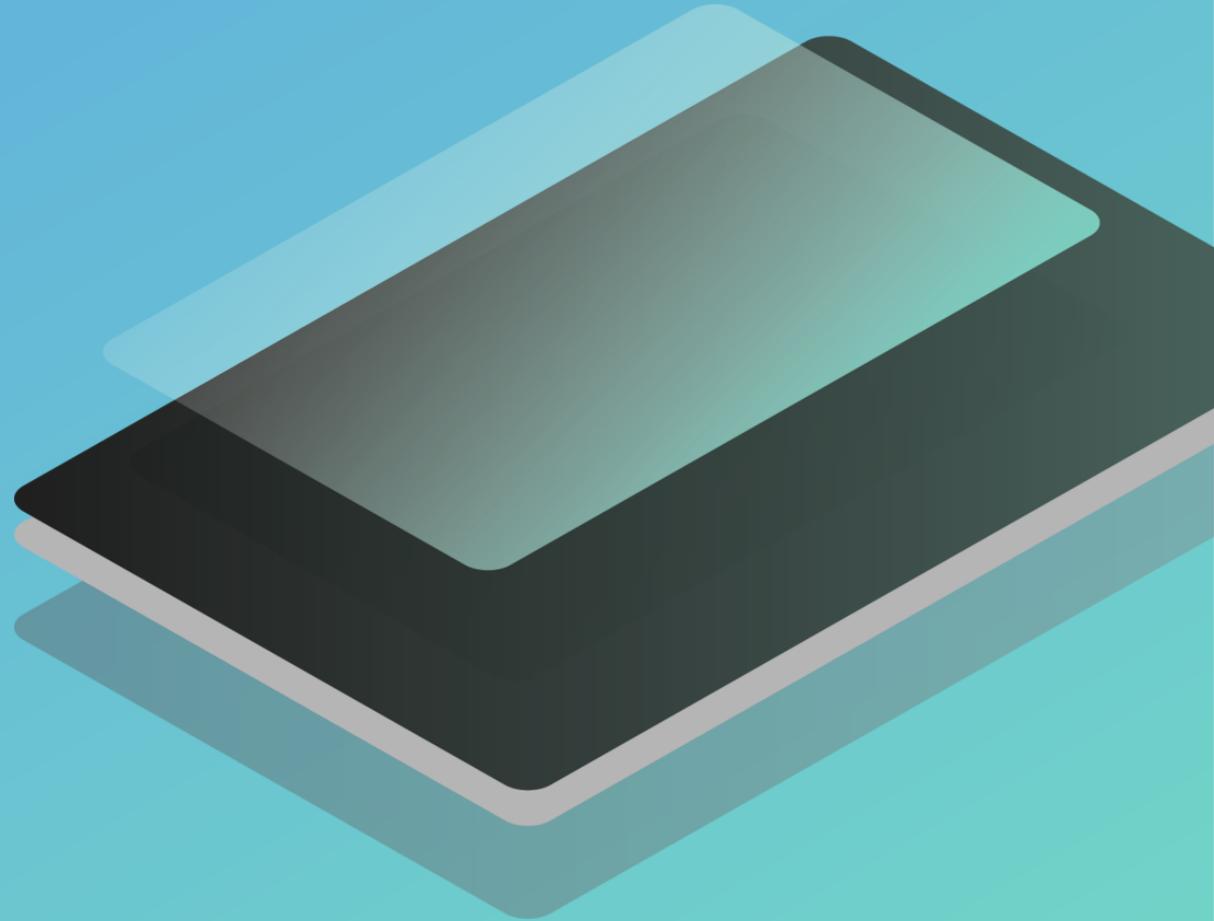




Seguridad y confianza digital

Escuela Oficial de Idiomas de Palencia

 Carlos Oliveros López



Índice

01 Marco normativo

02 Competencia digital

03 Información y alfabetización
informativa

04 Comunicación y colaboración

05 Creación de contenidos digitales

06 Resolución de problemas

07 Seguridad

08 Actividad



Marco normativo

Marco normativo

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



Artículo 1. Objeto y finalidad.

1. El objeto de la presente orden es regular el proyecto denominado «Plan de Seguridad y Confianza Digital en el ámbito educativo» en la Comunidad de Castilla y León.

2. La finalidad de este proyecto es fomentar el uso seguro, crítico y responsable de las tecnologías de la información y la comunicación (en adelante, TIC) entre todos los miembros de la comunidad educativa, en especial en el alumnado.

Artículo 2. Objetivos del proyecto.

Este proyecto pretende lograr los siguientes objetivos:

- a) Impulsar la alfabetización digital de todos los miembros de la comunidad educativa.
- b) Formar sobre el uso seguro de internet, especialmente a los menores.
- c) Informar y sensibilizar sobre las situaciones de riesgo más habituales a las que deben hacer frente los menores cuando navegan por internet.
- d) Elaborar planes básicos de seguridad por edades.
- e) Ofrecer información y ayuda en relación con situaciones no deseadas, usurpaciones de identidad, comportamientos inadecuados, contenidos inapropiados o ilegales, así como cualquier otra situación incómoda encontrada en internet.
- f) Promocionar y difundir el buen uso de las TIC en la educación mediante la organización de cursos, talleres, encuentros, jornadas, etc.
- g) Dinamizar el uso seguro de las TIC en los centros educativos.

