I.E.S.
Ramón y Cajal

Tejiendo redes seguras

IES Ramón y Cajal

MODALIDAD A

Nivel 5 CoDiceTIC Excelente

Índice

Presentación

El IES Ramón y Cajal es un centro público, que depende de la Consejería de Educación de la Junta de Castilla y León, ubicado en el barrio de Las Delicias de la ciudad de Valladolid. Comenzó su andadura en el año 1980 como centro exclusivamente de Formación Profesional, pasando a ser con la promulgación de la LOGSE en 1990 Instituto de Educación Secundaria con el nombre, ya utilizado desde 1983, de Ramón y Cajal. El barrio de Las Delicias, el más populoso de Valladolid, cuenta con una población de más de 27.000 habitantes. Desde sus inicios, el barrio estuvo ligado a una población de base obrera, dado que sus orígenes están asociados a la llegada del ferrocarril a Valladolid en 1864 y la posterior construcción de los talleres centrales de reparación y mantenimiento de la Compañía del Norte, que llegaron a emplear a más de 2500 trabajadores a finales del siglo XIX, convirtiéndose estos trabajadores en los primeros habitantes de este barrio.

Desde entonces, Las Delicias ha albergado una mayoría de población trabajadora, aunque en los últimos años con la expansión del barrio hacia el norte y el este se ha constatado una mayor variedad social; también y desde los años 90 del pasado siglo se ha asistido al fenómeno de la llegada de un buen número de población inmigrante, que a día de hoy representa una incidencia más elevada que en el resto de la ciudad.

En el centro se imparten enseñanzas de Educación Secundaria Obligatoria (ESO), Bachillerato (BCH), Formación Profesional Básica (FPB), Ciclos Formativos de Grado Medio (CFGM) y de Grado Superior (CFGS) de las Familias Profesionales de Sanidad, Imagen Personal y Química. La diversidad educativa explica la diversificación en el alumnado en lo referente a edad, nacionalidad, inquietudes culturales y nivel socio-económico. El curso 23-24 cuenta con 1050 alumnos y 143 profesores, de los que 86 imparten enseñanzas de FP.

En los últimos años se viene desarrollando cada curso el denominado ""Proyecto integral de Centro", basado en la metodología ABP, que implica a todos los niveles educativos. De modo multidisciplinar, en los últimos cursos se ha trabajado en "El Callejero del Ramón y Cajal", "Cavando trincheras de paz" y "Sostenibilidad: sembrando el futuro"

El instituto ha obtenido el Certificado de Centro de Excelencia Profesional de FP de Alto Nivel, cuenta con Proyecto Erasmus, Sello de Vida Saludable y la calificación de Centro Educativo Sostenible. Ha obtenido un primer premio "Alianza STEAM, Niñas en Pie de Ciencia" 2023 y participa en varios programas Aula-Empresa. El curso 23-24 destacan Y tú ¿cómo lo haces? Aprendiendo de las Empresas y RYC Emprende: innova, crea y desarrolla el espíritu emprendedor.

Hemos de resaltar en este punto una realidad que desde los últimos años ha tenido y está teniendo una presencia cada vez mayor y más dramática; esto es, la crisis económica que afecta a un número cada vez mayor de las familias de nuestros alumnos. La precariedad laboral y el paro han provocado que esté aumentando alarmantemente el número de familias en riesgo de exclusión social. A pesar de ello, a mayoría de las familias se ocupan y preocupan por la educación que reciben sus hijos y responden positivamente cuando han de realizarse acciones que fomenten la estrategia digital del Centro, que cuenta con un nivel 5 Excelente de Certificación CoDice TIC. Para las familias, una buena educación debe combinar desarrollo personal, hábitos de conducta adecuados y resultados académicos satisfactorios, a lo que se ha de sumar la firme voluntad del Centro en aras a incentivar la motivación y el interés del alumnado, introduciendo en la metodología docente las TIC (pizarra digital, audiovisuales, ordenador, laboratorio de idiomas, Plan de Formación con itinerarios TIC específicos) y una progresiva digitalización.

Justificación

La utilización cada vez más frecuente de dispositivos electrónicos y redes por parte del alumnado, tanto en el Centro Educativo como fuera de él, tiene potenciales usos educativos pero también importantes riesgos. Se hace cada vez más urgente contemplar estos aspectos en nuestros planes educativos, y en especial en el Plan TIC, para que tanto alumnado como profesorado tome conciencia de la imprescindible necesidad de protección de la seguridad y la privacidad, máxime si nos encontramos ante menores.

La irrupción de las nuevas tecnologías en las aulas producida en los últimos años no ha tenido precedentes, lo que unido a la especial vulnerabilidad de los menores y el gran volumen de datos personales susceptible de tratamientos (8,1 millones de estudiantes no universitarios en España según datos del Ministerio de Educación), llevó a la Agencia Española de Protección de Datos a la realización de una inspección sectorial de oficio sobre servicios de cloud computing en el sector educativo en el año 2015.

En la referida inspección, esta Agencia detectó la utilización al margen de las plataformas educativas de los centros, de diversas aplicaciones informáticas instaladas generalmente en los dispositivos móviles del profesorado y alumnado donde se podían registrar datos de carácter personal, incluidas imágenes y calificaciones, y la utilización de servicios o herramientas de almacenamiento en nube de documentos y ficheros en general en los que compartir información entre el alumnado y el profesorado de forma habitual.

Del análisis de esta inspección y el Selfie realizado entre los meses de diciembre de 2022 y enero de 2023 a toda la Comunidad Educativa del IES Ramón y Cajal, se desprenden las siguientes medidas, acciones y buenas prácticas desarrolladas durante el curso 2023-2024, separadas para los cuatros bloques de aplicaciones que aparecen en el estudio y que nos servirán de punto de partida para nuestro Proyecto “Tejiendo redes seguras” junto con el Plan TIC.

1.- APPS MÓVILES

Existen multitud de Apps para el entorno educativo, instalables en dispositivos móviles tipo tableta o teléfono móvil inteligente, aunque la mayoría ofrecen también la posibilidad de utilización desde un ordenador personal con navegador de internet. El uso de estas aplicaciones supone en muchos casos el almacenamiento de datos personales, si bien normalmente limitados al nombre y apellidos de los alumnos.

Las aplicaciones utilizadas responden a una gran variedad, que se pueden clasificar en los siguientes tipos según su funcionalidad (se mencionan entre paréntesis algunas aplicaciones a modo de ejemplo):

1. Aplicaciones que implementan cuadernos de notas, agendas y organizador de clases para los docentes (IDOCEO, ADDITIO, TEACHER AIDE).
2. Aplicaciones puramente destinadas a ofrecer materiales didácticos atrayentes para el alumnado y de utilidad para el profesorado, de diferentes materias como matemáticas, ciencias, (DIDAKIDS), incluyendo gamificación (CLASSCRAFT, KAHOOT), etc.
3. Aplicaciones para la creación de hilos de discusión y debate, para compartir mapas mentales, conceptuales y esquemas (MINDOMO).
4. Aplicaciones para la elaboración de presentaciones (PREZI, TED).
5. Aplicaciones que facilitan la comunicación entre el profesorado, el alumnado y las familias.
6. Si bien esta funcionalidad se suele incorporar en las plataformas educativas, existen apps con esta finalidad exclusiva. También, dentro de este tipo de aplicaciones, señalar que se ha detectado la utilización de mensajería WHATSAPP en los entornos educativos.
7. Creación de vídeos (ANIMOTO, MOVIE MAKER). Edición de fotografías y vídeos (PicCOLLAGE)
8. Acceso a plataformas de

aprendizaje (MOODLE, LMS WORDPRESS…) para compartir recursos de estudio, trabajos en grupo...

2.- UTILIZACIÓN DE SISTEMAS DE ALMACENAMIENTO EN NUBE

Las herramientas de almacenamiento en nube más utilizadas son: DROPBOX, Google DRIVE, iCLOUD y para los docentes de la Consejería de Educación el OneDrive de Office 365.

Son utilizadas tanto por el profesorado como por el alumnado con la finalidad fundamental de compartir documentos, normalmente apuntes de clase y materiales didácticos en general, así como trabajos de los alumnos. En algunas ocasiones también se utilizan estas herramientas para almacenar datos personales tales como listas de asistencia, calificaciones, fotos y vídeos.

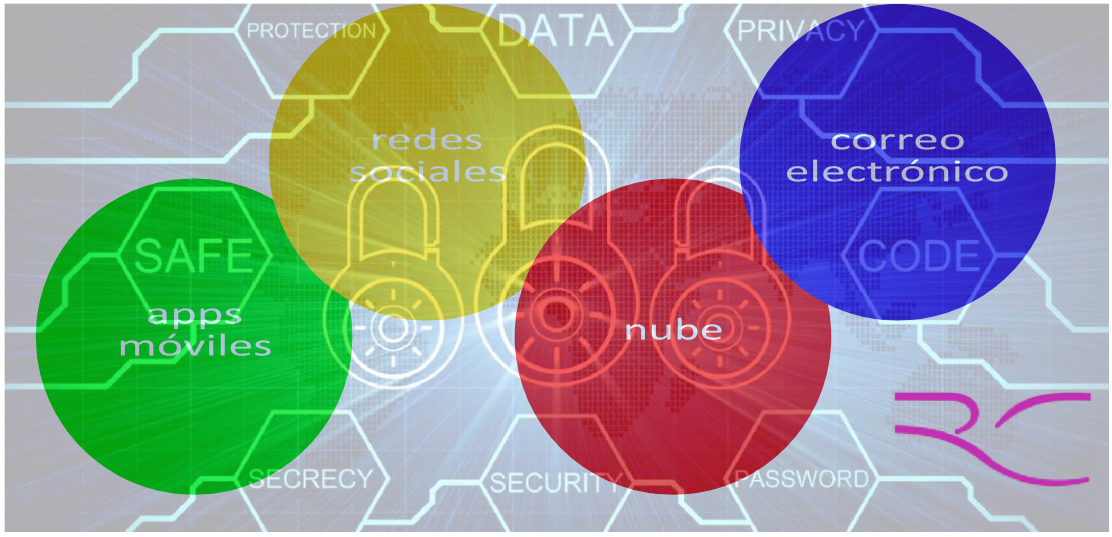
3.- UTILIZACIÓN DE REDES SOCIALES

La utilización de las redes sociales en los Centros educativos cada vez es más frecuente en los Centros. Twitter e Instagram son las más utilizadas y en menor medida Facebook. A estas hay que añadir nuevas plataformas como Tik-Tok.

Las suelen utilizar tanto el profesorado como alumnado, fundamentalmente como canal de comunicación y como medio de compartir información (fotos, información de eventos, etc.) generando una mayor cohesión del alumnado pero incrementando los riesgos en internet y el compromiso de la privacidad.

4.- UTILIZACIÓN DE CORREOS ELECTRÓNICOS DISTINTOS DE LA MENSAJERÍA DE LA PLATAFORMA EDUCATIVA DEL CENTRO

El correo facilitado por la plataforma Educacyl no es el único sistema utilizado por los centros para comunicarse por mensajería, siendo utilizados otros correos electrónicos, mayoritariamente correos corporativos.



Marco normativo

La Comisión Europea puso en marcha en

marzo de 2010 «la Estrategia Europa 2020» que contiene, entre otras iniciativas, la creación de la Agenda Digital Europea cuya finalidad era conseguir que la Unión Europea fuera en 2020 una potencia tecnológica y digital, a la vez que se garantice la confianza y seguridad en el uso de las tecnologías de la información y la comunicación.

