

---

“Capacitación en materia de **seguridad TIC** para padres,  
madres, tutores y educadores de menores de edad”

[Red.es]

---

## UNIDADES DIDÁCTICAS SUPLANTACIÓN DE IDENTIDAD PRIMARIA (6-12 años)

## UNIDADES DIDÁCTICAS SUPLANTACIÓN DE IDENTIDAD PRIMARIA

---

UNIDADES DIDÁCTICAS SUPLANTACIÓN DE IDENTIDAD PRIMARIA.....	2
1. UNIDAD DIDÁCTICA I: PREVENIR LA SUPLANTACIÓN DE IDENTIDAD EN MENORES .....	4
1.1. FICHA RESUMEN.....	4
1.2. OBJETIVOS DIDÁCTICOS .....	5
1.3. COMPETENCIAS.....	5
1.4. CONTENIDOS.....	6
1.5. METODOLOGÍA .....	7
1.6. ACTIVIDADES .....	8
1.6.1. Sesión 1: Protege tus datos.....	8
1.6.2. Sesión 2: Adivina quién es .....	10
1.7. EVALUACIÓN.....	13
1.8. DOCUMENTACIÓN DE APOYO.....	13
2. UNIDAD DIDÁCTICA II: CUANDO SOY VÍCTIMA DE SUPLANTACIÓN DE IDENTIDAD ¿QUÉ PUEDO HACER? .....	15
2.1. FICHA RESUMEN.....	15
2.2. OBJETIVOS DIDÁCTICOS .....	16
2.3. COMPETENCIAS.....	16
2.4. CONTENIDOS.....	17
2.5. METODOLOGÍA .....	18
2.6. ACTIVIDADES .....	18
2.6.1. Sesión 1: ¿Cómo sé si me han suplantado? .....	18
2.6.2. Sesión 2: Han suplantado mi identidad, ¿ahora qué hago?.....	20
2.7. EVALUACIÓN.....	21
2.8. DOCUMENTACIÓN DE APOYO.....	22

*La presente publicación pertenece a Red.es y está bajo una licencia Reconocimiento-No comercial 4.0 España de Creative Commons, y por ello está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:*

- *Reconocimiento: El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a Red.es como a su sitio web: [www.red.es](http://www.red.es). Dicho reconocimiento no podrá en ningún caso sugerir que Red.es presta apoyo a dicho tercero o apoya el uso que hace de su obra.*
- *Uso No Comercial: El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.*

*Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de Red.es como titular de los derechos de autor. Nada en esta licencia menoscaba o restringe los derechos morales de Red.es.*

*<http://creativecommons.org/licenses/by-nc/4.0/deed.es>*

# 1. UNIDAD DIDÁCTICA I: PREVENIR LA SUPLANTACIÓN DE IDENTIDAD EN MENORES

## 1.1. FICHA RESUMEN

### Objetivos didácticos

- Conceptualizar la suplantación de identidad.
- Trabajar la prevención de la suplantación de identidad.

### Competencias

- **Competencias digitales:** de información, en comunicación y de seguridad.
- **Competencias básicas:** en comunicación lingüística, en el conocimiento y la interacción con el mundo físico, de autonomía e iniciativa personal, social y ciudadana y para aprender a aprender.

### Contenidos

- **Conceptuales:**
  - Identidad digital, suplantación de identidad, robo o usurpación de identidad.
- **Procedimientos:**
  - Conocimiento de los tipos de fraudes relacionados con la suplantación de identidad.
  - Modos principales de realizar una suplantación de identidad.
  - Puesta en práctica de medidas que favorezcan la prevención de una suplantación de identidad.
  - Conocer las medidas básicas de navegación segura a través la red que sirvan para prevenir una suplantación de identidad.
- **Actitudes:**
  - Despertar el sentido de precaución, cautela e y desconfianza frente a indicios de una posible suplantación de identidad.
  - Desarrollar el sentido crítico al confiar en los demás en la red.
  - La importancia de hacer un uso responsable de las nuevas tecnologías y tener un comportamiento digital adecuado y seguro para prevenir una suplantación de identidad.

### Metodología

- Temporalización: 2 sesiones (de 45 minutos cada una).
- Metodología basada en conocimientos previos, activa, participativa, de descubrimiento.
- Recursos didácticos: debate, puesta en común, reflexión grupal y anuncio.

### Actividades

- Sesión 1. Protege tus datos.
- Sesión 2. Adivina quién es.

### Evaluación

- Métodos de evaluación: participación, observación y actividad de evaluación.
- Criterios de evaluación:
  - Los/as alumnos/as conocen qué es la suplantación de identidad y la identidad digital, qué es un robo o usurpación de identidad, las distintas técnicas de suplantación de identidad, recomendaciones para la prevención de la suplantación de identidad, estrategias de realizar una navegación segura en Internet.
  - Los/las alumnos/as desarrollan una actitud crítica y de denuncia ante una situación de suplantación de identidad y de empatía ante la víctima.
  - Los/as alumnos/as diferencian qué datos sirven para identificarlos y por tanto es peligroso compartirlos y facilitarlos a desconocidos, ya que podrían derivar en una suplantación de identidad.