Marco normativo

Resolución de 2 de julio de 2020, de la Dirección General de Evaluación y Cooperación Territorial, por la que se publica el Acuerdo de la Conferencia Sectorial de Educación sobre el marco de referencia de la competencia digital docente.



AREA 1 – INFORMACIÓN Y ALFABETIZACIÓN INFORMACIONAL

AREA 2 – COMUNICACIÓN Y COLABORACIÓN

AREA 3 – CREACIÓN DE CONTENIDOS DIGITALES

AREA 4 – SEGURIDAD

AREA 5 – RESOLUCIÓN DE PROBLEMAS

Fuente: <https://bit.ly/3xPbFZm>

Competencia digital

1. INFORMACIÓN Y ALFABETIZACIÓN INFORMACION

- Navegación, búsqueda y evaluación de información y contenidos digitales presentes en la red.
- Gestión y almacenamiento de información, datos y contenidos digitales.
- Evaluación de la información y contenidos.

Navegación, búsqueda y evaluación de información y contenidos digitales presentes en la red.



Operadores de búsqueda



Gestión y almacenamiento de información, datos y contenidos digitales.



Colecciones de Edge



Wakelet



OneDrive

Evaluación de la información y contenidos.

Autoría:

- ¿Puedes identificar al responsable?
- ¿puedes contactar con él?

Objetividad:

- ¿Intentan vender algo?
- ¿por qué y para quien se ha publicado?

Contenido:

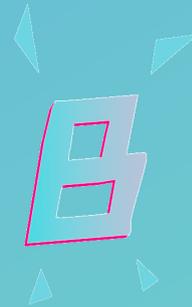
- ¿Incluye enlaces externos y/o bibliografía?

Actualidad:

- ¿El contenido está actualizado?
- ¿tiene enlaces rotos?

Usabilidad:

- ¿Es fácil navegar por la página?
- ¿hay un enlace visible a la institución u organización que la ampara?



2. COMUNICACIÓN Y COLABORACIÓN

- Interacción mediante las tecnologías digitales
- Compartir información y contenidos
- Colaboración mediante canales digitales
- Netiqueta
- Gestión de la identidad digital

Interacción mediante las tecnologías digitales



Teams



Teams

Colaboración mediante canales digitales

EDUCACIÓN 3.0
LÍDER INFORMATIVO EN INNOVACIÓN EDUCATIVA



Yammer

Netiqueta



Plan de seguridad y confianza digital en el ámbito educativo.

REGLAS DE NETIQUETA

1. REGLA N.º 1. Recuerde lo humano
2. REGLA N.º 2. Sea ético.
3. REGLA N.º 3. Sepa en que lugar del ciberespacio está
4. REGLA N.º 4. Respete el tiempo y el ancho de banda de los demás
5. REGLA N.º 5. Ponga de su parte, vease muy bien en línea
6. REGLA N.º 6. Comparta el conocimiento de los expertos
7. REGLA N.º 7. Ayuda a que las controversias se mantengan bajo control
8. REGLA N.º 8. Respeto por la privacidad de los demás
9. REGLA N.º 9. No abuse de las ventajas que pueda usted tener
10. REGLA N.º 10. Examine los errores de otros

genially

Junta de Castilla y León
Consejería de Educación

#Se_con_TIC

Gestión de la identidad digital



Gestión de la identidad digital

- Es una representación virtual que nos permite interactuar en la red, proyectar una personalidad y difundir una trayectoria personal o profesional.
- Es posible no querer tener una identidad digital, pero ello no garantiza que otras personas hablen o publiquen material de un individuo determinado, o bien suplante su identidad en Internet.
- La propia identidad digital debería ser totalmente coherente con la real, pero la red puede ser el escenario idóneo para realizar algunas actividades que no serían posibles de realizar en lo analógico.
- Todo lo que se publica en Internet queda para la posteridad, hecho que puede tener consecuencias futuras en la imagen y la reputación personal.
- Crear una identidad digital significa entender la tecnología y participar de ella.
- Hay buenas razones para tener varias identidades digitales en contextos diferentes, como en la vida, pero es también un riesgo, del mismo modo que alguien puede engañar, también puede ser engañado.
- La credibilidad y la confianza, en el mundo virtual, también se gestionan aportando información responsable y ética.

