

Este proyecto ha sido cofinanciado con el apoyo del programa Erasmus+ de la Comisión Europea. Esta publicación refleja únicamente las opiniones de sus autores, y ni la Comisión Europea ni el SEPIE se hacen responsables del uso que pueda hacerse de la información aquí contenida.

Tema

Competencias en alfabetización informacional

Duración

90-120 minutos

Nivel

Avanzado

Pasos del pensamiento computacional utilizados

Descomposición
Reconocimiento de patrones
Abstracción
Pensamiento algorítmico

Enfoque metodológico

Gamificación
Aprendizaje basado en retos
Aprendizaje colaborativo
Aprendizaje experiencial

CAJA DE APRENDIZAJE DE ACTIVIDADES DESENCHUFADAS

«¿Es seguro» – Comprender los riesgos digitales

En esta actividad, los participantes analizan situaciones digitales cotidianas que implican mensajes, correos electrónicos y llamadas telefónicas sospechosos. Mediante el trabajo colaborativo, evalúan el nivel de riesgo, identifican señales de alerta y deciden cuál es la acción más segura. Asimismo, aprenden a proteger su información personal y financiera, así como a verificar las solicitudes antes de responder. Al finalizar la actividad, habrán establecido normas sencillas, prácticas y aplicables de forma recurrente para utilizar los servicios digitales con mayor seguridad y confianza.

Grupo objetivo

Adultos con baja cualificación y escasas competencias digitales
Adultos con baja cualificación y escasa formación académica o profesional
Adultos con baja cualificación y escasa participación en programas de formación continua

Objetivos de aprendizaje

Desglosar una comunicación o solicitud digital en pasos claros y manejables.

Reconocer las señales de alerta habituales de comunicaciones digitales sospechosas o inseguras.

Identificar información sensible que debe protegerse, como contraseñas, datos bancarios y datos personales.

Aplicar reglas sencillas de toma de decisiones para determinar la respuesta probablemente más segura.

Explicar y demostrar decisiones seguras con claridad durante actividades de simulación de situaciones (juego de roles).

Áreas de Competencia

a) Competencias de Innovación

Creatividad
Pensamiento crítico
Resolución de problemas
Comunicación
Colaboración

b) Competencias de Alfabetización Informacional

Capacidad para acceder, comprender y analizar críticamente la información
Interpretación de contenido digital y visual
Conciencia de la influencia y los sesgos de los medios de comunicación

c) Competencias para la Vida y la Carrera Profesional

Flexibilidad y adaptabilidad
Iniciativa y autonomía
Sociabilidad y competencia intercultural
Productividad
Liderazgo y responsabilidad

Resultados del Aprendizaje

Desglosar una situación digital en pasos claros y manejables;

Identificar señales de alerta comunes en mensajes, correos electrónicos y llamadas telefónicas sospechosos o inseguros;

Distinguir entre acciones probablemente seguras, potencialmente arriesgadas e inseguras;

Aplicar algoritmos de seguridad sencillos para proteger información personal, financiera y de inicio de sesión;

Elegir y explicar una respuesta adecuada ante riesgos digitales cotidianos;

Demostrar una toma de decisiones probablemente más segura en situaciones de juego de roles.

Notas

Utilice ejemplos sencillos y realistas, como mensajes de texto, correos electrónicos, llamadas telefónicas y solicitudes en línea.

Seleccione situaciones que resulten familiares y relevantes para la vida cotidiana de los participantes.

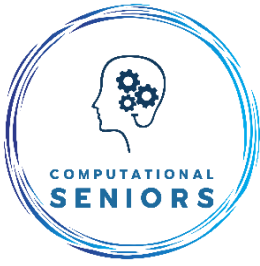
Fomente el debate y el intercambio voluntario de experiencias, sin presionar a los participantes para que revelen información personal.

Ofrezca orientación cuando sea necesario, permitiendo al mismo tiempo que los participantes analicen las situaciones y tomen sus propias decisiones.

Utilice un lenguaje claro y accesible, y explique cualquier término digital desconocido.

Haga hincapié en que cualquiera puede ser engañado por un mensaje convincente y en que pedir ayuda es una estrategia de seguridad sensata.

Refuerce la importancia de detenerse, comprobar y verificar una solicitud antes de responder, hacer clic en un enlace o compartir información.



Cofinanciado por
la Unión Europea

«¿Es seguro» –
Comprender los
riesgos digitales

Paso 1: Descomposición

Los alumnos adultos reciben tarjetas impresas que describen situaciones digitales sencillas y realistas; por ejemplo: «Recibes un mensaje solicitando tus datos bancarios» (Anexo 1) o «Recibes una llamada telefónica en la que te piden tu contraseña» (Anexo 2).

Se pide a los alumnos adultos que:

- Desglosen cada situación en pasos más pequeños y manejables;
- Identifiquen quién inició la comunicación y cómo se estableció el contacto;
- Determinen qué información o acción se está solicitando;
- Identifiquen qué se espera que haga el destinatario;
- Consideren las posibles consecuencias de seguir la solicitud.