### Documentación de apoyo

- Monográfico de Suplantación de Identidad.
- Curso en línea Seguridad TIC y Menores.

## 1.2. OBJETIVOS DIDÁCTICOS

Cuando termine de ejecutarse la unidad didáctica, el alumnado deberá ser capaz de identificar, reconocer, prevenir y poner en práctica todos los conocimientos asimilados durante el desarrollo de la unidad didáctica.

- Conceptualizar el riesgo: ¿Qué es la suplantación de identidad?
  - Conocer qué es la identidad digital.
  - Saber a qué se refiere el concepto de suplantación de identidad.
  - Aprender que es un robo o usurpación de la identidad.
- Trabajar la prevención de la suplantación de identidad.
  - Aplicar las medidas de la navegación segura en Internet junto con las orientaciones y apoyo de los mayores, que permitan prevenir el riesgo de suplantación de identidad.
  - Comportarse de una manera responsable y aplicando las normas aprendidas previamente.
  - Ser consciente de los peligros a los que estamos expuestos en la red.
  - Tomar consciencia del papel activo que el menor tienen en la prevención de una suplantación de identidad.

## 1.3. COMPETENCIAS

Esta unidad didáctica permite al alumnado participante trabajar las **competencias digitales** tomando como referencia las del “Marco Común de la Competencia Digital Docente” (INTEF: Ministerio de Educación, Cultura y Deporte):

- a. Competencia de información: el alumnado recibirá instrucción sobre cómo navegar y buscar información en Internet para prevenir el riesgo que supone la suplantación de identidad, aplicando un criterio de filtrado, evaluando la información hallada y aplicando un sentido crítico.
- b. Competencia en comunicación: el alumnado se entrenará en el desarrollo de habilidades para interactuar con las nuevas tecnologías, con el objetivo de compartir información y contenidos de forma adecuada, siendo crítico con la información que encuentre, evitando de este modo el riesgo que supone que otros accedan a información y datos que podrían llevar a una suplantación de identidad.

- c. Competencia de seguridad: el alumnado recibirá información sobre cómo protegerse de los riesgos que suponen la suplantación de identidad.

Esta unidad didáctica permite trabajar con el alumnado participante las siguientes **competencias básicas** establecidas en la Ley Orgánica 2/2006, de 3 de mayo, de Educación:

- a. Competencia en comunicación lingüística: el alumnado conocerá el lenguaje específico relacionado con la suplantación de identidad. Incluyendo el uso del lenguaje no sólo para describir, sino interpretar, representar, comprender, construir conocimiento, así como la autorregulación de pensamiento, emociones y conducta.
- b. Competencia en el conocimiento y la interacción con el mundo físico: el alumnado entrenará la habilidad para interactuar con el mundo físico, en los aspectos generados por la acción humana, previniendo en todo momento una suplantación de identidad, posibilitando la comprensión de sucesos, la predicción de consecuencias y la actividad dirigida a la mejora y preservación de las condiciones de vida propia y de los demás.
- c. Competencia de autonomía e iniciativa personal: el alumnado recibirá información para desenvolverse adecuadamente y de forma independiente para prevenir los riesgos provocados por una suplantación de identidad.
- d. Competencia social y ciudadana: el alumnado reflexionará sobre la realidad social en la que vivimos, empleando el juicio ético basado en valores y buenas prácticas. Se fomentará la actuación del alumnado bajo criterio propio, siempre orientado a la mejora de la convivencia.
- e. Competencia para aprender a aprender: con la metodología empleada se pretende que el alumnado disponga de habilidades para iniciarse en su propio aprendizaje y que sea capaz de continuar aprendiendo de forma cada vez más eficaz y autónoma frente a evitar compartir información y datos personales en diferentes situaciones y contextos que pueda encontrar a lo largo de su vida.

#### 1.4. CONTENIDOS

- **Conceptuales:**
  - Identidad digital.
  - Suplantación de identidad.
  - Robo o usurpación de identidad.

- **Procedimentales:**
  - Conocimiento de los tipos de fraudes relacionados con la suplantación de identidad.
  - Modos principales de realizar una suplantación de identidad.
  - Puesta en práctica de medidas que favorezcan la prevención de una suplantación de identidad.
  - Conocer las medidas básicas de navegación segura a través la red que sirvan para prevenir una suplantación de identidad.
- **Actitudinales:**
  - Despertar el sentido de precaución, cautela e y desconfianza frente a indicios de una posible suplantación de identidad.
  - Desarrollar el sentido crítico al confiar en los demás en la red.
  - La importancia de hacer un uso responsable de las nuevas tecnologías y tener un comportamiento digital adecuado y seguro para prevenir una suplantación de identidad.