3. CREACIÓN DE CONTENIDOS DIGITALES

Licencias y derechos de autor



Creación y evaluación de contenido



genially



Mindomo™



Microsoft Stream



5. RESOLUCIÓN DE PROBLEMAS

RESOLUCIÓN DE PROBLEMAS TÉCNICOS		<p><u>CENTRO DE SOPORTE JCYL</u></p> <p>Web de soporte de EducaCyL con información y recursos de interés.</p>		<p><u>MICROSOFT</u></p> <p>Web de soporte y formación de las herramientas corporativas de Office 365.</p>
		<p><u>MOODLE</u></p> <p>Manuales de uso y soporte sobre la herramienta corporativa Moodle.</p>		<p><u>OSI</u></p> <p>Línea de ayuda y soporte de la Oficina de Seguridad del Internauta</p>

IDENTIFICACIÓN DE NECESIDADES TECNOLÓGICAS		<p><u>SELFIE</u></p> <p>Herramienta de autoreflexión de la competencia digital del docente y el alumno.</p>		<p><u>CERTICYL</u></p> <p>Certificación de la competencia digital a través de las diferentes sedes del CyL digital.</p>
--	---	---	---	---

5. RESOLUCIÓN DE PROBLEMAS

INNOVACIÓN EDUCATIVA		<p><u>CFIE PROVINCIAL</u></p> <p>Oferta formativa relacionada con la competencia digital del profesorado en los CFIEs provinciales de referencia.</p>		<p><u>CRFPTIC</u></p> <p>Proyectos de Innovación Educativa convocados por el CRFPTIC y otros CFIEs regionales.</p>
		<p><u>PROYECTOS DE INNOVACIÓN EDUCACYL</u></p> <p>Convocatoria de Proyectos de Innovación Educativa en EducaCyL.</p>		<p><u>SIMO EDUCACIÓN</u></p> <p>Proyectos innovadores, experiencias y premios educativos en el Salón Internacional de Tecnología e Innovación Educativa.</p>
		<p><u>APRENDE INTEF</u></p> <p>Formación online a través del INTEF con MOOC, NOOC y SPOOC relacionados con la competencia digital del profesorado.</p>		<p><u>MINISTERIO DE EDUCACIÓN Y FP</u></p> <p>Formación en red del profesorado a través del Ministerio de Educación y Formación Profesional.</p>
		<p><u>MEJORA ESCUELA PÚBLICA</u></p> <p>Asociación para la promoción de buenas prácticas y proyectos de innovación educativa.</p>		<p><u>GRANDES PROFES, GRANDES INICIATIVAS</u></p> <p>Premios para la promoción de proyectos innovadores y de éxito entre la comunidad educativa.</p>

¿CUÁNTO SABES DE CIBERSEGURIDAD?



4. SEGURIDAD

- Protección de dispositivos
- Protección de datos personales e identidad digital
- Protección de la salud

Protección de dispositivos

Creando un espacio de trabajo seguro

Identifica cada elemento y aplica estos consejos para garantizar la seguridad de la información de tu empresa.

COPIAS DE SEGURIDAD

Te ayudan a proteger la información y a disponer de una versión de respaldo en caso de perder la original. Aplica la regla 3-2-1.

DISPOSITIVOS IOT

Los dispositivos inteligentes son cada vez más comunes en las casas, pero si no están bien configurados pueden ser la puerta de entrada a una gran cantidad de amenazas.

DISPOSITIVOS EXTRAÍBLES (USB)

Deshabilita la autoejecución de dispositivos USB. Serás menos vulnerable en caso de que contengan algún fichero infectado.

POST-IT O INFORMACIÓN A LA VISTA

Es importante no dejar a la vista datos relevantes, como claves de acceso.

SISTEMA BLOQUEADO

Siempre que abandones tu equipo, bloquea la sesión. Es un buen hábito para mantener a raya las miradas indiscretas.

DOCUMENTOS Y CARPETAS EN LA MESA

Los documentos en un cajón no están a salvo, mejor mantén la información cifrada.

IMPRESORA O ESCANER

Es preferible que utilices tus dispositivos. Si usas uno compartido, recuerda eliminar la bandeja de entrada cuando termines de utilizarlo.

WEBCAM

Mantén el control de tu webcam para evitar fraudes, como la sextorsión y el robo de información. Tapa la cámara cuando no la estés usando.

WIFI/ROUTER

Realiza siempre conexiones seguras. Configura tu router y ten cuidado con las redes públicas.

ACTUALIZACIONES AUTOMÁTICAS

Cada día aparecen nuevas amenazas y vulnerabilidades, por lo que debes mantener el software del equipo actualizado para hacer frente a dichos riesgos.

RED PRIVADA VIRTUAL (VPN)

Si tu empresa no te facilita ninguna VPN concreta para teletrabajar, te recomendamos que instales una para añadir una capa extra de seguridad a tus conexiones.

¡Sigue estas pautas y disfruta de un entorno de trabajo seguro!

PERMISOS DE APLICACIONES

Protección de dispositivos

1



Bloquear

+ INFO

2



Bloqueo automático

+ INFO

3



Copia de seguridad

+ INFO

4



No compartir el dispositivo

+ INFO

5



Privacidad

+ INFO

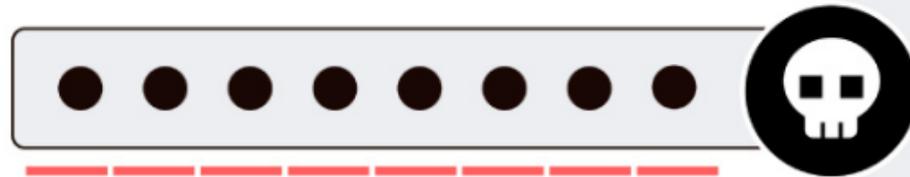
Protección de dispositivos (contraseñas)

Ataques a las contraseñas

¡Infórmate sobre ellos y protégete adecuadamente para que no te afecten!