Dentro de este marco europeo, el Consejo de Ministros de 15 de febrero de 2013, aprobó la creación de la Agenda Digital para España con más de 100 líneas de actuación estructuradas en torno a seis grandes objetivos, uno de los cuales consiste en reforzar la confianza en el ámbito digital. La Ley Orgánica 8/2013, de 9 de diciembre, para la mejora de la calidad educativa indica en su preámbulo que "las tecnologías de la información y la comunicación serán una pieza fundamental para producir el cambio metodológico que lleve a conseguir el objetivo de mejora de la calidad educativa". Asimismo, establece que "el uso responsable y ordenado de estas nuevas tecnologías por parte del alumnado debe estar presente en todo el sistema educativo y serán una herramienta clave en la formación del profesorado y en el aprendizaje de los ciudadanos a lo largo de la vida, al permitirles compatibilizar la formación con las obligaciones personales o laborales, así como también en la gestión de los procesos".

En este sentido, la Consejería de Educación de la Junta de Castilla y León consideró de especial importancia impulsar el desarrollo de las tecnologías de la información y la comunicación en el ámbito educativo de forma segura y responsable. A tal efecto, la Dirección General de Innovación Educativa y Formación del Profesorado, mediante Resolución de 17 de octubre de 2014, puso en marcha con carácter experimental, en el curso 2014-15, el proyecto denominado «Plan de Seguridad y Confianza Digital en el ámbito educativo», como elemento de coordinación, información, difusión y promoción del uso seguro de internet por parte de los miembros de la comunidad educativa. Como consecuencia del éxito de dicho proyecto se publicó la ORDEN EDU/834/2015, de 2 de octubre, por la que se regula el proyecto denominado «Plan de Seguridad y Confianza Digital en el ámbito educativo» en la Comunidad de Castilla y León.

Del posterior Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 la Junta de Castilla y León publica un documento denominado: " Consentimiento informado tratamiento de imágenes/voz de alumnos en centros de titularidad pública" en el que se informa y recaba el consentimiento del alumnado como base jurídica que permitirá a los centros el tratamiento de voz/imágenes del alumnado.

En otro orden de cosas, el Informe emitido el 01/06/2022 por la Comisión Evaluadora para la concesión del CoDice TIC planteaba como propuesta de mejora en el apartado 3.2.8 ÁREA 8 - SEGURIDAD Y CONFIANZA DIGITAL:

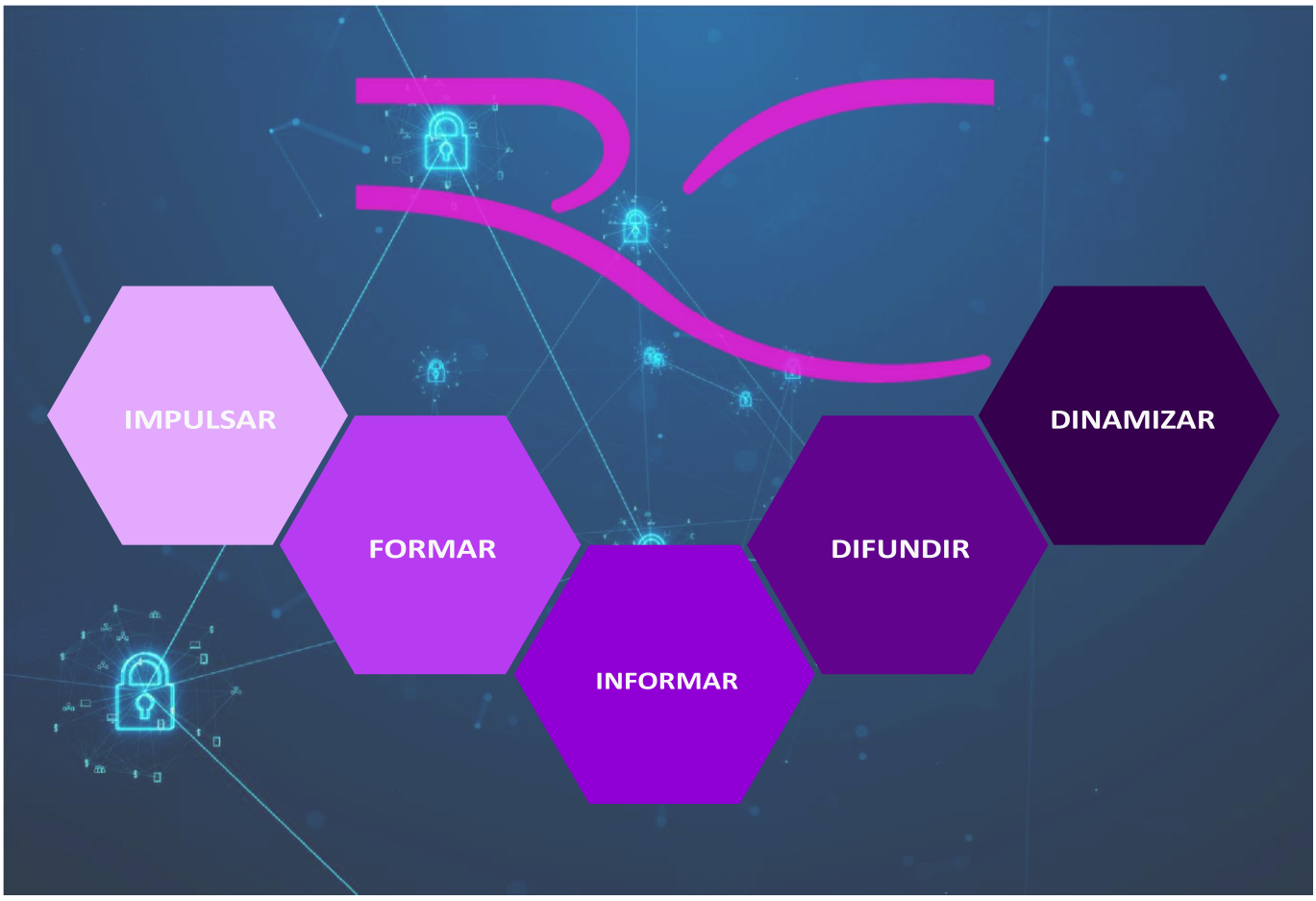
- Definir procedimientos para informar, concienciar e integrar en el proceso educativo criterios sobre la propiedad intelectual, derechos de autor y propiedad industrial.
- Planificar formación sobre la seguridad y la confianza digital para toda la comunidad educativa.

Todo esto nos impulsó a plantear “Tejiendo redes seguras” en nuestro Centro, cuya finalidad es fomentar el uso seguro, crítico y responsable de las tecnologías de la información y la comunicación entre todos los miembros de la comunidad educativa, en especial en el alumnado menor de edad, desarrollando acciones y buenas prácticas con las que se pretende impulsar una educación de calidad (ODS número 4) incorporando los derechos a la educación digital y el derecho a la protección de datos en el sistema educativo español en sus etapas no universitarias.

Objetivos

Este plan tiene como destinatarios todos los integrantes de la Comunidad Educativa: alumnado, profesorado y familias del centro educativo. El Proyecto “Tejiendo redes seguras” del IES Ramón y Cajal pretende:

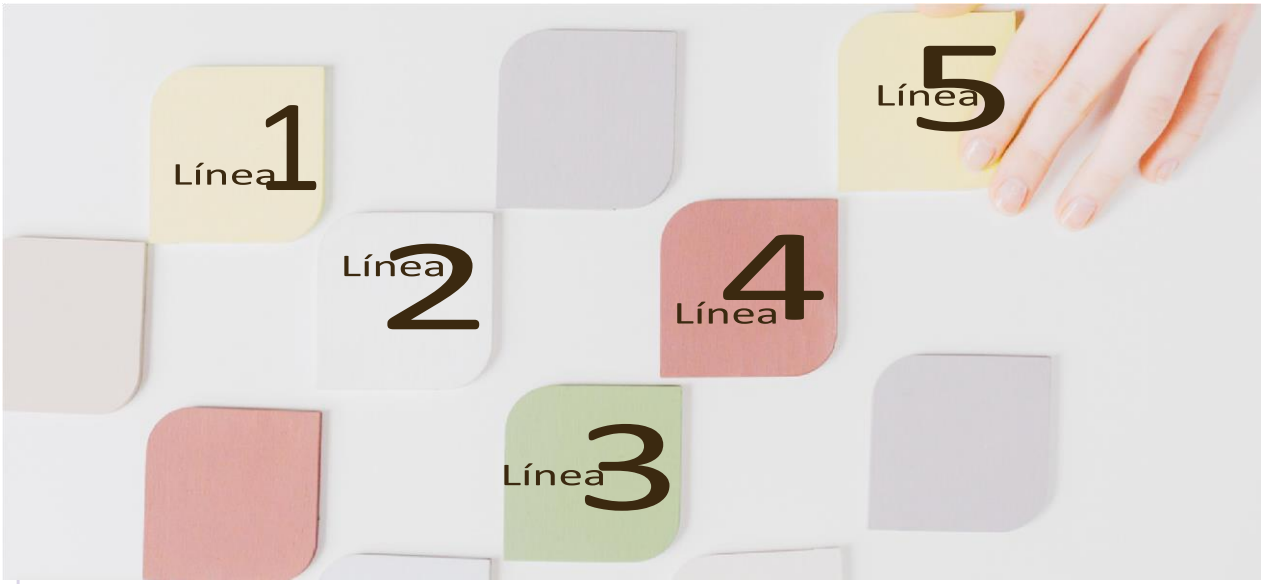
1. Impulsar el uso seguro del entorno digital a todos los miembros de la comunidad educativa, especialmente a los menores edad.
2. Comunicar, sensibilizar y formar sobre las situaciones de riesgo más habituales a las que nos enfrentamos al navegar por la red, en especial entre los menores.
3. Informar y ayudar en relación con situaciones no deseadas, usurpaciones de identidad, comportamientos inadecuados, contenidos inapropiados o ilegales, así como cualquier otra situación incómoda encontrada en la red.
4. Promocionar y difundir el buen uso de las TIC en la educación mediante la organización de cursos, talleres, encuentros, jornadas, etc.
5. Dinamizar el uso seguro de las TIC en el Instituto.



Líneas de Actuación

Las líneas que vertebran este Plan de actuaciones son:

- **Línea 1:** Potenciación del entorno virtual del centro a través de la Red Escuelas Conectadas favoreciendo la navegación segura gracias a las cuentas personales de Educacyl y el DOMINIO propio del Centro gestionado por una empresa externa.
- **Línea 2:** Confección de materiales específicos sobre seguridad y confianza digital.
- **Línea 3:** Elaboración de protocolos en relación con situaciones de usurpaciones de identidad en la red, conductas inadecuadas y/o contenidos inapropiados o ilícitos.
- **Línea 4:** Realización de actividades de formación, talleres, jornadas y encuentros sobre la protección de datos personales, privacidad, seguridad y bienestar digital para todos los miembros de la Comunidad Educativa.
- **Línea 5:** Fomento y realización de iniciativas encaminadas al uso correcto de las TIC en el Instituto a través de la participación en eventos que promuevan el uso seguro y responsable de internet entre la Comunidad Educativa (Día de Internet Segura 7 de Febrero).