## 1.5. METODOLOGÍA

Esta unidad didáctica se compone de una serie de actividades programadas para realizar en dos sesiones. Estas actividades tendrán una duración total aproximada de una hora lectiva cada una y es conveniente que se realicen en el orden establecido.

No debe tratarse de una clase magistral sino que la metodología debe ser activa y participativa en todo momento y muy interactivo entre docente y alumnado, fomentando el diálogo y el aprendizaje constructivo mediante actividades lúdicas.

Se utilizarán recursos didácticos como el debate, puesta en común, reflexión grupal y anuncio.

Para desarrollar la unidad didáctica será necesario el siguiente material:

- Pizarra o papelógrafo.
- Cartulina y rotuladores.
- Folios.

## 1.6. ACTIVIDADES

Las actividades que se van a realizar en esta unidad didáctica se estructuran en diferentes sesiones del siguiente modo.

### 1.6.1. Sesión 1: Protege tus datos

**Parte inicial:** En primer lugar es necesario que el docente realice una explicación previa para situar al alumnado en el concepto de suplantación de identidad y lo que supone este riesgo.

Se recomienda comenzar por un *Brainstorming* o tormenta de ideas para detectar el conocimiento previo del alumnado. El docente introducirá preguntas al alumnado para debatir los conocimientos previos.

A continuación se explicará en clase algunos conceptos básicos relacionados con el riesgo de suplantación de identidad: concepto, algunos ejemplos característicos de este tipo de fraude, formas principales de suplantación de identidad, y consecuencias de *suplantación de identidad*. Se aporta el siguiente cuadro conceptual que puede servir de referencia al docente (siempre teniendo en cuenta que la explicación debe adaptarse al alumnado de primaria):

#### Guía para el docente

La **identidad digital** puede ser definida como el conjunto de la información sobre un individuo o una organización expuesta en Internet (datos personales, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital.

Entendemos **la suplantación de identidad** como **“el uso de información personal para hacerse pasar por otra persona con el fin de obtener un beneficio propio”**.

#### **Algunos ejemplos característicos de este tipo de fraude**

- Registrar un perfil en una red social con el nombre de otra persona sin su consentimiento y utilizando datos o imágenes de la víctima.
- Acceder sin consentimiento a una cuenta ajena para tener acceso a la información allí almacenada.
- Acceder sin consentimiento a una cuenta ajena utilizando los datos personales y haciéndose pasar por el suplantado.
- Publicación sin consentimiento de anuncios o comentarios utilizando el nombre de un tercero o incluso utilizando sus datos personales para identificarse con terceras personas a través, por ejemplo, de correo o mensajería instantánea (Whatsapp).

Las dos **formas principales de suplantación de identidad** entre menores de primaria (6-12 años) son:

1. Entrar sin consentimiento en la cuenta de otro menor para:

- Acceder a información sensible como puede ser el caso de una foto o un video.
- Acosar o desprestigiar a la otra persona (casos de suplantación de identidad), por ejemplo, publicando comentarios polémicos o denigrantes que serán vistos por terceros.
- Ganarse la amistad de un menor con el fin de cometer un abuso sexual (casos de grooming donde el acosador utiliza la usurpación de identidad para acceder a cuentas que sirvan de “puente” para facilitar el contacto con la víctima).

2. Crear una cuenta para hacerse pasar por otra persona. Aunque esta forma se suele dar en menores, es uno de los casos más frecuentemente utilizados para suplantar a gente famosa.

**Parte principal:** se formarán grupos de 4 alumnos/as, cada grupo debe aportar 6 formas, medios, lugares, web... en los que su información personal pueda hacerse pública (algunos ejemplos son: redes sociales, mail, mensajes de Whatsapp, juegos online...). Este ejercicio será muy breve, dispondrán de 5 minutos para trabajar en grupo. A continuación, por turnos, un portavoz de cada grupo pondrá en común los resultados. Con este ejercicio se pretende que reflexionen sobre contextos en los que pueden tener riesgo de hacer pública información y datos personales, para trabajar a continuación una serie de preguntas.

Para finalizar la actividad, se realizará un pequeño debate que permita a los alumnos reflexionar sobre la importancia de preservar sus datos e información personal para prevenir la suplantación de identidad. Para ello el docente utilizará las siguientes preguntas:

- ¿Alguna vez habéis facilitado información personal a desconocidos? ¿A través de qué medio? ¿En qué contexto?
- ¿En alguna ocasión habéis aportado información de otra persona a un desconocido o conocido? ¿Le habéis pedido permiso?
- ¿Os ha causado algún tipo de problema? ¿Y una fotografía? ¿Y un vídeo?
- ¿Creéis adecuado que todo el mundo pueda acceder a vuestros datos e imágenes? ¿Y si es otra persona quien hace esto posible?

