circunstancias específicas. Integrar el conocimiento teórico y práctico para tomar decisiones informadas y responsables sobre el uso de la tecnología digital en beneficio de la salud y el bienestar.
Conocer la existencia de patrones de actuación para salvaguardar la salud de un uso inadecuado de la tecnología. Dimensiones clave a considerar: 1. **Identificación de riesgos para la salud:** Comprender los posibles riesgos para la salud asociados con el uso inadecuado de la tecnología, como fatiga visual, dolor de espalda o problemas de sueño. 2. **Conocimiento de prácticas saludables:** Reconocer y comprender las prácticas saludables al utilizar la tecnología, como tomar descansos regulares, ajustar la configuración del dispositivo o mantener una postura ergonómica. 3. **Capacidad para implementar medidas preventivas:** Ser capaz de aplicar medidas preventivas básicas para proteger la salud al utilizar la tecnología, como establecer límites de tiempo, realizar pausas y estiramientos, o	Analizar e identificar tecnologías digitales concretas y rutinarias para la inclusión y el bienestar social. Dimensiones clave a considerar: 1. **Conocimiento de tecnologías digitales inclusivas:** Evaluar la capacidad de identificar y comprender tecnologías digitales diseñadas para promover la inclusión y el bienestar social, así como su funcionamiento y aplicaciones prácticas. 2. **Habilidad para evaluar el impacto social y de salud:** Evaluar la capacidad de analizar cómo las tecnologías digitales pueden afectar positivamente la inclusión y el bienestar social, así como comprender los posibles riesgos y desafíos asociados. 3. **Capacidad de selección y recomendación:** Evaluar la capacidad de seleccionar y recomendar tecnologías digitales específicas que sean adecuadas para promover la inclusión y el	Variar el uso de las tecnologías digitales para el bienestar social y la inclusión social. Dimensiones clave a considerar: 1. **Conocimiento Avanzado de Tecnologías Digitales para el Bienestar Social:** evaluar el conocimiento profundo de una amplia gama de tecnologías digitales y su aplicación específica en la promoción del bienestar social y la inclusión. 2. **Habilidades Avanzadas de Evaluación y Análisis:** se centra en la capacidad del usuario para evaluar críticamente las tecnologías digitales disponibles y determinar cuáles son las más apropiadas y efectivas para promover el bienestar social y la inclusión social. 3. **Capacidad para Innovar y Adaptarse:** evaluar la capacidad del usuario para ser innovador en el uso de tecnologías digitales existentes o para adaptar y crear

utilizar herramientas de protección de la vista.	bienestar social en diversos contextos y poblaciones.	nuevas soluciones tecnológicas que promuevan el bienestar social y la inclusión social de manera efectiva.
		Crear y compartir un plan de acción para reducir al mínimo la contaminación digital. Dimensiones clave a considerar: 1. **Creación y Diseño de Estrategias:** Evaluar la capacidad del usuario para desarrollar un plan de acción efectivo para minimizar la contaminación digital, lo que implica la habilidad para identificar problemas, establecer objetivos claros y diseñar estrategias concretas para abordar esos problemas. 2. **Análisis de Impacto y Evaluación:** Evaluar la capacidad del usuario para analizar el impacto de las estrategias propuestas y evaluar su efectividad a través de métricas y criterios específicos. Esto implica la capacidad de recopilar datos relevantes, analizar resultados y tomar decisiones informadas basadas en la evaluación. 3. **Comunicación y Colaboración:** Evaluar la capacidad del usuario para comunicar de manera efectiva el plan de acción propuesto y colaborar con otros para su implementación. Esto incluye la capacidad de presentar ideas de manera clara y persuasiva, así como trabajar en equipo para lograr objetivos comunes.
		Entender y mitigar los riesgos asociados con la Realidad Virtual y la Realidad Aumentada. Dimensiones clave a considerar: 1. **Conocimiento de los riesgos y beneficios:** Evaluar la comprensión profunda de los riesgos potenciales para la salud física y mental asociados con el uso de la Realidad Virtual y la Realidad Aumentada, así como la capacidad para identificar y analizar los posibles beneficios de estas tecnologías. 2. **Habilidades de mitigación de riesgos:** Evaluar la capacidad para desarrollar estrategias efectivas para mitigar los riesgos identificados, incluida la aplicación de medidas de seguridad y la promoción de prácticas de uso seguro y responsable de la Realidad Virtual y la Realidad Aumentada. 3. **Capacidad de análisis y evaluación:** Evaluar la habilidad para analizar críticamente las implicaciones de salud y bienestar de la Realidad Virtual y la Realidad Aumentada, así como la capacidad para evaluar el impacto de estas tecnologías en la vida cotidiana y