Apoyo del facilitador:

- El facilitador puede preguntar: «¿Qué sucedió primero?», «¿Qué quiere la persona?», «¿Qué podría pasar si el destinatario sigue la solicitud?»;
- Ayudar a los alumnos adultos a centrarse en un aspecto a la vez;
- Hacer hincapié en comprender la situación con claridad.

Este paso ayuda a los alumnos adultos a comprender situaciones digitales de manera sencilla y estructurada.

Paso 2: Reconocimiento de patrones

Los estudiantes adultos reciben ejemplos adicionales de mensajes digitales, correos electrónicos, llamadas telefónicas y solicitudes en línea.

Se les pide que comparen las distintas situaciones e identifiquen similitudes y diferencias.

Identificar señales de alerta recurrentes, tales como:

- Solicitudes de información personal, financiera o de inicio de sesión;
- Lenguaje urgente o amenazante, como «¡actúe ahora!»;
- Remitentes desconocidos o inesperados;
- Enlaces o archivos adjuntos sospechosos;
- Ofertas, premios o promesas que parecen poco realistas;
- Presión para responder sin verificar la información.

Apoyo del facilitador:

- El facilitador puede preguntar: «¿Qué parece sospechoso?», «¿Ha visto algo así antes?»;

- Resaltar las señales de alerta recurrentes;
- Fomentar el intercambio de experiencias personales.

Este paso ayuda a los estudiantes adultos a reconocer patrones recurrentes en comunicaciones digitales sospechosas y a aplicar este conocimiento al evaluar situaciones desconocidas.

Paso 3: Abstracción

Los estudiantes adultos se centran en los elementos esenciales necesarios para evaluar si una situación digital es probablemente segura, sospechosa o insegura.

Se les pide que:

- Identifiquen información sensible que debe protegerse, como contraseñas, datos bancarios, códigos de verificación y datos personales;
- Distingan las señales de advertencia relevantes de los detalles menos importantes;
- Identifiquen el riesgo principal que presenta cada situación;
- Decidan si la comunicación es probablemente segura, si requiere verificación adicional o si es insegura;
- Formulen principios de seguridad sencillos que puedan aplicarse en situaciones similares.

Apoyo del facilitador:

- El facilitador puede preguntar: «¿Qué información no debe compartirse nunca?», «¿Qué detalle es el más importante para evaluar el riesgo?», «¿Qué se puede ignorar porque no afecta a la decisión?».
- Hacer hincapié en normas de seguridad sencillas.
- Ayudar a los estudiantes adultos a centrarse en los riesgos clave.

Este paso ayuda a los estudiantes adultos a simplificar situaciones digitales complejas, centrarse en la información más importante y tomar decisiones de seguridad más fundamentadas.

Paso 4: Pensamiento Algorítmico

Los participantes adultos desarrollan (individualmente o en grupo) un algoritmo claro y paso a paso para responder de manera segura ante comunicaciones digitales sospechosas.

El algoritmo debe guiar al usuario desde el momento en que recibe un mensaje, correo electrónico o llamada telefónica hasta la toma de la decisión final y la ejecución de la acción adecuada.

Se pide a los participantes adultos que:

- Definan los pasos principales del proceso de toma de decisiones;
- Ordenen los pasos en una secuencia lógica;
- Incluyan puntos de decisión utilizando reglas del tipo «si... entonces...»;
- Especifiquen qué acción debe emprenderse en cada situación;
- Representen visualmente el algoritmo mediante tarjetas, flechas, símbolos o un diagrama de flujo sencillo.

El algoritmo puede incluir la siguiente secuencia:

- Recibir la comunicación.
- Identificar al remitente y el canal de comunicación.
- Determinar qué información o acción se solicita.
- Detectar señales de alerta, como urgencia, amenazas, enlaces sospechosos, solicitudes inesperadas o peticiones de información confidencial.
- Decidir si es posible verificar la identidad del remitente.
- Elegir la respuesta adecuada.

Ejemplos de reglas de decisión:

- Si el remitente es desconocido, no responder de inmediato.
- Si la comunicación solicita una contraseña, un código de verificación o información bancaria, no compartir dicha información.

Por último, los participantes adultos:

- Ponen a prueba sus algoritmos de seguridad mediante simulaciones o juegos de rol;
- Explican y justifican sus decisiones;
- Comparan los distintos algoritmos desarrollados por los grupos;
- Identifican qué reglas resultan más útiles en situaciones de la vida real;

- Revisan su proceso de toma de decisiones cuando es necesario.

Apoyo del facilitador:

- El facilitador puede preguntar: «¿Qué debe hacer el usuario en primer lugar?», «¿Qué decisión hay que tomar en este punto?».
- Fomentar el pensamiento crítico para la toma de decisiones.
- Reforzar los hábitos de seguridad.

Este paso ayuda a los participantes adultos a transformar principios generales de seguridad en un algoritmo de toma de decisiones claro, estructurado y reproducible.