- ¿Qué podría pasar si otra persona tiene vuestros datos personales y puede hacerse pasar por vosotros?

**Parte final:** El docente concluirá el debate haciendo reflexionar al alumnado sobre las graves consecuencias que puede tener la suplantación de identidad y cómo preservando nuestra información y datos personales podemos prevenir este riesgo. Si los demás no tienen nuestros datos, no pueden suplantarnos.

### 1.6.2. Sesión 2: Adivina quién es

**Parte inicial:** explicación en clase cómo pueden los/as alumnos/as tener un papel activo para prevenir una situación de Suplantación de identidad, es decir cómo pueden prevenir este riesgo. Para ello utilizará la siguiente guía en la que se detalla las recomendaciones a trasladar a los menores para prevenir la suplantación de identidad.

#### Guía para el docente

Los datos personales son aquellos que pueden servir para identificarnos en un contexto determinado.

Hay que tener en cuenta que, quizás, un dato aislado en un determinado momento o contexto no es suficiente para identificar a una persona. Sin embargo, si existen otros datos en otros lugares de la Red y es posible relacionarlos entre sí, pueden llegar a identificar a la persona. En ese caso, la privacidad se puede ver comprometida si terceras personas usan esa información sin nuestro conocimiento con intenciones de gastarnos una broma, reírse un rato, obtener un beneficio, etc. Aunque todos los datos personales son importantes, quizás la imagen, nuestra fotografía, es el que nos identifica con mayor claridad.

#### **Recomendaciones a trasladar a los/as menores para evitar la suplantación de identidad**

- Limita la difusión voluntaria de datos personales y privados en redes sociales, juegos online, mensajería instantánea, formularios y aplicaciones.
- Configura de forma correcta las opciones de privacidad de los diferentes sitios web que frecuentas.
- Debes ser discretos a la hora de publicar fotografías en la web y, sobre todo, de que se debe «pensar antes de publicar» de forma impulsiva para poder valorar las posibles consecuencias del comportamiento en la red.
- Cuenta con cuentas de usuario diferentes para cada una de las personas que utilizan el equipo compartido con contraseñas personales para regular el acceso a éste, cuando compartas ordenador con amigos y sobre todo con desconocidos. De esta forma, cada usuario podrá tener su propio escritorio -con aquellos archivos y carpetas a los que pueda acceder- de forma que tan solo el usuario administrador,

con permiso para poder administrar las diferentes cuentas, pueda instalar aplicaciones o modificar aspectos importantes de la configuración.

- Bloquea las ventanas emergentes.
- Haz uso de los filtros antispam.
- Lleva a cabo una adecuada gestión de contraseñas. Modifícalas periódicamente.
- Para poder llevar a cabo una buena práctica en el uso de servicios tales como el correo electrónico, las redes sociales, la mensajería instantánea o la propia navegación no se debe olvidar que no debes acceder a enlaces que resulten sospechosos. Igualmente se debe tener precaución con las descargas que se realizan, desconfiar de remitentes desconocidos en correos y no abrir ficheros adjuntos sospechosos.
- Así mismo, algunos indicios que se deben tener en cuenta para sospechar que un correo electrónico tiene fines maliciosos son:
  - Enlaces disfrazados: en este caso, los enlaces en el correo electrónico estarán presentados de forma que parezcan auténticos.
  - “Es urgente que actúes”: se debe ser cautelosos con los correos que den sentido de urgencia, con mensajes tales como: “tu cuenta está a punto de ser eliminada”, “tu cuenta debe ser actualizada”, etc. Se trata de un claro ejemplo de técnica de ingeniería social, al apremiar al lector y dificultar que pueda tomar una decisión razonada.
  - Cuenta equivocada: debes estar seguro que los correos llegan a la cuenta adecuada y a la que se ha facilitado de entre las varias que se pueden tener para ello. De lo contrario se podría sospechar que se trata de un fraude.
- En el caso de juegos en línea, presta atención al software del juego utilizando el programa oficial del mismo y asegurarse también de que los plugins (programas que se anexan a otros para aumentar sus funcionalidades) que se descarguen sean realmente oficiales.
- Ten cuidado con los mecanismos de recuperación de contraseñas. En este sentido hay que tener presente que se deben establecer preguntas secretas que solamente sean conocidas por la propia persona como medida de seguridad.
- Bloquear el ordenador y cerrar las sesiones al terminar de usar el equipo como medida para “cerrar la puerta” a cualquier persona ajena al mismo.
- Ten cuidado con las conexión en ordenadores públicos y las redes WiFi gratis.
- Instala y habilita un cortafuegos en tu equipo.
- Actúa con cautela ya que no todos los datos que se encuentran en la web han de ser ciertos.
- Establece una contraseña para el bloqueo de la pantalla del teléfono.