Línea de Actuación 1: Dominio propio del Centro. Potenciación del entorno virtual del centro a través de la Red Escuelas Conectadas

1.1 Actuaciones:

1.1.1 Conexión y configuración a la Red de Escuelas Conectadas

El objeto de esta actuación es el de explicar de manera rápida y sencilla la interacción con la solución Wi-Fi recientemente desplegada en el Instituto perteneciente al conjunto de centros que forman el proyecto de Escuelas Conectadas llevado a cabo en la comunidad de Castilla y León. Este proyecto, que cuenta con financiación del Fondo Europeo de Desarrollo Regional (FEDER), dando un paso más hacia la incorporación generalizada de las Tecnologías de la Información y la Comunicación al sistema Educativo, consiste en dotar de conectividad a internet mediante redes de banda ancha ultrarrápida y la implantación de una red inalámbrica a los centros docentes públicos no universitarios.

A través de los puntos de acceso (AP) desplegados por el centro gracias al proyecto, se hacen disponibles distintas redes Wi-Fi, con distintos SSID (identificadores), para distintos propósitos y con distintos permisos.

La solución proporciona acceso diferenciado para personal docente, personal de administración, navegación general (pe: alumnos) e invitados.

Estas redes Wi-Fi guardan similitud con la arquitectura de las redes cableadas de la VPN educativa en propósito y orientación a cada usuario según su perfil. Las redes estarán disponibles tanto para equipos portátiles como para cualquier equipo con interfaz Wi-Fi, garantizando una correcta conectividad y los estándares más altos de seguridad y privacidad.Aunque, por seguridad, desde las redes Wi-Fi no se da acceso, de momento, a muchos recursos cableados del centro, pues sólo accederán aquellos dispositivos con interfaz Wi-Fi a las redes de la presente solución.

Para conectarse a cada red Wi-Fi, los usuarios deberán utilizar sus credenciales en la red educativa de la JCyL: esto es, el **nombre de usuario y clave** que utiliza para acceso a los servicios educativos, como el portal educativo de la Junta de Castilla y León:
(https://www.educa.jcyl.es/es).

Deberán conectar con la red correspondiente a su perfil:

- **Perfil general:** Pensado para el alumnado, aunque tendrán acceso todos los usuarios generales de la red educativa de la JCyL (profesorado, familias…), se dispone de la red visible, la cual permite navegación general, acceso a dispositivos comunes (paneles, pizarras, proyectores) según la configuración de estos en la red y la convivencia en red de todos estos usuarios.
- **Perfil Docente:** Pensado para el profesorado, red oculta que hay añadir manualmente, la cual permite navegación general, supervisión de la actividad en los dispositivos de los alumnos y acceso a dispositivos comunes e impresoras según la configuración de estos en la red.
- **Perfil Administración:** Pensado para el equipo directivo y personal de administración, red oculta que hay añadir manualmente, la cual permite navegación general y acceso a dispositivos comunes e impresoras del Centro según la configuración de estos en la red.
- **Perfil Invitados:** Pensada para usuarios que no formen parte de la comunidad educativa de Castilla y León (pe: ponentes de charlas, personal municipal adscrito al centro…) red oculta que hay añadir manualmente, la cual, por petición del equipo directivo por el canal que se proveerá permitirá la navegación y uso de recursos según credenciales dadas, durante tiempo y alcance solicitado, según proceda.

1.1.3 Conexión y configuración a los ordenadores de los Equipos informáticos de las Aulas de Informática y aula de idiomas del centro

El centro dispone de tres aulas de informática y con un laboratorio de idiomas que cuenta con ordenadores. Este aula se puede utilizar como aula de informática cuando no está asignado para la docencia de idiomas (inglés, francés o alemán).

Es esencial que tanto el profesorado como el alumnado se responsabilice del correcto uso de estas aulas, por el bien de todos. Jamás se debe dejar al alumnado desatendidos durante la clase, y al final de la misma, el/la profesor/a debe ser el/la último/a en abandonar el aula.

A todo el alumnado se les activa también su cuenta personal para uso de los ordenadores del centro en las aulas de informática. El acceso y configuración del equipo que utilicen precisa introducir el usuario y contraseña. El usuario deberá cambiar la contraseña en su primer inicio de sesión. Es importante que lean con detenimiento las instrucciones en pantalla y se debe insistir en que no pierdan la contraseña. En todas estas aulas existen unas normas de uso que se encuentran sobre la mesa.

Línea de Actuación 2: Confección de materiales específicos sobre seguridad y confianza digital

Los Centros Educativos deben observar la debida diligencia con el tratamiento de los datos personales a los que tenga acceso el Centro, incluyendo aquellos obtenidos como consecuencia de la llegada de las tecnologías a las aulas y velar por que se reúnan las garantías para el cumplimiento de lo dispuesto en la normativa de protección de datos. Según el Reglamento General de Protección de Datos, la información ofrecida deberá ser concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en especial la dirigida a los menores.

Debe guardarse especial cuidado con los tratamientos de datos personales que sean facilitados por terceros sin mediación del titular de los datos, y en concreto, con la publicación de fotografías o vídeos de alumnos facilitados por otros alumnos o profesores.

Las aplicaciones educativas, que pueden ser de gran utilidad para el aprendizaje así como para la organización de las aulas, deben estar incluidas en la política de seguridad de los centros educativos. El profesorado deberá solicitar, previamente a su utilización, la autorización del centro.

Los tratamientos de datos personales mediante Apps deben de incluirse en la política de seguridad con las mismas garantías que cualquier otro tratamiento. El centro debe informar a los padres o tutores del comienzo de la utilización de la tecnología en las aulas, así como de las Apps que traten datos personales de los alumnos y su funcionalidad.

Algunas aplicaciones utilizadas no ofrecen la suficiente información para poder valorar su adecuación a la normativa. Por ejemplo, en materia de seguridad, sobre la ubicación de los datos, el periodo de retención de los mismos y/o los responsables de su tratamiento. En ocasiones no incluyen información ni tan siquiera sobre las finalidades del tratamiento, detectándose importante falta de transparencia y la posibilidad de prácticas de retención de datos opacas.

Dadas las funcionalidades que ofrecen estas aplicaciones y la tipología de los datos que tratan, los tratamientos efectuados podrían incluir la elaboración de perfiles de aprendizaje, preferencias o comportamiento de menores de edad, por parte de la Comisión TIC del centro.

Desde el Centro se promoverá el uso únicamente de aplicaciones que ofrezcan información claramente definida sobre los tratamientos efectuados, sus finalidades y responsables, así como sobre la ubicación de los datos, el periodo de retención, y las garantías con relación a su seguridad.

El profesorado deberá solicitar la autorización del Centro para el uso de estas aplicaciones. Una solicitud de autorización conllevará la evaluación de la aplicación desde el punto de vista de la seguridad de la información y la consiguiente autorización o denegación por parte del Centro.

Las aplicaciones que se utilicen deben permitir el control, por parte de los tutores o profesores, de los contenidos subidos por los menores, en especial de los contenidos multimedia (fotos, vídeos y grabaciones de voz de los alumnos).

En particular, se considera que el usuario y las familias deben ser informadas de la utilización de sistemas de almacenamiento en nube.

Por eso deben establecerse programas informativos de concienciación orientados hacia la protección de los datos personales, dirigidos a profesores y alumnos, sobre la importancia del uso correcto de aplicaciones. **Como norma general tanto el profesorado como el alumnado deberán utilizar las aplicaciones del Office 365 al que toda cuenta de Educacyl tiene acceso.**

2.1 Actuaciones:

2.1.1. Orientaciones prácticas sobre seguridad y confianza digital

El profesorado y el alumnado deben tener especial cuidado al publicar imágenes y vídeos mediante Apps y herramientas en nube para no poner en riesgo la intimidad de otras personas. Se recomienda leer la información sobre el servicio (política de privacidad y condiciones de uso) antes de empezar a utilizarlo. Al utilizar redes sociales se recomienda configurar las opciones de privacidad en el perfil de usuario para permitir el acceso a la información publicada a un grupo conocido y previamente definido de usuarios.

- Al facilitar datos en cualquier ámbito (en cualquier tipo de aplicación, en el registro de usuarios, en los contenidos) evitar incorporar datos del domicilio de los menores y otros datos personales que puedan poner en peligro su seguridad. Debe recomendarse no atender la demanda que puedan tener las aplicaciones para recabar datos personales, que pueda llevar al tratamiento excesivo de datos. Las contraseñas deben ser robustas, con suficientes caracteres y compuestas por mayúsculas, minúsculas, números y caracteres especiales, evitando las que sean fáciles de adivinar por otras personas. No se deben de facilitar nunca a otras personas.

- Al utilizar sistemas de almacenamiento de documentos en nube tipo Dropbox, iCloud o Google Drive, se debe evitar incluir datos personales sensibles, tales como datos relativos a la salud, contraseñas, datos bancarios, material audiovisual de contenido sensible, etc.

- En el marco de la utilización de este tipo de herramientas se recomienda la lectura de la guía de cloud publicada por la Agencia Española de Protección de Datos, accesible en el código QR que se encuentra a pie de esta página.

- Primará la utilización de las plataformas educativas que tiene nuestro centro y que permiten la interacción entre el alumnado, y entre este y el profesorado, sin menoscabo de poder establecer mecanismos de comunicación adicionales.

- Para los casos de tratamientos especiales de datos personales que puedan suponer un mayor riesgo, tal como el reconocimiento facial de menores de edad, que implica el tratamiento de datos biométricos, el/la responsable debe obtener el consentimiento expreso de los alumnos (si son mayores de 14 años) o de los padres o tutores (si son menores de 14 años) para aplicar dicho tratamiento a las imágenes con fines de identificación, y asegurarse que esta tecnología se utiliza únicamente para fines concretos especificados y legítimos.

El responsable de estas actuaciones será la Comisión TIC del Centro que contará con la colaboración del Equipo Directivo y con el apoyo de la/el responsable de Formación del Centro.

Agencia Española de Protección de Datos (AEPD)

La AEPD pone a nuestra disposición en su web materiales y distintas iniciativas relacionadas con la educación y los menores.

https://www.aepd.es/es/documento/guia-cloud-clientes.pdf

https://www.tudecideseninternet.es/es

- *2.1.2. Páginas sobre seguridad y confianza digital*

Línea 2

Pantallas amigas

Es una iniciativa por la promoción del uso seguro y saludable de las nuevas tecnologías en la infancia y adolescencia.

https://www.pantallasamigas.net

2.1.3. Creación de material sobre seguridad y confianza digital con el alumnado de Tecnologías de la Información y la Comunicación de Bachillerato

Uno de los objetivos curriculares de Bachillerato es permitir a este alumnado desarrollar los estándares de aprendizaje correspondiente: "Usar los sistemas informáticos y de comunicaciones de forma segura, responsable y respetuosa, protegiendo la identidad online y la privacidad, reconociendo contenido, contactos o conductas inapropiadas y sabiendo cómo informar al respecto".

Para ello se utilizarán diferentes aplicaciones del paquete office 365 y aplicaciones como Canva, Genially para la elaboración de videos, infografías, carteles que resultan atractivos en la difusión de esta información.

Línea de Actuación 3: Elaboración de protocolos en relación con situaciones de usurpaciones de identidad en la red, conductas inadecuadas y/o contenidos inapropiados o ilícitos.

En relación con la suplantación de identidad en Internet en España, el 78% de la población se muestra muy o bastante preocupada por la misma. Si bien es cierto que se vincula sobre todo a delitos económicos como usurpación de la tarjeta de crédito o la cuenta bancaria.

En los últimos seis años las estafas denunciadas con tarjetas de crédito, débito y cheques de viaje han aumentado a un ritmo anual del 34,3% y las estafas bancarias a un ritmo del 14,4%. En 2019, éramos el país de la Unión Europea con más casos de robo de identidad en la red. Aquí llegaron a estimarse en 1.600 millones de euros las pérdidas como consecuencia de este delito en 2017.