PASSWORD



Conocer cuáles son las estrategias que usan los ciberdelincuentes para intentar robar contraseñas nos ayuda a protegernos mejor de posibles ataques y amenazas

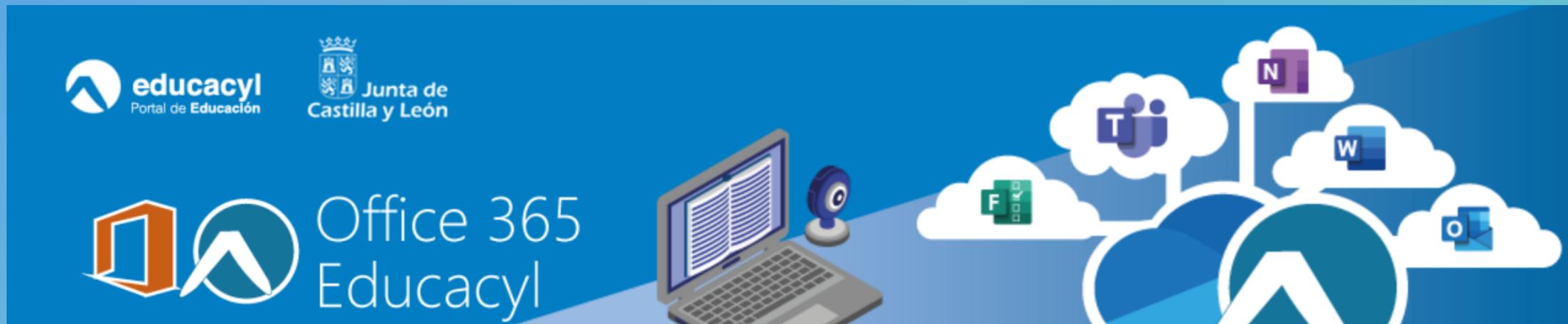
Protección de dispositivos



Protección de dispositivos



Protección de dispositivos (herramientas corporativas)



educacyl
Portal de Educación

 **Junta de Castilla y León**

 **Office 365**
Educacyl

Microsoft Office 365 applications: Word, Excel, PowerPoint, Teams, OneDrive.