**Parte principal:** El docente leerá al alumnado el siguiente texto:

Los datos personales son todos aquellos datos que pueden permitir la identificación de una persona: nombre, apellidos, DNI, teléfono, domicilio, dirección de email y la propia imagen que, en muchos casos, es el dato que más fácilmente permite una identificación.

Otras personas que no conocemos nos pueden identificar a través de la información que existe sobre nosotros en Internet.

Se dividirá la clase en 4 grupos. Cada alumno escribirá una serie de datos personales dos veces, en las dos mitades diferentes de una hoja, que luego separará. Una de las partes la entregará al docente y la otra la conservará ocultando su contenido. La información que deben incluir en la hoja es la siguiente:

- a. Los/as alumnos/as del grupo 1 escribirán: nombre, apellidos y teléfono.
- b. El grupo 2: domicilio, dirección de e-mail, descripción de una mancha de nacimiento.
- c. El grupo 3: nombre de tus padres, color de tu pelo y tu deporte favorito.
- d. El grupo 4: últimas vacaciones, muñeco preferido de la infancia y tu ropa preferida.

Como si de un sorteo se tratara, se van sacando cada una de estas mitades, se leen en voz alta los datos personales y se trata de adivinar a qué persona de la clase pertenecen. De esta forma, se puede comprobar que algunos datos, en ciertos contextos, permiten fácilmente reconocer a una persona (grupos 1 y 2). Por el contrario hay datos que dificultan más la identificación de la persona (grupos 3 y 4). El docente relacionará este ejercicio con la posibilidad de que suplanten la identidad de una persona si facilitamos una u otra información en Internet.

**Parte final:** por grupos (pueden ser los mismos que para el ejercicio anterior) el alumnado deberá diseñar y realizar un cartel de anuncio dirigido a menores de su edad, en el que refleje con texto e imágenes recomendaciones para prevenir la suplantación de identidad. Los anuncios se realizarán con cartulinas y rotuladores y se expondrán en clase.

## 1.7. EVALUACIÓN

Para comprobar que los objetivos planteados han sido alcanzados por el alumnado, el docente se basará en la observación, la ejecución de las actividades, la realización del mural y la participación en el debate.

Los criterios que deben contemplar en la evaluación son los siguientes:

Los/as alumnos/as conocen:

- Qué es la suplantación de identidad y la identidad digital.
- Qué es un robo o usurpación de identidad.
- Las distintas técnicas de suplantación de identidad
- Recomendaciones para la prevención de la suplantación de identidad.
- Estrategias de realizar una navegación segura en Internet.

Los/las alumnos/as desarrollan:

- Una actitud crítica y de denuncia ante una situación de suplantación de identidad.
- Una actitud de empatía ante la víctima de una situación de suplantación de identidad.

Los/as alumnos/as diferencian:

- Qué datos sirven para identificarlos y por tanto es peligroso compartirlos y facilitarlos a desconocidos, ya que podrían derivar en una suplantación de identidad.

## 1.8. DOCUMENTACIÓN DE APOYO

Los siguientes recursos son de utilidad para ampliar el conocimiento sobre la suplantación de identidad:

### **Monográfico de suplantación de identidad**

Marco teórico de referencia para sensibilizar sobre los riesgos de la suplantación de identidad y ofrecer pautas a padres, madres, tutores y educadores para su prevención entre los menores, así como mecanismos de actuación en caso de producirse.

Disponible en el portal de Chaval.es: <http://www.chaval.es>

### Curso en línea Seguridad TIC y Menores

Curso de 30 horas de duración bajo metodología **MOOC** (*Massive Online Open Course* - Curso en línea masivo y abierto-) dirigido a padres y educadores. Sensibiliza sobre los riesgos a los que se enfrentan los menores en el uso de Internet y las nuevas tecnologías, ofreciendo estrategias, pautas y recomendaciones para su prevención y respuesta en caso de producirse un incidente. Contiene un módulo exclusivo de suplantación de identidad.

Disponible en: <http://www.chaval.es>

## 2. UNIDAD DIDÁCTICA II: CUANDO SOY VÍCTIMA DE SUPLANTACIÓN DE IDENTIDAD ¿QUÉ PUEDO HACER?

### 2.1. FICHA RESUMEN

#### Objetivos didácticos

- Dar pautas sobre cómo actuar ante un caso de suplantación de identidad.
- Aprender a identificar una suplantación de identidad.

#### Competencias

- **Competencias digitales:** de información, en comunicación y de seguridad.
- **Competencias básicas:** en comunicación lingüística, en el conocimiento y la interacción con el mundo físico, de autonomía e iniciativa personal, social y ciudadana y para aprender a aprender.