Los delincuentes cibernéticos siguen imparables, buscando y encontrando maneras "creativas" de robar nuestros datos para cometer graves delitos. No obstante, pese a estar expuestos a esta amenaza y –en algunos casos- no poder evitar su ejecución, si podemos detectar, denunciar y minimizar sus efectos.

La suplantación de la identidad en Internet ocurre cuando alguien se apropia indebidamente de una identidad digital ajena. Quienes se dedican al robo o falsificación de identidades en la red aprovechan cualquier vulnerabilidad en los sistemas de seguridad informáticos. De esta manera, acceden a datos personales de los afectados para cometer delitos como estafas, fraudes y extorsión.

El cyberbulling y el grooming o acoso sexual de menores por Internet son lamentablemente comunes y muy frecuentes en la actualidad. Existe suplantación de identidad cuando un individuo crea una cuenta de email o perfil en redes sociales con los datos de otro. Ya sea una persona o empresa. En este caso, el propósito es hacerse pasar por la víctima y actuar en su nombre. Esta circunstancia es muy grave, porque el atacante puede cometer chantajes y otros delitos, así como publicar contenidos atribuibles al afectado para desprestigiarle. Desgraciadamente cada vez más frecuente en el ámbito escolar. Las consecuencias de la suplantación de identidad en redes sociales, páginas web falsas y posibles pérdida de prestigio es la posibilidad de que abran cuentas en redes sociales y/o el robo de contraseñas de acceso a éstas, con tu identidad. Solucionar la pérdida de prestigio que ocasiona este delito es con frecuencia muy complejo.

Los medios utilizados por los ciberdelincuentes para tener acceso a la información personal de sus víctimas son diversos. Algunos de ellos son:

- Mediante el acceso a las cuentas de las personas mediante técnicas de phishing y malware o lanzando ataques cibernéticos más sofisticados, difíciles de detectar. Estos pueden ser individuales o masivos.
- Mediante el envío de publicidad engañosa, con anuncios de ofertas y premios falsos, para solicitar datos de cuentas bancarias o de tarjetas de crédito, número telefónico, dirección, etc. Mediante la sustracción de información durante transacciones mediante redes Wi-Fi no seguras.
- Mediante el robo de equipos informáticos o dispositivos móviles de los usuarios.

Por desgracia, muchas de las formas de detectar la suplantación de identidad en Internet se manifiestan cuando ésta ya ha ocurrido.

Cuando se dispone de cuentas oficiales, como puede ser la cuenta de Educacyl, detectada la publicación sospechosa en el momento se puede tomar acciones inmediatas, como advertir a tus contactos y a la misma red social sobre la situación. Incluso puede bloquear la cuenta mientras se realizan las investigaciones adecuadas.

Por el contrario, si no se hace un seguimiento de dichas cuentas en redes sociales y publicaciones web, se corre graves riesgos. Entre estos, el de un ciberatacante, creando perfiles no autorizados. De ese modo, el delincuente tendrá la ventaja de publicar contenidos ficticios y hasta de estafar a usuarios.

3.1 Recomendaciones para prevenir la suplantación de identidad en internet:

Algunas de las recomendaciones para prevenir la suplantación de identidad:

- No dejar el DNI original o fotocopia en manos de terceros y fuera de nuestra vista.
- Asegurarse de que no se deja al alcance de cualquiera.
- En redes sociales, configurar la privacidad de vuestros perfiles lo máximo posible.
- Para las contraseñas, usar combinaciones alfanuméricas robustas (y no fechas o datos que puedan obtenerse con algo de ingeniería social).
- Revisar siempre la política de privacidad y las condiciones del servicio al que se vaya a acceder.
- Cuando se navegue por Internet, especialmente en sitios de compras, asegurarse de que la dirección empieza por HTTPS://, lo que indica que se trata de un sitio seguro.
- Evitar conectarse a Wi-Fi públicas.
- No compartir datos sensibles de forma abierta en Internet.
- No dejar el móvil o el ordenador con las cuentas abiertas desatendidos.
- Sospechar de correos con direcciones desconocidas o extrañas, que pidan entrar en algún enlace para solucionar algún problema con una de nuestras cuentas o que lleven archivos adjuntos, lo más seguro es que estéis ante un caso de phising.
- No compartir fotos o vídeos comprometedores. Los ciberdelincuentes buscan este tipo de contenidos, para después extorsionan a las víctimas bajo la excusa de que si no hacen lo que se les pide, harán público el vídeo.

3.2 Procedimiento para denunciar la suplantación de identidad en internet

Sin importar lo que puedan tardar las investigaciones, si se ha sido víctima de suplantación de identidad en Internet se debe denunciar ante las autoridades competentes. En España, este delito es tipificado como de "usurpación de identidad" en el Código Penal (Artículo 401). Por ejemplo: si la suplantación está vinculada con la estafa, el o los perpetradores pueden enfrentarse a penas de hasta cuatro años de prisión. Esto dependerá de la cantidad defraudada. Asimismo, quien incurra en usurpación para atentar contra el honor o revelar secretos personales de la víctima, podría pasar de seis meses a tres años en la cárcel.

3.2.1. Procedimiento

1. En primer lugar, reunir toda la evidencia posible: capturas de pantalla, URLs, comentarios de contactos, notificaciones. Se recogerán los estados de cuentas y facturas, si es un caso de fraude o estafa. Incluso, es aconsejable contactar con personas que estén dispuestas a declarar como testigos. Si está a tu alcance busca asesoramiento legal especializado.
2. Con las evidencias ya mencionadas, dirigirse al Grupo de Delitos Telemáticos de la Guardia Civil (GDT). También se puede recurrir a la Brigada Central de Investigación Tecnológica de la Policía Nacional. Ambos organismos están facultados para investigar y perseguir estos delitos en el ámbito nacional y fuera de nuestras fronteras. y presenta la denuncia.
3. Aparte de eso, notificar el hecho y presentar pruebas ante la Agencia Española de Protección de Datos.
4. Reclamar ante las Juntas Arbitrales de Consumo.
5. Poner una demanda ante la Oficina de Atención al Usuario de Telecomunicaciones.
6. Recurrir a los Tribunales de Justicia.

7. Pedir la cancelación de tus datos en caso de que te hayan incluido en un fichero de morosidad.

3.2.2. INCIBE. 017.

"Tu Ayuda en Ciberseguridad" es el servicio nacional, gratuito y confidencial que INCIBE pone a disposición de los usuarios de Internet y la tecnología con el objetivo de ayudarles a resolver los problemas de ciberseguridad que puedan surgir en su día a día. Está dirigido a los ciudadanos (usuarios de Internet en general) y menores y su entorno (padres, educadores y profesionales que trabajen en el ámbito del menor o la protección online ligada a este público).

El servicio es atendido por un equipo multidisciplinar de expertos, a través de las diferentes opciones de contacto, que ofrecen asesoramiento técnico, psicosocial y legal, **en horario de 8 de la mañana a 11 de la noche, los 365 días del año.**
https://www.incibe.es/linea-de-ayuda-en-ciberseguridad#formulario

https://www.incibe.es/linea-de-ayuda-en-ciberseguridad#linea

https://www.incibe.es/linea-de-ayuda-en-ciberseguridad#mensajeria

- ### *3.2.3. Páginas sobre situaciones de usurpaciones de identidad en la red, conductas inadecuadas y/o contenidos inapropiados o ilícitos.*

La Escuela de las Redes Sociales (School of Social Networks)

Es una iniciativa europea que pretende preparar a los menores para acceder a las redes sociales teniendo en cuenta los peligros a los que se exponen. En su web se proporcionan recursos para familias y centros educativos.

https://www.is4k.es .

CiberBulling

Es un proyecto de Pantallas amigas que pretende proporcionar información y recursos para identificar y prevenir las conductas de ciberacoso.

https://www.ciberbullying.com/

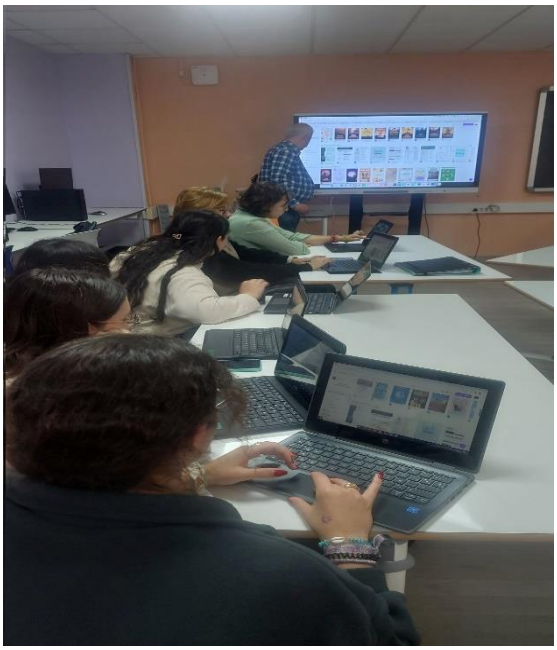
3.3 Creación de material sobre situaciones de usurpaciones de identidad en la red, conductas inadecuadas y/o contenidos inapropiados o ilícitos con el alumnado de Tecnologías de la Información y la Comunicación de Bachillerato

Uno de los objetivos curriculares de Bachillerato, como indicábamos en el apartado 2.1.3. de este documento, es permitir a este alumnado desarrollar los estándares de aprendizaje correspondiente:

"Usar los sistemas informáticos y de comunicaciones de forma segura, responsable y respetuosa, protegiendo la identidad online y la privacidad, reconociendo contenido, contactos o conductas inapropiadas y sabiendo cómo informar al respecto".

Para ello se utilizarán diferentes aplicaciones del paquete office 365 y aplicaciones como Canva, Genially para la elaboración de videos, infografías, carteles,...que resultan atractivos en la difusión de esta información.

...



016 hay salida

Línea de Actuación 4: Realización de actividades de formación, talleres, jornadas y encuentros sobre la protección de datos personales, privacidad, seguridad y bienestar digital dirigidas a todos los miembros de la Comunidad Educativa.

4.1 Formación para el profesorado

(Resolución de 4 de mayo de 2022, de la Dirección General de Evaluación y Cooperación Territorial, por la que se publica el Acuerdo de la Conferencia Sectorial de Educación, sobre la actualización del marco de referencia de la competencia digital docente).

El acuerdo de 30 de marzo de 2022, de la Conferencia Sectorial de Educación sobre la actualización del marco de referencia de la competencia digital docente establece que las tecnologías digitales son actualmente indispensables en los entornos laborales, sociales, económicos, deportivos, artísticos, culturales, científicos y académicos; han pasado a formar parte de nuestras vidas y a transformarlas. En el contexto educativo, hay que contemplar su presencia desde una doble perspectiva. Por una parte, como objeto mismo de aprendizaje, en la medida en la que, junto con la lectoescritura y el cálculo, forman parte de la alfabetización básica de toda la ciudadanía en las etapas educativas obligatorias y de educación de adultos y constituyen un elemento esencial de la capacitación académica y profesional en las enseñanzas postobligatorias. Por otra, los docentes y el alumnado han de emplearlas como medios o herramientas para desarrollar cualquier otro tipo de aprendizaje.

Este doble objetivo queda reflejado en el artículo 2 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, modificada por la Ley Orgánica 3/2020, de 29 de diciembre, en el que se fijan los fines del sistema educativo, y en los artículos correspondientes a las distintas enseñanzas en relación con los principios pedagógicos y el desarrollo curricular, así como en lo concerniente a la formación del profesorado y a la organización de los centros, aspectos contemplados, respectivamente, en los artículos 102 sobre formación permanente, 111 bis sobre las tecnologías de la información y la comunicación y 121 sobre el proyecto educativo.