Aulas Virtuales

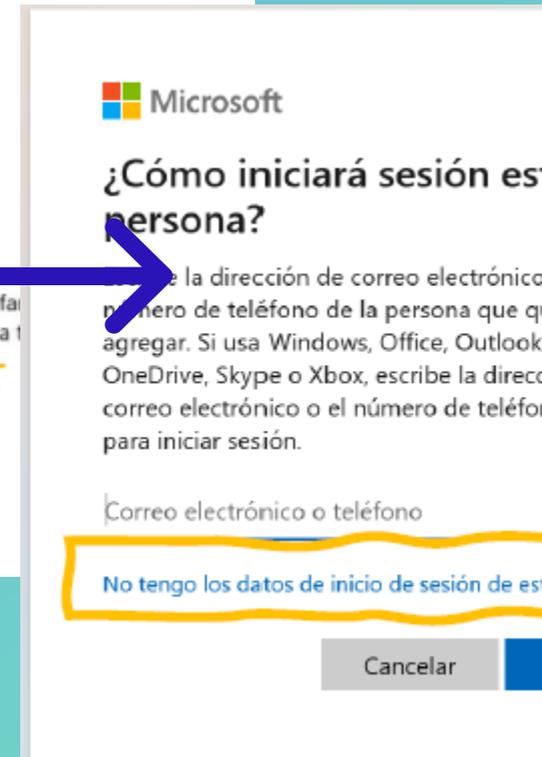
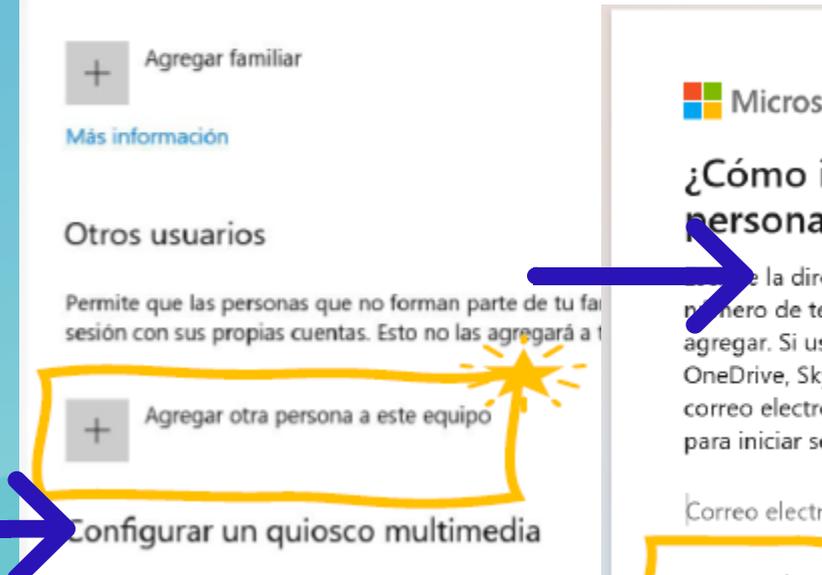
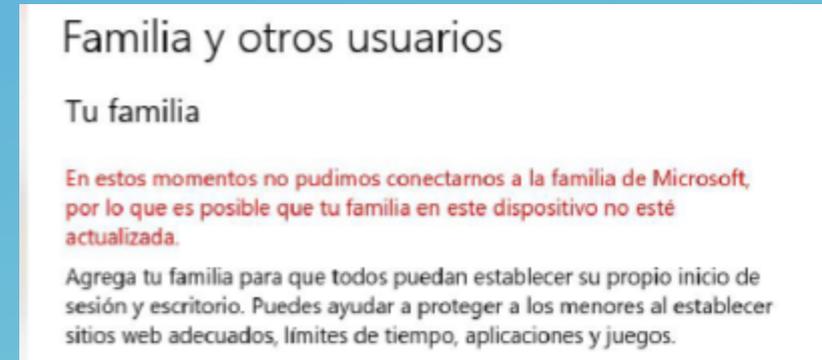
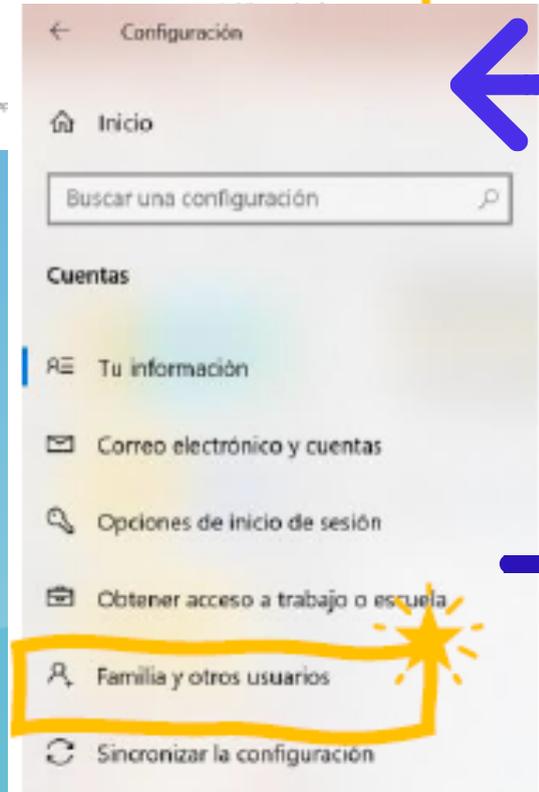
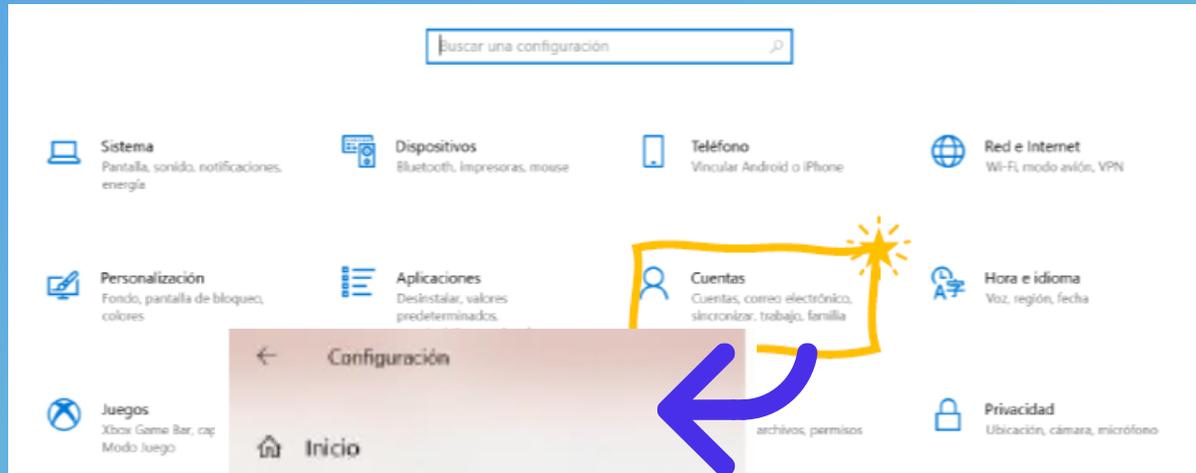
Educacyl

APP

ACGBW NQ

Illustrations: students, laptop, smartphone, graduation cap.

Protección de dispositivos (creación de usuarios específicos 1)



Protección de dispositivos (creación de usuarios específicos 2)

 Microsoft

Crear cuenta

[Usar un número de teléfono en su lugar](#)

[Obtener una nueva dirección de correo electrónico](#)

[Agregar un usuario sin cuenta Microsoft](#)

Crear un usuario para este equipo

Si quieres usar una contraseña, elige algo que te resulte fácil de recordar, pero que sea difícil de adivinar para los demás.