#### Contenidos

- **Conceptuales:**
  - Conceptualización del *grooming* como delito.
  - Repaso de conceptos de la unidad didáctica primera: identidad digital, suplantación de identidad, robo o suplantación de identidad.
- **Procedimentales:**
  - Identificación o reconocimiento de una suplantación de identidad.
  - Pautas para actuar frente a una suplantación de identidad.
- **Actitudinales:**
  - Desarrollo de actitud de cautela, precaución y desconfianza ante posibles indicios de suplantación de identidad.
  - Confianza de comunicación a un adulto responsable frente a una posible suplantación de identidad.
  - Actitud de denuncia frente a una posible suplantación de identidad.

#### Metodología

- Temporalización: 2 sesiones (de 45 minutos cada una).
- Metodología basada en conocimientos previos, activa, participativa, experiencial y constructiva.
- Recursos didácticos: pizarra, ordenador, papel, bolígrafos, proyector.

#### Actividades

- Sesión 1. ¿Cómo sé si me han suplantado?
- Sesión 2. Han suplantado mi identidad, ¿ahora qué hago?

#### Evaluación

- Métodos de evaluación: participación, observación y actividad de evaluación.
- Criterios de evaluación:
  - Los alumnos conocen cómo reconocer si se están haciendo pasar por ellos en Internet.
  - Los alumnos conocen cómo se siente una persona a la que han suplantado su identidad.
  - Los/as alumnos/as reflexionan.
  - Los alumnos conocen cómo actuar ante una suplantación de identidad.

#### Documentación de apoyo

- Monográfico de Suplantación de Identidad.
- Curso en línea Seguridad TIC y Menores.

## 2.2. OBJETIVOS DIDÁCTICOS

En la siguiente unidad didáctica se abordarán los siguientes objetivos:

- Dar pautas sobre cómo actuar ante un caso de *suplantación de identidad*:
  - Aprender a identificar una suplantación de identidad.
  - Actuar ante una suplantación de identidad.
  - Buscar ayuda ante una suplantación de identidad.

## 2.3. COMPETENCIAS

Esta unidad didáctica permite al alumnado participante trabajar las **competencias digitales** tomando como referencia las del “Marco Común de la Competencia Digital Docente” (INTEF: Ministerio de Educación, Cultura y Deporte):

- a. Competencia de información: el alumnado recibirá instrucción sobre cómo navegar y buscar información en Internet para actuar frente al riesgo que supone la suplantación de identidad, aplicando un criterio de filtrado, evaluando la información hallada y aplicando un sentido crítico.
- b. Competencia en comunicación: el alumnado se entrenará en el desarrollo de habilidades para interactuar con las nuevas tecnologías, con el objetivo de compartir información y contenidos de forma adecuada, siendo crítico con la información que encuentre, evitando de este modo el riesgo que supone que otros accedan a información y datos que podrían llevar a una suplantación de identidad.
- c. Competencia de seguridad: el alumnado recibirá información sobre cómo protegerse de los riesgos que suponen la suplantación de identidad.

Esta unidad didáctica permite trabajar con el alumnado participante las siguientes **competencias básicas** establecidas en la Ley Orgánica 2/2006, de 3 de mayo, de Educación:

- a. Competencia en comunicación lingüística: el alumnado conocerá el lenguaje específico relacionado con la suplantación de identidad. Incluyendo el uso del lenguaje no sólo para describir, sino interpretar, representar, comprender, construir conocimiento, así como la autorregulación de pensamiento, emociones y conducta.

- b. Competencia en el conocimiento y la interacción con el mundo físico: el alumnado entrenará la habilidad para interactuar con el mundo físico, en los aspectos generados por la acción humana, previniendo en todo momento una suplantación de identidad, posibilitando la comprensión de sucesos, la predicción de consecuencias y la actividad dirigida a la mejora y preservación de las condiciones de vida propia y de los demás.
- c. Competencia de autonomía e iniciativa personal: el alumnado recibirá información para desenvolverse adecuadamente y de forma independiente para prevenir los riesgos provocados por una suplantación de identidad.
- d. Competencia social y ciudadana: el alumnado reflexionará sobre la realidad social en la que vivimos, empleando el juicio ético basado en valores y buenas prácticas. Se fomentará la actuación del alumnado bajo criterio propio, siempre orientado a la mejora de la convivencia.
- e. Competencia para aprender a aprender: con la metodología empleada se pretende que el alumnado disponga de habilidades para iniciarse en su propio aprendizaje y que sea capaz de continuar aprendiendo de forma cada vez más eficaz y autónoma frente a evitar compartir información y datos personales en diferentes situaciones y contextos que pueda encontrar a lo largo de su vida.

## 2.4. CONTENIDOS

- **Conceptuales:**
  - Repaso de conceptos de la unidad didáctica primera: identidad digital, suplantación de identidad, robo o suplantación de identidad.
- **Procedimentales:**
  - Identificación o reconocimiento de una suplantación de identidad.
  - Pautas para actuar frente a una suplantación de identidad.
- **Actitudinales**
  - Desarrollo de actitud de cautela, precaución y desconfianza ante posibles indicios de suplantación de identidad.
  - Confianza de comunicación a un adulto responsable frente a una posible suplantación de identidad.
  - Actitud de denuncia frente a una posible suplantación de identidad.