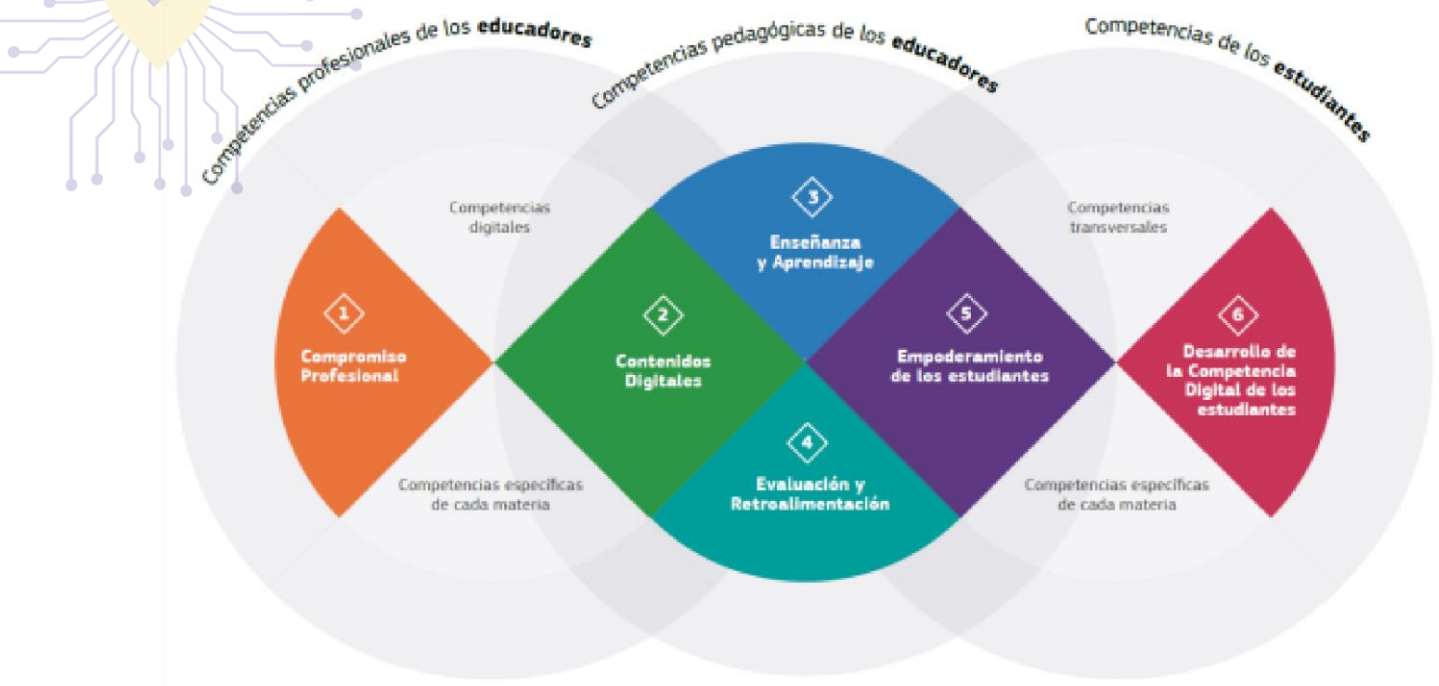
De forma específica, el marco que se recoge en este documento responde a lo establecido en el punto 6 del artículo 111 bis y supone la actualización y renovación del que fue acordado en la Conferencia Sectorial de Educación del 14 de mayo de 2020 y publicado mediante Resolución del 2 de julio de la Dirección General de Evaluación y Cooperación Territorial en BOE de 13 de julio de 2020. No obstante, a pesar de su reciente publicación, el rápido cambio experimentado por las tecnologías digitales y la aceleración en la extensión de su uso a consecuencia de la pandemia generada por el SARS-CoV-2 han hecho necesaria una profunda revisión.

En esta revisión, el marco se ha alineado con las propuestas autonómicas, estatales y europeas sobre competencias digitales con el objetivo de incorporar el conocimiento y la experiencia adquiridos durante los últimos años y facilitar la convergencia en la creación de un Espacio Europeo de Educación en 2025.

Esta disposición aprueba en el ámbito de sus competencias, la actualización del marco de referencia de la competencia digital docente desarrollada en el anexo I, atendiendo a lo establecido en el tercer punto del acuerdo suscrito por la Conferencia Sectorial de Educación en la reunión del 14 de mayo de 2020.

Este ANEXO I establece el marco de referencia de la competencia digital docente por áreas, competencias, etapas, niveles e indicadores de logro y ejemplificación a través de afirmaciones sobre el desempeño correspondiente al nivel de cada competencia. Las áreas son:

Área 1. Compromiso profesional



Área 2. Contenidos digitales
Área 3. Enseñanza y aprendizaje
Área 4. Evaluación y retroalimentación
Área 5. Empoderamiento del alumnado
Área 6. Desarrollo de la competencia digital del alumnado

Para el desarrollo de estas competencias se ha desarrollado a través del Plan Bianual de Formación del Profesorado del IES Ramón y Cajal un conjunto de actividades (Cursos, Seminarios y Grupos de Trabajo) dentro del itinerario “Mejora multidisciplinar de la actividad docente”

En concreto hemos centrado la actuación de este Proyecto especialmente en el área 1 apartado 1.5. **Protección de datos personales, privacidad, seguridad y bienestar digital del Marco de Referencia de la Competencia Digital Docente**. Esta nueva competencia, que no estaba presente ni en el DigCompEdu 2017 ni en el S4T 2021 procede de un desarrollo independiente de la competencia 2.3 del DigcompEdu 2017, en la que se trataban tanto cuestiones relacionadas con la protección de los derechos de propiedad intelectual como aspectos relacionados con la protección de datos, la privacidad y derechos digitales. En este sentido, conviene remarcar que, aunque esta cuestión concierne, ante todo, a las Administraciones Educativas y a los titulares de los centros privados, es importante que el profesorado conozca estos riesgos y aplique de forma responsable los protocolos del centro y sepa cuáles son los criterios utilizados para determinar si un recurso o tecnología puede o no ser empleado.
Pretendemos desarrollar los siguientes niveles de progresión:

A1. Conocimiento general de medidas para proteger los datos personales, la privacidad, la seguridad, los derechos digitales y el bienestar al utilizar las tecnologías digitales en contextos educativos.

A2. Conocimiento y aplicación, de forma

guiada, de las medidas de protección de los datos personales y la privacidad, así como de las de seguridad y salvaguarda de los derechos digitales y el bienestar al utilizar las tecnologías digitales en contextos educativos reales.

B1. Uso sistemático y autónomo de las medidas establecidas para proteger los datos personales y la privacidad, así como las medidas de seguridad y salvaguarda de los derechos digitales y el bienestar al utilizar las tecnologías digitales en el centro educativo.

B2. Colaboración en la evaluación de los planes y protocolos del centro relacionados con la protección de datos personales, la privacidad, la seguridad, los derechos digitales y el bienestar al utilizar las tecnologías digitales.

C1. Identificación de riesgos y concreción de medidas para la protección de datos, la privacidad y los derechos digitales y para la seguridad en el centro educativo y colaboración en el diseño de las actuaciones para lograr una convivencia positiva en relación con el uso de las tecnologías digitales.

C2. Convertirse en un referente en el diseño y aplicación de protocolos o medidas de seguridad, protección de datos personales, privacidad, derechos digitales y bienestar relacionados con la utilización de las tecnologías digitales en el ámbito educativo.

4.1.1. Actividades de formación para el profesorado

- Inclusión en el Plan de Formación del Profesado del Centro de una línea de actuación que desarrolle el área 1 apartado 1.5. Protección de datos personales, privacidad, seguridad y bienestar digital del Marco de Referencia de la Competencia Digital Docente.

- Organización de una semana de formación bajo el lema:*" Protección de datos personales, privacidad, seguridad y bienestar digital. Derecho o deber".* Esta semana se organizará conjuntamente con talleres, encuentros y charlas dirigidas al alumnado y la AMPA.

- Difusión de todas aquellas jornadas, cursos... relacionadas con la línea 4 de este Proyecto, que se organicen a través del correo diario de centro y cuyo responsable será el Responsable de Formación del Centro.

4.2 Formación para el alumnado

En esta actuación el Plan se centra en el área 6 apartado 6.4. Uso responsable y bienestar digital del Marco de Referencia de la Competencia Digital Docente. Esta nueva competencia procede de un desarrollo independiente de la competencia 2.3 del DigcompEdu 2017, en la que se trataban tanto cuestiones relacionadas con la protección de los derechos de propiedad intelectual como aspectos relacionados con la protección de datos, la privacidad y derechos digitales. En este sentido, conviene remarcar que, aunque esta cuestión concierne, ante todo, a las Administraciones Educativas y a los titulares de los centros privados, es importante que el profesorado conozca estos riesgos y aplique de forma responsable los protocolos del centro y sepa cuáles son los criterios utilizados para determinar si un recurso o tecnología puede o no ser empleado.

Pretendemos desarrollar los siguientes niveles de progresión:

- A1. Conocimiento y comprensión de los aspectos implicados en la utilización responsable y saludable de las tecnologías digitales y de los criterios didácticos para que el alumnado adquiera hábitos de uso seguro y adopte decisiones reflexivas.
- A2. Aplicación de propuestas didácticas, de forma guiada, para el desarrollo de la competencia del alumnado en el uso responsable, seguro y sostenible de las tecnologías digitales y para garantizar su bienestar digital.
- B1. Integración de los aspectos curriculares relativos al desarrollo de la competencia digital del alumnado sobre el uso seguro, responsable, crítico, saludable y sostenible de las tecnologías digitales en los procesos de enseñanza y aprendizaje de forma autónoma competencia digital del alumnado en el uso responsable, seguro, crítico, saludable y sostenible de las tecnologías digitales.
- B2. Diseño y adaptación de las estrategias pedagógicas para potenciar el desarrollo de la competencia digital.
- C1. Coordinación o diseño de las actuaciones del centro para desarrollar la competencia digital del alumnado en el uso de las tecnologías digitales de forma segura, responsable, crítica, saludable y sostenible
- C2. Investigación e innovación sobre las prácticas de enseñanza y aprendizaje, de forma que se adapte a la continua evolución de los riesgos y de las tecnologías dirigidas al desarrollo de la competencia digital del alumnado en el uso de las dispositivos y servicios digitales de forma segura, responsable, crítica, saludable y sostenible.

4.2.1. Actividades de formación para el alumnado

Para conseguir el pleno desarrollo de estos niveles de progresión se han desarrollado una serie de *talleres* a lo largo de todo el curso escolar, con el fin de que al finalizar estas acciones formativas el alumnado fuese capaz de:

1. Identificar los riesgos potenciales derivados de la utilización de Internet.
2. Reconocer cuáles son los riesgos más habituales para la seguridad de nuestros datos e información personal cuando navegamos por la red.
3. Enumerar las diferentes medidas de protección existentes para proteger su privacidad en todo momento.
4. Determinar las medidas de seguridad que debemos establecer en nuestros dispositivos y comunicaciones cuando utilizamos internet.
5. Identificar correctamente los principales fraudes que podemos encontrarnos en la red.
6. Identificar eficazmente posibles supuestos de ciberdelincuencia y enumerar y describir las medidas para protegernos adecuadamente.