¿Quién va a usar este PC?

Dale seguridad.

Protección de dispositivos (sistema de bloqueo del dispositivo)

The image shows a sequence of steps to configure screen protection in Windows. It starts with the Settings app, where the 'Personalización' (Personalization) category is selected. Within this category, the 'Pantalla de bloqueo' (Lock screen) option is highlighted. This leads to the 'Pantalla de bloqueo' (Lock screen) settings page, where the 'Protector de pantalla' (Screen protector) toggle is turned on. Below this, the 'Elegir una aplicación para mostrar el estado detallado en la pantalla de bloqueo' (Choose an app to show detailed status on the lock screen) section is visible, showing a search bar and a list of apps with plus signs. The 'Elegir qué aplicaciones muestran el estado rápido en la pantalla de bloqueo' (Choose which apps show quick status on the lock screen) section is also visible, showing a search bar and a list of apps with plus signs. The 'Mostrar imagen de fondo de la pantalla de bloqueo en la pantalla de inicio de sesión' (Show lock screen background on the sign-in screen) toggle is turned on. At the bottom, the 'Configuración del tiempo de espera de la pantalla' (Screen timeout settings) and 'Configuración de protector de pantalla' (Screen protector settings) links are highlighted. A blue arrow points from the 'Configuración de protector de pantalla' link to a separate window titled 'Configuración del protector de pantalla' (Screen protector settings). This window shows the 'Protector de pantalla' (Screen protector) dropdown menu set to '(ninguno)' (none), with 'Configuración...' (Settings...) and 'Vista previa' (Preview) buttons. The 'Esperar' (Wait) section is set to 1 minute, and the 'Mostrar la pantalla de inicio de sesión al reanudar' (Show sign-in screen when resuming) checkbox is checked. The 'Administración de energía' (Power management) section is also visible, with a link to 'Cambiar configuración de energía' (Change power settings). A blue arrow points from the 'Configuración de protector de pantalla' link to the 'Configuración del protector de pantalla' window. Another blue arrow points from the 'Mostrar imagen de fondo de la pantalla de bloqueo en la pantalla de inicio de sesión' toggle to the 'Mostrar la pantalla de inicio de sesión al reanudar' checkbox. A yellow starburst is placed over the 'Configuración de protector de pantalla' link and the 'Configuración del protector de pantalla' window.

Buscar una configuración

Sistema
Pantalla, sonido, notificaciones, energía

Dispositivos
Bluetooth, Impresoras, mouse

Personalización
Fondo, pantalla de bloqueo, colores

Anuncios

Juegos
Xbox Game Bar, capturas de pantalla, Modo Juego

Configuración

Inicio

Buscar una configuración

Personalización

Fondo

Colores

Pantalla de bloqueo

Temas

Fuentes

Inicio

Barra de tareas

Pantalla de bloqueo

Mostrar datos curiosos, recomendaciones y mucho más de Windows y Cortana en la pantalla de bloqueo

Activado

Elegir una aplicación para mostrar el estado detallado en la pantalla de bloqueo

+ + S + + + +

Elegir qué aplicaciones muestran el estado rápido en la pantalla de bloqueo

+ + + + + +

Mostrar imagen de fondo de la pantalla de bloqueo en la pantalla de inicio de sesión

Activado

[Configuración del tiempo de espera de la pantalla](#)

[Configuración de protector de pantalla](#)

Configuración del protector de pantalla

Protector de pantalla

(ninguno) Configuración... Vista previa

Esperar: 1 minutos Mostrar la pantalla de inicio de sesión al reanudar

Administración de energía

Puede conservar energía y optimizar el rendimiento si ajusta el brillo de la pantalla y otras configuraciones de energía.

[Cambiar configuración de energía](#)

Aceptar Cancelar Aplicar

Protección de dispositivos (conexión a redes seguras)



Perfil de red

Público
El equipo se establece como oculto para otros dispositivos de la red y no se puede usar para compartir archivos e impresoras.

Privada
Para una red de confianza, como la de tu hogar o el trabajo. El equipo se establece como reconocible y se puede usar para compartir archivos e impresoras si lo configuras.

[Establecer la configuración de firewall y seguridad](#)

Establecer ubicación de red

Personalizar la configuración de red

Nombre de red:

Tipo de ubicación:

Pública
Se limitará la detección de otros equipos y dispositivos, y es posible que el uso de esta red se restrinja para algunos programas.

Privada
Esto le permite ver otros equipos y dispositivos y permite también que este equipo se pueda detectar.

[Deseo ayuda para elegir](#)

Icono de red:

[Combinar o eliminar ubicaciones de red](#)

- ES PREFERIBLE NO CONECTARTE A REDES ABIERTAS.
- ACCEDE A UNA RED CON SEGURIDAD WPA O WPA2.
- NO INICIES SESIÓN EN NINGÚN LUGAR QUE NO SEA TU EQUIPO PERSONAL O DE TRABAJO.
- ELIMINA LOS DATOS DE LA RED MEMORIZADOS EN NUESTRO EQUIPO (borrar historial, olvidar red, etc.)