- Fomento de la autonomía y la responsabilidad del menor para comunicar y denunciar una posible suplantación.

## 2.5. METODOLOGÍA

No debe tratarse de una clase magistral sino que la metodología debe ser activa, experiencial y participativa en todo momento y muy interactivo entre profesor y alumno, fomentando el diálogo y el aprendizaje constructivo mediante actividades lúdicas.

La unidad didáctica se llevará a cabo en dos sesiones, con una hora lectiva de duración cada una. El orden de las actividades es recomendable que se mantenga, ya que cada una se estructura en una parte inicial de introducción y conceptualización del riesgo, una parte principal en la que se desarrolla la actividad y una parte final en la que el docente realizará las conclusiones.

Se utilizarán recursos didácticos como el debate grupal, el *Brainstorming*, trabajo en grupo, reflexión grupal y el juego, adaptados siempre al grupo de edad al que nos dirigimos.

Para desarrollar la unidad didáctica será necesario el siguiente material:

- Pizarra o papelógrafo.
- Rotuladores.
- Folios.
- Post-it.
- Material que cada alumno/a tenga habitualmente en su pupitre.

## 2.6. ACTIVIDADES

Las actividades que se van a realizar en esta unidad didáctica se estructuran en sesiones del siguiente modo:

### 2.6.1. Sesión 1: ¿Cómo sé si me han suplantado?

**Parte inicial:** en primer lugar es necesario que el docente comience haciendo un *Brainstorming* o tormenta de ideas para hacer un repaso de los conceptos explicados en la unidad didáctica 1 de primaria de suplantación de identidad. (Si no se ha realizado la unidad 1 de primaria de suplantación de identidad es necesario realizar una breve explicación con los contenidos incluidos en la parte inicial de la actividad 1 de dicha unidad didáctica).

Para ello el docente introducirá la lluvia de ideas con preguntas como las siguientes:

- ¿Recordáis en qué consiste el riesgo de suplantación de identidad?
- ¿Recordáis cómo pueden suplantar vuestra identidad?
- ¿Os acordáis de qué técnicas podéis utilizar para prevenir la suplantación de identidad?

**Parte principal:** a continuación el docente pedirá a la mitad de los/as niños/as de la clase que salgan al pasillo, la otra mitad de la clase ocupará cada uno un lugar que no es el suyo e intentará dejar algún rastro, alguna huella de que ha estado haciéndose pasar por el otro/a compañero/a. Algunas huellas serán más evidentes y otras más difíciles de encontrar. Por ejemplo: realizarán un ejercicio en una libreta, cambiarán el estuche de bolsillo en la mochila, usurparán un bolígrafo, escribirán en una libreta en un color que no es el habitual... cualquier acto que suponga haber suplantado la identidad del/a otro alumno/a.

Acto seguido los/as alumnos/as del pasillo pasarán a sus pupitres y dispondrán de 10 minutos para revisar sus cosas y averiguar qué rastro ha dejado el suplantador de identidad.

Seguidamente cada alumno/a pondrá en común qué tipo de suplantación ha sufrido, cómo se ha sentido, qué consecuencias podría tener, etc.

El docente hará una breve comparación con la suplantación de identidad en la red, realizando una reflexión con el alumnado. Podría guiarla con preguntas del tipo: ¿qué consecuencias podría tener una suplantación en la red? ¿Cómo os daríais cuenta de que habéis sufrido una suplantación de la identidad en Internet?

Parte final: para concluir la actividad el docente presentará al alumnado la información sobre cómo podemos saber que hemos sufrido una suplantación de identidad. Para ello puede utilizar como referencia el siguiente esquema:

### Guía para el docente

#### ¿Cómo podemos saber que hemos sufrido una suplantación de identidad?

Entre los indicios que los menores tienen para detectar que han sufrido una suplantación de identidad se encuentran:

- Accesos o usos anómalos de las cuentas.
- Inminente desactivación o activación de algún servicio.
- Cambio en el estado de los juegos online.

#### 2.6.2. Sesión 2: Han suplantado mi identidad, ¿ahora qué hago?

**Parte inicial:** el docente iniciará la actividad realizando una exposición como recordatorio de la sesión anterior, haciendo hincapié en cómo podemos comprobar que hemos sufrido una suplantación de identidad.

**Parte Principal:** el docente dividirá al grupo clase en grupos de 4 o 5 alumnos/as. Cada grupo debe hacer una lluvia de ideas sobre qué hacer si sufren una suplantación de identidad, teniendo en cuenta que en la sesión anterior lo han sufrido en primera persona. Serán válidas aportaciones sobre qué hacer ante una suplantación de identidad en red o fuera de ella. Las diferentes aportaciones que generen deben anotarlas cada una en un *post-it* que el docente les repartirá (de color diferente a cada grupo) y a continuación pegarlos en la pizarra. Para hacer la dinámica más divertida se puede dar un tiempo de 10 o 15 minutos en los que cada grupo debe aportar el máximo de mecanismos de respuesta posibles y según los vayan generando irán pegándolos en la pizarra.