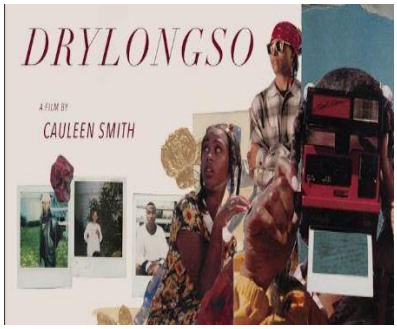
¿Qué actividades concretas hemos llevado a la práctica?

- Organización de una semana de formación bajo el lema:*" Protección de datos personales, privacidad, seguridad y bienestar digital. Derecho o deber".* Esta semana contó conjuntamente con talleres, encuentros y charlas dirigidas al profesorado y la AMPA.

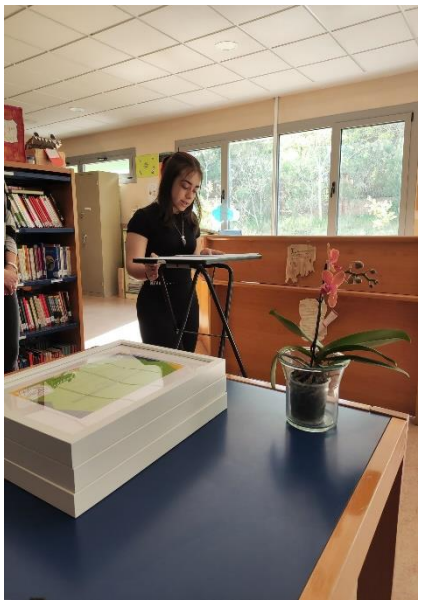
- Organización de talleres organizados por diferentes entidades como Cuerpo Nacional de Policía, Policía Municipal de Valladolid, organizaciones, asociaciones... relacionados con protección de datos personales, privacidad, seguridad y bienestar digital y que se incluyen en los Planes de centro propios del Departamento de Orientación, o en los que colabore como Plan de Acción Tutorial.

- Seminci Joven: Varios grupos del Centro acuden a las sesiones de la SEMINCI JOVEN. En concreto, la película "Las gentiles" aborda el tema de la privacidad en Instagram y las Redes sociales, además de las consecuencias nefastas que puede acarrear su abuso.

En el caso de los alumnos menores de edad, la película seleccionada fue Drylongso, historia creada a partir de imágenes Polaroid.



- **Certamen literario "Cuida tu privacidad":** Se ha realizado un concurso literario consistente en la composición de relatos, poemas y redacciones bajo la premisa de la protección de datos. Se celebró la lectura en público en la biblioteca del Centro de los textos ganadores, publicándose un dossier digital.


- **Desayúnate con respeto**: actividad realizada con 1º y 2º de la ESO. El objetivo a alcanzar era 0 apercibimientos por el uso indebido del móvil en clase. El aula ganadora obtuvo un desayuno saludable como premio, completado con dinámicas “cara a cara” con el fin de poner en valor la comunicación interpersonal.


- **Participación en la Liga Debate**: Todos los cursos los alumnos de Bachillerato participan en el diseño de argumentos a favor y en contra de un determinado tema, para posteriormente y por sorteo, proceder a su defensa. Este año, la Junta de Castilla y León puso sobre la mesa la Incidencia de la irrupción de la Inteligencia Artificial en la Educación, y nuestros alumnos basaron sus argumentaciones en su relación y vínculo con la seguridad digital y la necesaria preservación del Derecho a la intimidad.

- **Cinefórum sobre Seguridad Digital:** Durante diez sesiones se planteó el visionado de distintas películas sobre seguridad digital, en el salón de actos del Centro. La acogida fue excelente, con posterior debate y análisis de los riesgos presentes en la red y la importancia de la privacidad.

- **Hackaton de ideas emprendedoras FP Up:** actividad consistente en el diseño desde 0 de una empresa a partir de la premisa “Iniciativa emprendedora y protección de datos”. La idea ganadora resultó “DiviérteT sin pantallas”, una propuesta de ocio alternativo para los recreos y las extraescolares, fomentando además de modo simultáneo el desarrollo de las soft skills o habilidades blandas del alumnado a partir de la comunicación e interacción interpersonal.

- **Charla riesgos presentes en la Red:** Asistencia con alumnado de Bachillerato a la “Caja Negra de Crimen y Ficción”, charla sobre los posibles riesgos presentes en la Red y sus consecuencias.

4.3 Páginas sobre el uso seguro de internet. para todos los miembros de la Comunidad Educativa.

- **Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF)**

La web del INTEF contiene una colección de casi 400 materiales digitales sobre menores y seguridad digital, accesibles mediante un buscador que filtra según criterios de temática, público destinatario, etapa educativa, tipo de recurso, fuente y licencia de uso.

Uno saludable comohttps://intef.es/

- **Oficina de Seguridad del Internauta (OSI)**

En la web se pueden encontrar guías sobre distintos aspectos de la seguridad en Internet y recursos para niños, familia y educadores.

Oficina de Seguridad del Internauta

https://www.osi.es/es

- **Instituto Nacional de Ciberseguridad (INCIBE)**

Una de las iniciativas de esta organización es el Programa Cibercooperantes, con sesiones para centros educativos y otras actuaciones que promueven la concienciación y formación

https://www.incibe.es

4.4 Formación para las madres y padres del Centro

Conscientes del reto que supone educar en un entorno tan complejo, en continuo cambio, y en el que son mayoría los que se consideran inexpertos y poco habilidosos, el elaborar un itinerario de mediación parental facilitará la tarea de acompañamiento en la educación de los hijos en el uso seguro y responsable de la red.

Es preciso abordar estrategias y pautas que nos permitan avanzar en la acción educadora, tales como:

- Estrategias que ayuden en la supervisión, orientación y acompañamiento de los hijos en Internet, en especial a la hora de establecer límites y normas.
- Pautas de mediación parental en función de la edad del menor, con las que ir evolucionando en función de sus necesidades y madurez.
- Recomendaciones específicas sobre el uso de las tecnologías para comportarse de manera adecuada en línea, prevenir el acoso, gestionar de manera apropiada la privacidad y la identidad digital, y protegerse ante virus y fraudes.
- Formas de actuar en caso de producirse un incidente en Internet: ciberacoso, suplantación de identidad, filtración de imágenes comprometidas (sexting).

4.4.1. Actividades de formación para madres y padres de alumnos del Centro

Se ha organizado una semana de formación bajo el lema:*" Hablemos de la Protección de datos"* con talleres, encuentros y charlas dirigidas al profesorado y alumnado.

Se ha colaborado además con la AMPA en todos aquellos cursos, talleres, iniciativas que fomentan iniciativas en pro del uso seguro de internet de los menores y la protección de datos.

Además, se han realizado debates en la Radio del Instituto, RAYCA Radio, con el lema "La privacidad ¿Derecho o deber?

- *4.4.2. Páginas sobre el uso seguro y responsable de internet para madres y padres de la Comunidad Educativa.*

https://www.is4k.es/sites/default/files/contenidos/herramientas/is4k_guia_mediacion_parental_inter net.pdf

https://files.incibe.es/is4k/is4k_guia_controles_parentales.pdf

Línea de Actuación 5: Fomento y realización de iniciativas encaminadas al uso correcto de las TIC en el Instituto a través de la participación de eventos que promuevan el uso seguro y responsable de internet entre la Comunidad Educativa. Día de Internet Segura (7 de Febrero) y Día Mundial de Internet (17 de Mayo)

El Día de Internet Segura o Safer Internet Day (SID) es un evento internacional organizado por la red INSAFE/INHOPE de Centros de Seguridad en Internet en Europa, con el apoyo de la Comisión Europea.

A modo de curiosidad, el SID se celebra el segundo día de la segunda semana del segundo mes del año y reúne a millones de personas de todo el mundo para impulsar cambios positivos y concienciar acerca de la seguridad en Internet, organizando distintos eventos y actividades.

Este día no solo pretende la creación de una Internet más segura, sino una Internet mejor, a través del uso responsable, respetuoso, crítico y creativo que todos hagamos.

El SID se dirige a todos los públicos: niños y jóvenes; padres, tutores, profesores, educadores y trabajadores sociales; así como las empresas, organismos y responsables políticos, animándoles a participar de forma activa en la creación juntos de una Internet mejor.

Desde el Instituto Nacional de Ciberseguridad (INCIBE), propone que nos unamos a la iniciativa internacional y celebrar el #DíaDeInternetSegura con actividades para fomentar, entre niños, jóvenes y sus entornos más cercanos, un uso seguro y positivo de las tecnologías digitales, promocionando sus competencias en esta materia y ayudándoles a ser respetuosos, críticos y creativos, en línea con los principios digitales europeos.

Para ello, desde el INCIBE se han realizado, en colaboración con el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), tres talleres online interactivos, que han tenido lugar el pasado 7 de febrero, con el objetivo de ayudar al alumnado a desarrollar sus competencias digitales para aprender a realizar un uso seguro y responsable de Internet. Estos talleres están disponibles en la web del INTEF.

Nos hemos sumado al desarrollo de talleres que se organizan desde la Consejería de Educación Otra de las actuaciones para hacer llegar la información a los centros, familias y alumnado recogida en el portal Educacyl.

https://www.educa.jcyl.es/plandeseguridad/es/materiales/propuesta-talleres-centros-familiasalumnado

Se ha diseñado una línea formativa especial dedicada a la "Educación mixta y a distancia" con el objetivo de informar y formar a las familias sobre las herramientas, estrategias y actuaciones necesarias para ayudar a sus hijos en este nuevo modelo de educación híbrida. Además de conocer su funcionamiento, también lo consideramos como un elemento necesario para comunicación con el centro, con los tutores de sus hijos e incluso para comunicación entre las mismas familias.

Para la planificación, organización y desarrollo de este plan de formación se han tenido en cuenta las peticiones de las familias a través de las Federaciones, AMPA y desde los equipos directivos y tutores de los centros.

También se han diseñados talleres relacionados con el PSCD, haciendo especial incidencia en los meses de febrero y mayo, en los que se celebra: el Día Internacional de Internet Seguro (Safer Internet Day) y el Día Mundial de Internet.

Temáticas de formación - las principales líneas que se han programado son:

1. Formación para una educación mixta y a distancia:
2. Formación inicial y básica en el conocimiento y principales aplicaciones y utilidades para la educación de las herramientas educativas institucionales de Office 365 (OneDrive, Teams, paquete básico de Office), aulas virtuales Moodle, así como en las características de una educación mixta (metodologías, sistemas de comunicación con familias y alumnos, organización y gestión del tiempo y las tareas…)
3. Formación sobre los contenidos y secciones del Portal de educación (Educacyl).
4. Formación en temas seguridad e identidad digital del PSCD:
   - Confianza digital y prevención del ciberacoso.
   - Prevención de adicciones sin sustancia y el juego on line.

5.1 Actuaciones:

5.1.1. Realización a través de un concurso de vídeos de corta duración relacionados con la información, difusión y promoción del uso seguro de Internet en los centros educativos, seguridad, privacidad, confidencialidad e identidad digital.

El Plan de seguridad y confianza digital en el ámbito educativo de la Consejería de Educación contempla entre sus actuaciones la realización y exposición de vídeos de corta duración relacionados con la información, difusión y promoción del uso seguro de Internet en los centros educativos, seguridad, privacidad, confidencialidad e identidad digital.