Puesta a punto para el nuevo curso

Con la vuelta de las vacaciones, repasaremos las buenas prácticas para mantener a raya a los ciberdelincuentes.

La segunda vida de nuestros dispositivos

Qué medidas de seguridad debemos tomar para deshacernos correctamente de nuestros dispositivos antiguos.

Protección de dispositivos (herramientas)



Oficina
de Seguridad
del Internauta

Acceso remoto

Antirrobo

Cortafuegos



Cifrado

Copia seguridad

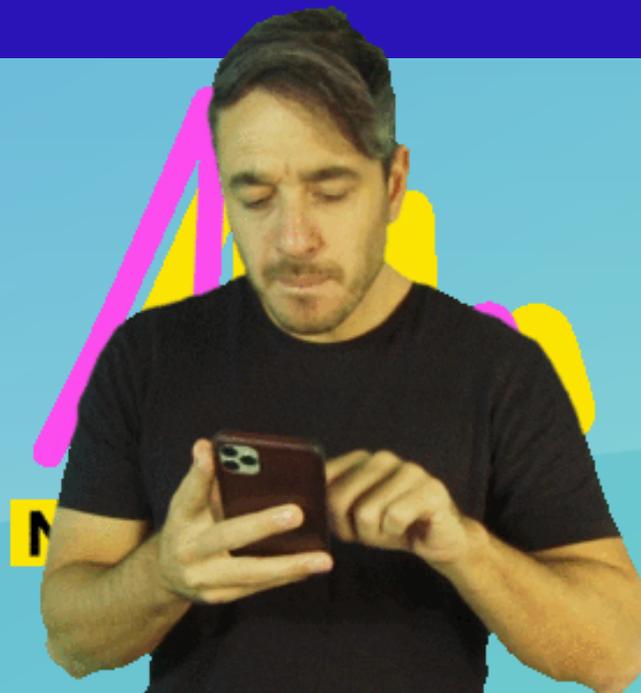
Mantenimiento



Limpieza

Antivirus

¿CUÁNTO SABES DE PROTECCIÓN DE DATOS?



Protección de datos personales e identidad



**Junta de
Castilla y León**

Consejería de Educación

INSTRUCCIÓN DE LA DIRECCIÓN GENERAL DE CENTROS, PLANIFICACIÓN Y
ORDENACIÓN EDUCATIVA SOBRE EL TRATAMIENTO DE DATOS DE IMAGEN / VOZ DE
ALUMNOS EN CENTROS DOCENTES DE TITULARIDAD PÚBLICA DE CASTILLA Y LEÓN.



Protección de datos personales e identidad

a.

¿Qué es un dato de carácter personal?

Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.



El nombre y apellidos de un alumno, de sus padres, su dirección, su número de teléfono o su correo electrónico son datos de carácter personal. También lo son las imágenes de los alumnos o, por ejemplo, la profesión, los estudios o el lugar donde trabajan los padres, o su número de cuenta bancaria.

f.

¿Quién es el responsable del tratamiento de datos?

El responsable del tratamiento es la persona física o jurídica, pública o privada, que decide sobre la finalidad, contenido y uso del mismo, bien por decisión directa o porque así le viene impuesto por una norma legal.

Cuando se trate de centros educativos públicos, el responsable del tratamiento será normalmente la Administración pública correspondiente: la Consejería de la Comunidad Autónoma competente en materia educativa, salvo para los centros de Ceuta y Melilla o los centros en el exterior titularidad del Estado dependientes del Ministerio de Educación Cultura y Deporte.

Cuando se trata de centros concertados y privados los responsables del tratamiento de los datos serán los propios centros.

Protección de datos personales e identidad



¿Pueden los profesores recoger datos personales directamente de los alumnos?

Sin perjuicio de los datos personales recabados por los centros o las Administraciones educativas al matricularse los alumnos, y que son facilitados a los profesores para el ejercicio de la función docente, cuando éstos recaben otros datos de carácter personal, como grabaciones de imágenes o sonido con la finalidad de evaluar sus conocimientos u otros datos relacionados con la realización de dichos ejercicios, o los resultados de su evaluación, estarían legitimados para hacerlo, en el marco de las instrucciones, protocolos o régimen interno que el centro o la Administración educativa haya adoptado.

Protección de datos personales e identidad



¿Puede un centro educativo acceder al contenido de dispositivos electrónicos de los alumnos, como los sistemas de mensajería instantánea (WhatsApp) o redes sociales?

Dada la información que se contiene en los dispositivos con acceso a internet, así como la trazabilidad que se puede realizar de la navegación efectuada por los usuarios, el acceso al contenido de estos dispositivos de los alumnos, incluyendo su clave, supone un acceso a datos de carácter personal que requiere el consentimiento de los interesados o de sus padres o tutores si se trata de menores de 14 años.