Finalizado el tiempo, un portavoz de cada grupo leerá y explicará las propuestas de su grupo, se puntuará la actividad a modo de juego, recibiendo un punto por cada propuesta original y diferente del resto y 0,5 por cada propuesta válida, pero que se repita con el resto de grupos.

Parte final: como conclusión el docente anotará en la pizarra todos los mecanismos de respuesta aportados entre todos los grupos y a continuación completará la explicación con las recomendaciones que se plantean en la siguiente guía.

### Guía del docente

#### **En caso de ser víctimas de suplantación de identidad tenemos que conocer:**

- Denunciar ante la plataforma o el servicio a través del cual haya tenido lugar, notificando esta situación a la red social o sistema implicado para solicitarles que tomen las medidas necesarias para restaurar el nivel de seguridad anterior a la suplantación de identidad.
- En caso de denuncia, es necesario recopilar todas las pruebas y evidencias relacionadas con la suplantación de identidad producida en el menor.
- Contactar con los buscadores que están enlazando a esa información para evitar la indexación a la misma.
- Denunciar el caso a la agencia de protección de datos.
- Como medida de seguridad, sería conveniente cambiar todas las contraseñas que piense le hayan podido interceptar (Ej.: Redes sociales, correo electrónico, etc.), y en la medida de lo posible, tratar de deshacer lo que haya realizado el agresor en nuestro nombre.
- En caso de requerir denunciar un caso de suplantación de identidad en menores ante los cuerpos de seguridad del estado, se deben conocer los siguientes grupos especializados:

○Policía Nacional (Brigada de Investigación Tecnológica): [www.policia.es/bit](http://www.policia.es/bit)  
 Correo electrónico (consultas genéricas): [delitos.tecnologicos@policia.es](mailto:delitos.tecnologicos@policia.es) Correo electrónico (pornografía infantil): [denuncias.pornografia.infantil@policia.es](mailto:denuncias.pornografia.infantil@policia.es) Teléfonos: 915.822.751/752/753/754/75

○Guardia Civil (Grupo de Delitos Telemáticos)  
[www.gdt.guardiacivil.es/webgdt/home\\_alerta.php](http://www.gdt.guardiacivil.es/webgdt/home_alerta.php). Teléfono: 900.101.062 (Oficina de atención al ciudadano)

## **2.7. EVALUACIÓN**

Para comprobar que los objetivos planteados han sido alcanzados por el alumnado, el docente se basará en la observación, la ejecución de las actividades y la participación en las reflexiones en grupo.

Los criterios que deben contemplar en la evaluación son los siguientes:

Los/as alumnos/as saben:

- Cómo reconocer si se están haciendo pasar por ellos en Internet.
- Detectar una suplantación a través de cambios en los juegos online, usos anómalos de sus cuentas, desactivación o activación de algún servicio.

Los/las alumnos/as vivencian de forma experiencial:

- Cómo se siente una persona a la que han suplantado su identidad y lo exponen a los demás.

Los/as alumnos/as reflexionan:

- Sobre la importancia de dirigirse a un adulto responsable para comentar la posibilidad de que hayan sufrido una suplantación de identidad.

Los/as alumnos/as desarrollan:

- Confianza para denunciar y/o comunicar a un adulto una posible suplantación de identidad.

Los/as alumnos/as tienen pautas para actuar frente a una suplantación de identidad, saben que:

- Deben denunciar a un adulto.
- Es conveniente recopilar todas las pruebas y evidencias relacionadas con la suplantación.
- Deben cambiar todas las contraseñas que haya interceptado el suplantador.

## 2.8. DOCUMENTACIÓN DE APOYO

Los siguientes recursos son de utilidad para ampliar el conocimiento sobre la suplantación de identidad:

### Monográfico de suplantación de identidad

Marco teórico de referencia para sensibilizar sobre los riesgos de la suplantación de identidad y ofrecer pautas a padres, madres, tutores y educadores para su prevención entre los menores, así como mecanismos de actuación en caso de producirse.

Disponible en el portal de Chaval.es: <http://www.chaval.es>

### Curso en línea Seguridad TIC y Menores

Curso de 30 horas de duración bajo metodología **MOOC** (*Massive Online Open Course* - Curso en línea masivo y abierto-) dirigido a padres y educadores. Sensibiliza sobre los riesgos a los que se enfrentan los menores en el uso de Internet y las nuevas tecnologías, ofreciendo estrategias, pautas y recomendaciones para su prevención y respuesta en caso de producirse un incidente. Contiene un módulo exclusivo de suplantación de identidad.

Disponible en: <http://www.chaval.es>