Desde la Comisión TIC se planteará un concurso para animar al alumnado a la presentación anual de dicho Certamen

5.1.2. Creación de material sobre la información, difusión y promoción del uso seguro de Internet en los centros educativos

Se ha convocado un concurso para el diseño de infografías, flyer y post para Instagram que permitiera:

- Identificar los riesgos potenciales derivados de la utilización de Internet.
- Reconocer cuáles son los riesgos más habituales para la seguridad de nuestros datos e información personal cuando navegamos por la red.
- Determinar las medidas de seguridad que debemos establecer en nuestros dispositivos y comunicaciones cuando utilizamos internet.

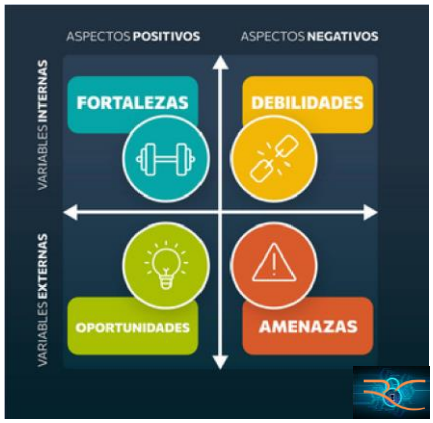
5.1.3. Páginas sobre el uso seguro de internet. y responsable

Recursos para trabajar en el aula

Descubre todos los recursos pedagógicos que tenemos a tu disposición en IS4K para que puedas trabajar y concienciar a los más jóvenes en el uso...

6.Seguimiento y Evaluación

El seguimiento y evaluación del Proyecto “Tejiendo redes seguras” permitirá comprobar el desarrollo de las actuaciones previstas e intervenir en su revisión siempre que sea necesario para conseguir los objetivos establecidos, proponiendo además nuevas buenas prácticas. El método utilizado para esta evaluación y seguimiento será el Método DAFO.



DAFO es el acrónimo de Debilidades, Amenazas, Fortalezas y Oportunidades. Gracias al análisis de cada una de estas 4 variantes, tendrás un análisis completo de la situación del proyecto.

Este análisis, resulta tremendamente útil a la hora de:

- Conocer cuáles son sus debilidades del plan e intentar mejorarlas.
- Descubrir sus fortalezas, potenciarlas y centrar los esfuerzos de comunicación y difusión en resaltarlas.
- Conocer qué oportunidades de crecimiento ofrece el plan en función del momento de desarrollo.
- Anticiparse a las posibles amenazas para estar prevenidos y tener un plan de actuación para evitar sus posibles efectos negativos

Las acciones de seguimiento incluyen:

- Recopilación, tratamiento y análisis de la información relativa al sistema de indicadores.
- Realización de una memoria anual de seguimiento del plan, así como de la memoria de evaluación final del mismo.
- Elaboración de las propuestas de modificación de las actuaciones a desarrollar en el marco temporal del plan que se consideren necesarias.
- Coordinación con otros organismos públicos, entidades y asociaciones que puedan participar en la ejecución y desarrollo del plan.
- Modificación y reorientación, en caso necesario, de los planteamientos y medidas a partir de las propuestas desarrolladas.

Para la evaluación del Proyecto “Tejiendo redes seguras” hemos utilizado una serie de indicadores. Los indicadores constituyen la principal fuente de información en los procesos de seguimiento y evaluación. A través de ellos se constata qué se ha realizado, cómo se ha realizado y cuáles son los resultados e impactos que se están generando. Los indicadores del Proyecto se encuentran asociados a los objetivos y a las líneas de actuación. La medición de los indicadores y su seguimiento se hará anualmente, y se combinarán mediciones cuatrimestrales para los indicadores que así lo permitan, y mediciones acumulativas para todos los indicadores.

6.1 Responsable del Proyecto.

El responsable del proyecto será la Comisión TIC que contará con la colaboración del Equipo Directivo y con el apoyo del responsable de Formación del Centro.

I.E.S.
Ramón y Cajal

EVALUACIÓN DE INDICADORES DE CONSECUCIÓN DEL PROYECTO "TEJIENDO REDES SEGURAS"

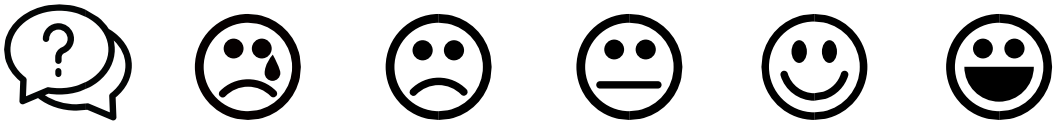
Profesorado

Edad:

Sexo: VH

Considera que se ha impulsado el uso seguro del entorno digital entre el profesorado de la comunidad educativa.

Considera que se ha comunicado y sensibilizado sobre las situaciones de riesgo más habituales al navegar por la red.



Considera que se ha formado sobre las situaciones de riesgo más habituales al navegar por la red .

Considera que se ha informado en relación a situaciones no deseadas, usurpaciones de identidad, comportamientos inadecuados, contenidos inapropiados o ilegales, así como cualquier otra situación incómoda encontrada en la red.

Considera que se ha ayudado, si ha sido necesario, en relación a situaciones no deseadas, usurpaciones de identidad, comportamientos inadecuados, contenidos inapropiados o ilegales, así como cualquier otra situación incómoda encontrada en la red.

Junta de Castilla y León
Consejería de Educación
GOBIERNO DE ESPAÑA MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

EVALUACIÓN DE INDICADORES DE CONSECUCIÓN DEL PROYECTO "TEJIENDO REDES SEGURAS"

Profesorado

Considera que se ha promocionado y difundido el buen uso de las TIC en el centro mediante la organización de cursos, talleres, encuentros, jornadas, etc.

El número de cursos, talleres, encuentros, jornadas, etc. organizados por el centro se considera adecuado

Considera que se ha dinamizado el uso seguro de las TIC en el Instituto

Considera que se ha informado suficientemente sobre las situaciones de riesgo más habituales al navegar por la red

Considera que se ha formado suficientemente sobre las situaciones de riesgo más habituales al navegar por la red

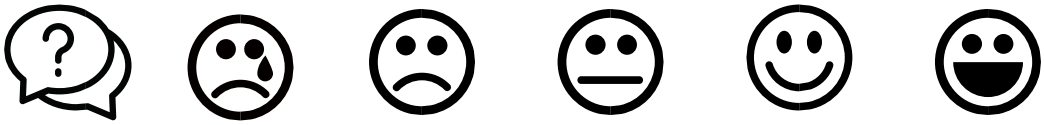
Profesorado

Considera que la configuración a la Red de Escuelas Conectadas desde su dispositivo (móvil, tablet,...) ha sido ...

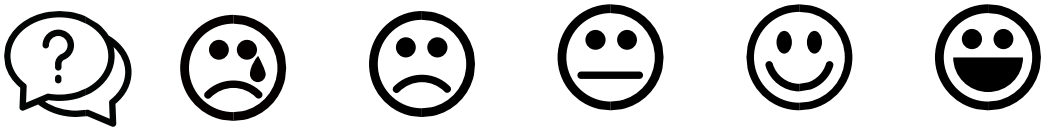
EVALUACIÓN DE INDICADORES DE CONSECUCIÓN DEL PROYECTO "TEJIENDO REDES SEGURAS"

Considera que se la conexión a la Red de Escuelas Conectadas desde su dispositivo (móvil, tablet,...) ha sido ...

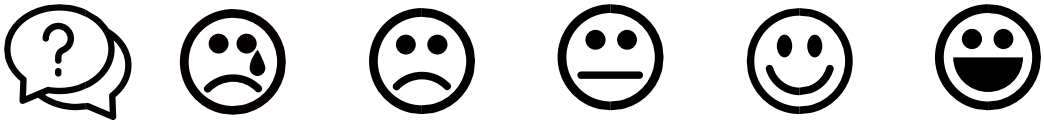
Considera que la configuración a la Red DOMINIO del centro desde su dispositivo (móvil, tablet,...) ha sido ...



Considera que la conexión a la Red DOMINIO del centro desde su dispositivo (móvil, tablet,...) ha sido ...



Considera que la configuración a los ordenadores de los Equipos informáticos de las Aulas de Informática y aula de idiomas del centro ha sido ...



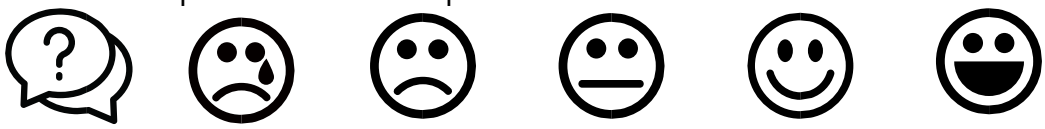
Profesorado

El material elaborado sobre seguridad y confianza digital con el alumnado en la materia de "Tecnologías de la Información y la Comunicación" de Bachillerato lo considera:

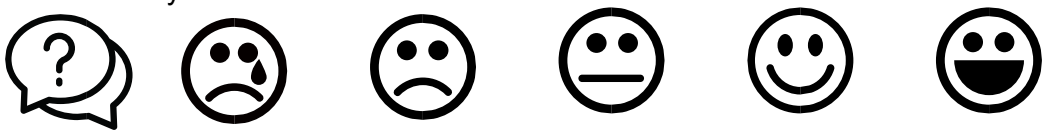
Las recomendaciones para prevenir la suplantación de identidad en internet las considera:

EVALUACIÓN DE INDICADORES DE CONSECUCIÓN DEL PROYECTO "TEJIENDO REDES SEGURAS"

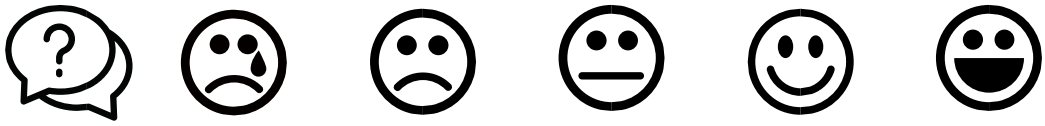
Los procedimiento para denunciar la suplantación de identidad en internet las considera:



El material que se ha creado sobre situaciones de usurpaciones de identidad en la red, conductas inadecuadas y/o contenidos inapropiados o ilícitos. con el alumnado en la materia de "Tecnologías de la Información y la Comunicación" de Bachillerato lo considera:



Las actividades de formación para el profesorado relacionadas con este Plan las considera:



El número de actividades de formación para el profesorado relacionadas con este Plan las considera:

EVALUACIÓN DE INDICADORES DE CONSECUCIÓN DEL PROYECTO "TEJIENDO REDES SEGURAS"

Considera que el concurso de vídeos de corta duración relacionados con la información, difusión y promoción del uso seguro de Internet en los centros educativos, seguridad, privacidad, confidencialidad e identidad digital ha sido ...

El material elaborado sobre la información, difusión y promoción del uso seguro de Internet en los centros educativos lo considero

Si quiere hacer alguna consideración en relación al objetivo que pretende promocionar y difundir el buen uso de las TIC en la educación mediante la organización de cursos, talleres, encuentros, jornadas…Si su respuesta es Si, por favor descríbalo a continuación:

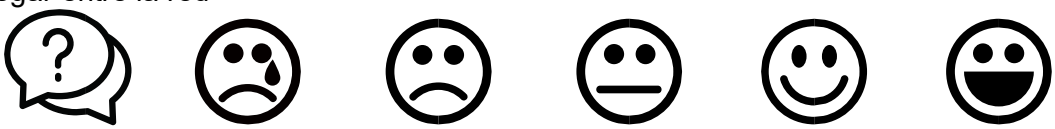
Alumnado

EVALUACIÓN DE INDICADORES DE CONSECUCIÓN DEL PLAN DE SEGURIDAD DIGITAL (P.S.D.)