No obstante, en situaciones en las que pudiera estar presente el interés público, como cuando se ponga en riesgo la integridad de algún alumno (situaciones de ciberacoso, sexting, grooming o de violencia de género) el centro educativo podría, previa ponderación del caso y conforme al protocolo que tenga establecido, acceder a dichos contenidos sin el consentimiento de los interesados.

Protección de datos personales e identidad



¿Pueden los profesores crear grupos con aplicaciones de mensajería instantánea con los alumnos?

Con carácter general, las comunicaciones entre los profesores y los alumnos deben tener lugar dentro del ámbito de la función educativa y no llevarse a cabo a través de aplicaciones de mensajería instantánea. Si fuera preciso establecer canales específicos de comunicación, deberían emplearse los medios y herramientas establecidas por el centro educativo y puestas a disposición de alumnos y profesores (por ejemplo, áreas específicas en la intranet del centro o uso de plataformas que cumplan los requisitos que se verán más adelante) o por medio del correo electrónico.

En situaciones concretas, como la realización de una tarea o trabajo específico, por ejemplo con motivo de la participación en un concurso escolar, o de refuerzo que fueran necesarias, se podrían crear con carácter excepcional, siendo aconsejable la participación en el grupo de un tercero, padre o madre de los alumnos.

Protección de datos personales e identidad



¿Pueden los profesores grabar imágenes de los alumnos y difundirlas a través de aplicaciones de mensajería instantánea a los padres?

No como parte del ejercicio de la función educativa de la que es responsable el centro docente. No obstante, en aquellos casos en los que el interés superior del menor estuviera comprometido, como en caso de accidentes o indisposiciones en una excursión escolar, y con la finalidad de informar y tranquilizar a los padres, titulares de la patria potestad, se podrían captar las imágenes y enviárselas. También podría ser posible en los grupos generados a través de aplicaciones de mensajería instantánea relacionados con la específica situación del alumno, a los que se ha hecho referencia en la pregunta anterior.

Protección de datos personales e identidad



¿Pueden los profesores facilitar las calificaciones oralmente en clase?

Como se ha indicado, no existe una regulación respecto de la forma de comunicar las calificaciones. Aunque sería preferible que las calificaciones se notificasen en la forma indicada en el punto anterior, sería posible enunciarlas oralmente, evitando comentarios adicionales que pudieran afectar personalmente al alumno.

Protección de datos personales e identidad



¿Pueden los padres solicitar las calificaciones de sus hijos mayores de edad?

Si los alumnos fueran mayores de edad (18 años) sus padres podrán solicitar el acceso a las calificaciones cuando éstos fueran los que corrieran con los gastos educativos o de alimentos, pues en ese caso existiría un interés legítimo de los padres, derivado del mantenimiento de sus hijos mayores de edad, en conocer su evolución académica sobre el que no prevalecerían los derechos y libertades de éstos.

Protección de datos personales e identidad



¿Pueden los padres solicitar los exámenes de sus hijos para llevárselos a casa y repasarlos?

Esta cuestión no depende de la normativa de protección de datos, pues no se trata de un derecho de acceso a los datos, sino de acceso a documentación que, en su caso, deberá ser resuelta por el centro o la Administración educativa correspondiente con arreglo a su normativa interna y demás legislación sectorial que sea de aplicación.

Protección de datos personales e identidad



¿Puede un profesor grabar imágenes de los alumnos para una actividad escolar?

Los profesores, en el desarrollo de la programación y enseñanza de las áreas, materias y módulos que tengan encomendados, pueden disponer la realización de ejercicios que impliquen la grabación de imágenes, normalmente de los propios alumnos, que sólo deberán estar accesibles para los alumnos involucrados en dicha actividad, sus padres o tutores y el profesor correspondiente.

Es decir, en ningún caso el mero hecho de realizar la grabación supone que la misma se pueda difundir de forma abierta en internet y que se pueda acceder de manera indiscriminada.

En estos casos el responsable del tratamiento es el propio centro o la Administración educativa.

Protección de la salud





ACTIVIDAD FINAL



i76oym9o

<https://wke.lt/w/s/rXIQ8o>

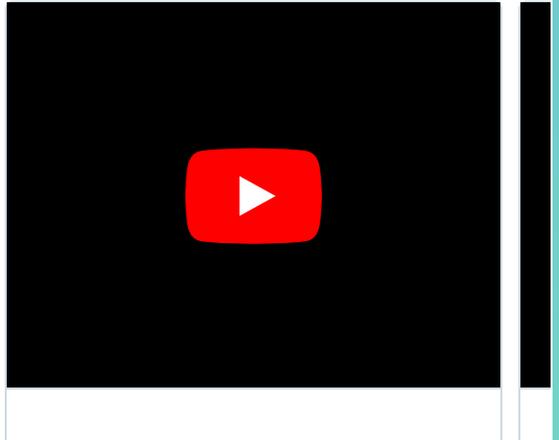


EOI PALENCIA
3 5 Items

Recursos seguridad y confianza digital

Información y alfabetización informacional

Navegación, búsqueda y filtrado de información, datos y contenidos digitales.



Mil gracias