		proponer soluciones efectivas para abordar cualquier riesgo potencial.
Protección medioambiental		
Conocer los riesgos que puede correr mi salud física y psicológica al utilizar de forma incorrecta la tecnología. Dimensiones clave a considerar: 1. **Conocimiento de los efectos negativos para la salud física:** se centra en comprender cómo el uso inadecuado de la tecnología puede afectar directamente al cuerpo humano, como la fatiga ocular, el dolor de espalda debido a una mala postura, entre otros. 2. **Conciencia de los impactos en la salud mental:** evaluar la comprensión de cómo el uso excesivo de la tecnología puede influir en el bienestar psicológico, como el estrés, la ansiedad o la adicción a dispositivos electrónicos. 3. **Reconocimiento de las prácticas seguras de uso:** se enfoca en identificar las acciones y prácticas que pueden ayudar a mitigar los riesgos para la salud al utilizar la tecnología, como tomar descansos regulares, mantener una postura ergonómica y limitar el tiempo de pantalla.	Conocer cuál es el impacto del uso de las tecnologías digitales y tomar medidas para minimizar dicho impacto. Dimensiones clave a considerar: 1. **Conciencia ambiental digital:** Evaluar el conocimiento sobre los impactos ambientales del uso de tecnologías digitales y la comprensión de cómo las acciones digitales afectan al medio ambiente. 2. **Habilidades para la gestión ambiental digital:** Evaluar la capacidad para tomar medidas concretas para minimizar el impacto ambiental del uso de tecnologías digitales, como el uso eficiente de la energía, la reducción de residuos electrónicos y la adopción de prácticas sostenibles. 3. **Conciencia de seguridad digital:** Evaluar la comprensión de cómo las prácticas digitales pueden afectar la seguridad y privacidad de los datos, así como la adopción de medidas para proteger la información personal y la seguridad en línea.	Tomar medidas que reduzcan la huella de carbono para cuidar el entorno (uso de aplicaciones). Dimensiones clave a considerar: 1. **Conocimiento y comprensión de la huella de carbono digital:** - Esta dimensión evaluaría la comprensión del concepto de huella de carbono digital, incluyendo cómo se calcula y cómo las acciones individuales pueden influir en ella. 2. **Competencia técnica en la optimización del uso de aplicaciones:** - En esta dimensión se evaluaría la habilidad para utilizar técnicas y herramientas específicas dentro de las aplicaciones digitales con el fin de minimizar la huella de carbono. 3. **Conciencia de la sostenibilidad y la responsabilidad ambiental:** - Esta dimensión evaluaría la comprensión de la importancia de la sostenibilidad y la responsabilidad ambiental en el contexto del uso de aplicaciones digitales, así como la capacidad para tomar decisiones informadas que reduzcan el impacto ambiental.
	Fomentar un desarrollo tecnológico centrado en las personas y en la mejora del bienestar global, teniendo en cuenta su impacto en la sociedad y el entorno y aplicando criterios de sostenibilidad. Dimensiones clave a considerar: 1. **Conciencia del impacto tecnológico:** Comprender cómo las tecnologías afectan a las personas, la sociedad y el medio ambiente. Reconocer la importancia de considerar el impacto social y ambiental al desarrollar tecnologías. 2. **Aplicación de criterios de sostenibilidad:** Aplicar principios de sostenibilidad al desarrollo y uso de tecnologías. Evaluar el impacto de las tecnologías en términos de sostenibilidad ambiental y social. 3. **Enfoque centrado en las personas:** Valorar la importancia de desarrollar tecnologías que se adapten a las necesidades y capacidades de las personas. Considerar la inclusión y la accesibilidad al diseñar y utilizar tecnologías.	Crear y compartir un plan de acción para reducir al mínimo la contaminación digital. Dimensiones clave a considerar: 1. **Aplicar conocimientos técnicos:** evaluar la capacidad del usuario para aplicar conocimientos técnicos sobre tecnologías digitales y su impacto ambiental para diseñar estrategias efectivas de reducción de la contaminación digital. 2. **Analizar el impacto ambiental:** se centra en la capacidad del usuario para analizar el impacto ambiental de las tecnologías digitales y las prácticas digitales en relación con la contaminación y proponer medidas para mitigar este impacto. 3. **Crear soluciones sostenibles:** evaluar la habilidad del usuario para generar soluciones innovadoras y sostenibles para reducir la contaminación digital, teniendo en cuenta los principios de sostenibilidad y la minimización del impacto ambiental.
		Promover el diseño y uso de tecnologías sostenibles. Dimensiones clave a considerar:

		1. **Comprensión de conceptos y principios**: Evaluar la comprensión profunda de los conceptos relacionados con la sostenibilidad, el diseño y el uso de tecnologías sostenibles. 2. **Aplicación práctica**: Evaluar la capacidad para aplicar los conocimientos adquiridos en la promoción y desarrollo de tecnologías sostenibles en diferentes contextos. 3. **Análisis crítico y toma de decisiones**: Evaluar la capacidad para analizar críticamente situaciones relacionadas con el diseño y uso de tecnologías sostenibles, así como tomar decisiones informadas para promover prácticas más sostenibles.

Características de la prueba de evaluación

La prueba de certificación será realizada por ordenador mostrándose una prueba con las siguientes características:

- Se incluirán preguntas con distintos formatos para poder evaluar el conocimiento y la habilidad necesaria para nivel de competencia digital, incluyendo: preguntas de opción múltiple, simulaciones interactivas y preguntas donde los usuarios deberán examinar una situación mostrada en una imagen para escoger la opción correcta.
    - Nota: las preguntas de simulación interactivas se basarán en aplicaciones cuyo uso esté muy extendido y aceptado, evitando herramientas con funcionalidades o requisitos muy específicos.
- Por cada una de las 4 competencias digitales se incluirán 9 preguntas para cada uno de los niveles de competencia (básico, medio y avanzado), es decir, un total de 27 preguntas para cada competencia digital y de 108 preguntas para la certificación completa de SEGURIDAD.
- Una vez el usuario finalice la prueba se calculará el nivel alcanzado a nivel de competencia digital (básico, medio o avanzado) y a su vez, se calculará el nivel alcanzado en el área competencial (básico, medio o avanzado).
- Los rangos de puntuación que se han establecido para la obtención de los niveles a nivel de competencia digital son:
    - (0-4) Nivel Inicial
    - (4-13) Nivel básico
    - (14-22) Nivel medio
    - (23-27) Nivel avanzado
    - Para calcular el nivel a nivel de área competencial se realizará un cálculo similar pero proporcional sobre 27x4=108 preguntas totales.