Edad:
Sexo: VH

Considera que se ha impulsado el uso seguro del entorno digital entre el alumnado de la comunidad educativa.

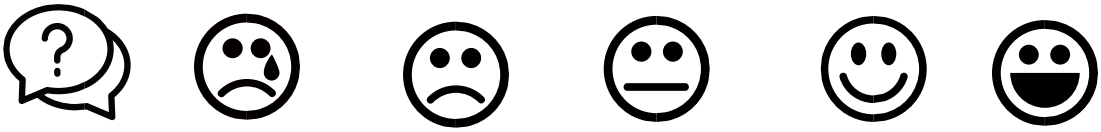
Considera que se ha comunicado y sensibilizado sobre las situaciones de riesgo más habituales al navegar entre la red



Considera que se ha formado sobre las situaciones de riesgo más habituales al navegar entre la red.

Considera que se ha informado suficientemente en relación a situaciones no deseadas, usurpaciones de identidad, comportamientos inadecuados, contenidos inapropiados o ilegales, así como cualquier otra situación incómoda encontrada en la red.

Considera que se ha ayudado, si ha sido necesario, en relación a situaciones no deseadas, usurpaciones de identidad, comportamientos inadecuados, contenidos inapropiados o ilegales, así como cualquier otra situación incómoda encontrada en la red.

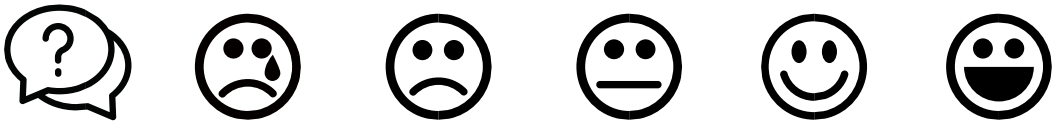


Alumnado

EVALUACIÓN DE INDICADORES DE CONSECUCIÓN DEL PROYECTO "TEJIENDO REDES SEGURAS"

Considera que se ha promocionado y difundido el buen uso de las TIC en el centro mediante la organización de cursos, talleres, encuentros, jornadas, etc.

El número de cursos, talleres, encuentros, jornadas, etc. organizados por el centro se considera adecuado

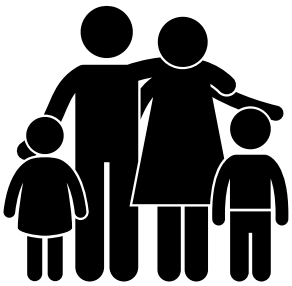


Considera que se ha dinamizado el uso seguro de las TIC en el Instituto

Considera que se ha informado suficientemente sobre las situaciones de riesgo más habituales al navegar por la red

Considera que se ha formado suficientemente sobre las situaciones de riesgo más habituales al navegar por la red

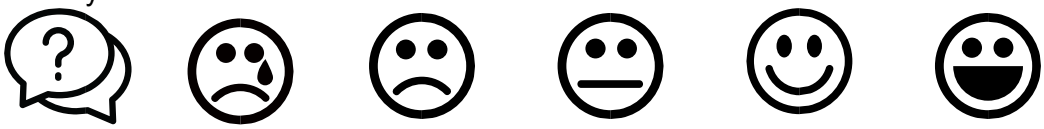
La configuración a la Red de Escuelas Conectadas desde su dispositivo (móvil, Tablet) ha sido



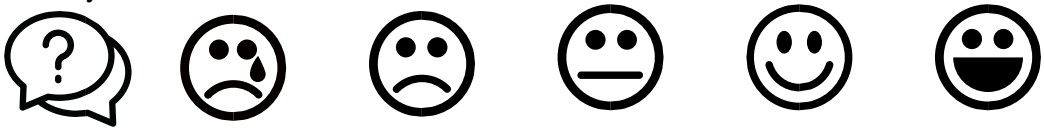
EVALUACIÓN DE INDICADORES DE CONSECUCIÓN DEL PROYECTO "TEJIENDO REDES SEGURAS"

La conexión a la Red de Escuelas Conectadas desde su dispositivo (móvil, tablet,...) ha sido ...

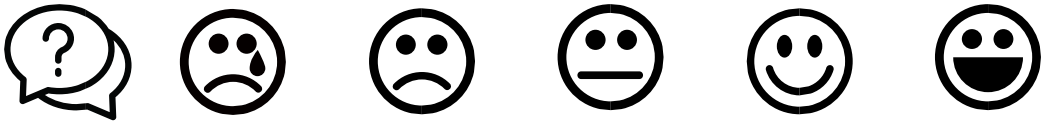
Considera que la configuración a los ordenadores de los Equipos informáticos de las Aulas de Informática y aula de idiomas del centro ha sido ...



Considera que se la conexión a los ordenadores de los Equipos informáticos de las Aulas de Informática y aula de idiomas del centro ha sido ....

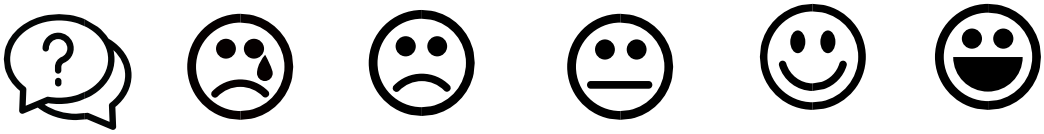


Considera que las recomendaciones para prevenir la suplantación de identidad en internet son:



Considera que el concurso de vídeos de corta duración relacionados con la información, difusión y promoción del uso seguro de Internet en los centros educativos, seguridad, privacidad, confidencialidad e identidad digital ha sido:

Considera que los procedimientos para denunciar la suplantación de identidad en internet son:



EVALUACIÓN DE INDICADORES DE CONSECUCIÓN DEL PROYECTO "TEJIENDO REDES SEGURAS"

Considera que el material elaborado sobre la información, difusión y promoción del uso seguro de Internet en los centros educativos ha sido:

Familias

Edad:
Sexo: VH

Considera que se ha impulsado el uso seguro del entorno digital entre las madres y padres de la comunidad educativa.

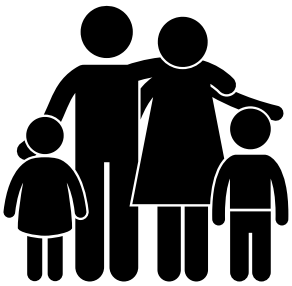
Considera que se ha comunicado y sensibilizado sobre las situaciones de riesgo más habituales al navegar por la red .

Considera que se ha formado sobre las situaciones de riesgo más habituales al navegar por la red.

Si quiere añadir alguna consideración no contemplada en los apartados anteriores, hágalo aquí

_____

_____



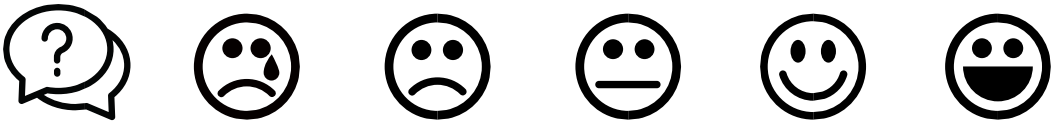
EVALUACIÓN DE INDICADORES DE CONSECUCIÓN DEL PROYECTO "TEJIENDO REDES SEGURAS"

Considera que se ha ayudado, si ha sido necesario, en relación a situaciones no deseadas, usurpaciones de identidad, comportamientos inadecuados, contenidos inapropiados o ilegales, así como cualquier otra situación incómoda encontrada en la red.

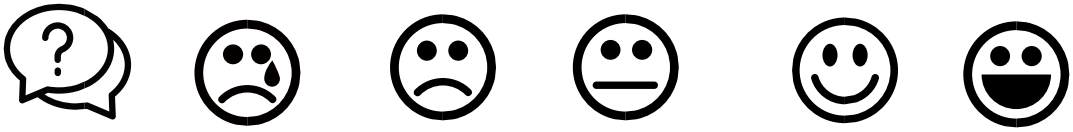
Considera que se ha informado en relación a situaciones no deseadas, usurpaciones de identidad, comportamientos inadecuados, contenidos inapropiados o ilegales, así como cualquier otra situación incómoda encontrada en la red.

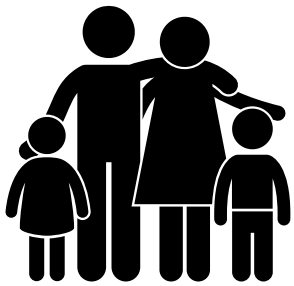
Considera que se ha promocionado y difundido el buen uso de las TIC en el centro mediante la organización de cursos, talleres, encuentros, jornadas, etc.

Considera que el número de cursos, talleres, encuentros, jornadas, etc. organizados por el centro ha sido el adecuado



Considera que se ha dinamizado el uso seguro de las TIC en el Instituto





EVALUACIÓN DE INDICADORES DE CONSECUCIÓN DEL PROYECTO "TEJIENDO REDES SEGURAS"

Considera que las recomendaciones para prevenir la suplantación de identidad en internet han sido:

Considera que se ha informado suficientemente sobre las situaciones de riesgo más habituales al navegar por la red

Considera que el concurso de vídeos de corta duración relacionados con la información, difusión y promoción del uso seguro de Internet en los centros educativos, seguridad, privacidad, confidencialidad e identidad digital ha sido:

Considera que el material elaborado sobre la información, difusión y promoción del uso seguro de Internet en los centros educativos ha sido ...

Puede añadir cualquier consideración que considere oportuna si no ha sido contemplada en los apartados anteriores

_____

_____

WEBGRAFÍA

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2018).*GUÍA para clientes que contraten servicios de Computing Cloud* desde https://www.aepd.es/es/documento/guia-cloud-clientes.pdf

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2023).*GUÍA para clientes que contraten servicios de Computing Cloud* desde https://www.tudecideseninternet.es/es

- EDUCACYL (2023). PLAN DE SEGURIDAD YC ONFIANZA DIGITAL. *Propuesta de talleres para centros, familias y alumnado* desde https://www.educa.jcyl.es/plandeseguridad/es/materiales/propuesta-tallerescentros-familias-alumnado

- INSTITUTO NACIONAL DE CIBERSEGURIDAD (2023) desde https://www.incibe.es

- INSTITUTO NACIONAL DE TECNOLOGÍAS EDUCATIVAS Y DE FORMACIÓN DEL PROFESORADO (2023) desde https://intef.es/

- INTERNET SEGURA FOR KIDS (2023) desde https://www.is4k.es/

- INTERNET SEGURA FOR KIDS (2023). *Catálogo de recursos para trabajar en el aula* desde https://www.is4k.es

- INTERNET SEGURA FOR KIDS (2014) . *Guía de control parenteral* desde https://www.is4k.es/sites/default/files/contenidos/herramientas/is4k_guia_mediacion_parental_internet.pdf

- INTERNET SEGURA FOR KIDS (2017) . *Guía para el uso seguro y responsable de internet por los menores, Itinerario de mediación parenteral* desde https://www.is4k.es/sites/default/files/contenidos/herramientas/is4k_guia_mediacion_parental_internet.pdf

- OFICINA DE SEGURIDAD DEL INTERNAUTA (2023) desde https://www.osi.es/es

- PANTALLAS AMIGAS (2023) desde https://www.pantallasamigas.net

- PANTALLAS AMIGAS (2023) desde https://www.ciberbullying.com/