

PLAN DE SEGURIDAD Y CONFIANZA DIGITAL

IES ALISTE



ÍNDICE

A. INTRODUCCIÓN	1
B. OBJETIVOS.....	1
Objetivo general.....	1
Objetivos específicos	1
C. ORGANIZACIÓN Y RESPONSABLES.....	1
Equipo responsable del plan.....	1
D. ANÁLISIS DE RIESGOS DIGITALES.....	2
Riesgos relacionados con la seguridad y la privacidad	2
E. MEDIDAS DE SEGURIDAD.....	3
F. MEDIDAS DE PREVENCIÓN PARA LOS RIESGOS DIGITALES	4
G. ESTRUCTURA ORGANIZATIVA DE SEGURIDAD, SERVICIOS, REDES Y EQUIPOS.	5
H. CRITERIOS DE ALMACENAMIENTO Y CUSTODIA DE DATOS ACADÉMICOS, DIDÁCTICOS Y DOCUMENTALES	6
I. ACTUACIONES DE FORMACIÓN Y CONCIENCIACIÓN RELACIONADAS CON EL PSCD	6
Profesorado	6
Alumnado	6
Familias	7
J. PROTOCOLO DE ACTUACIÓN ANTE INCIDENTES DIGITALES	7
K. DIFUSIÓN.....	8
L. EVALUACIÓN Y REVISIÓN	8
ANEXO I:.....	10
ANEXO II: Cuestionario de evaluación del PSCD del IES. ALISTE	12
ANEXO III. Protocolos en caso de CIBER ACOSO	16

A. INTRODUCCIÓN

La transformación digital del sistema educativo implica el uso habitual de plataformas educativas, dispositivos digitales y herramientas de comunicación online. Este contexto genera oportunidades educativas, pero también **riesgos relacionados con la seguridad, privacidad, convivencia digital y uso responsable de la tecnología**.

El presente **Plan de Seguridad y Confianza Digital del IES Aliste** tiene como finalidad establecer protocolos para:

- Garantizar un **entorno digital seguro para alumnado, profesorado y familias**.
- Proteger **datos personales y sistemas informáticos** del centro.
- Prevenir **ciberacoso, uso inadecuado de dispositivos y riesgos en Internet**.
- Promover **competencia digital crítica y responsable**.

Este plan se desarrolla de acuerdo a la normativa vigente:

- Reglamento General de Protección de Datos (RGPD)
- Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD)
- LOMLOE
- Protocolos de convivencia escolar y ciberacoso.

B. OBJETIVOS

Objetivo general

Desarrollar una **cultura de seguridad digital en el centro educativo**, garantizando el uso seguro, ético y responsable de las tecnologías.

Objetivos específicos

- Proteger la **información y datos personales** del centro.
- Establecer **protocolos de seguridad informática**.
- Prevenir **ciberacoso, grooming, sexting y otros riesgos online**.
- Promover **competencia digital segura en el alumnado**.
- Formar al profesorado en **seguridad digital educativa**.
- Implicar a las familias en la **educación digital responsable**.

C. ORGANIZACIÓN Y RESPONSABLES

Equipo responsable del plan

	Funciones
Equipo Directivo	• Aprobar y supervisar el Plan • Implementar medidas técnicas • Supervisar el tratamiento de datos

Comisión TIC	• Elaborar, actualizar y difundir el Plan
Coordinador TIC	• Informar de incidencias y gestionar las mismas • Implementar medidas técnicas
Orientadora	• Orientar a J.E. en la elaboración del PAT y establecer acciones a desarrollar en tutoría de acuerdo con el presente plan
Equipo Docente	• Promover el uso seguro de herramientas digitales

D. ANÁLISIS DE RIESGOS DIGITALES

Los principales riesgos a los que para los que debemos preparar medidas de prevención y actuación son:

Riesgos relacionados con la seguridad y la privacidad

- Pérdida o difusión de datos personales (nombre, fotos, ubicación, contraseñas).
- Suplantación de identidad en redes sociales o plataformas educativas.
- Acceso no autorizado a cuentas del alumnado o del centro.
- Uso inadecuado de imágenes o vídeos de compañeros o docentes.

Riesgos de convivencia digital

- Ciberacoso o acoso digital entre iguales.
- Difusión de rumores, insultos o amenazas a través de mensajería o redes sociales.
- Exclusión social en entornos digitales (grupos cerrados, burlas online).
- Grabación y difusión de situaciones humillantes dentro o fuera del centro.

Riesgos relacionados con el acceso a contenidos inapropiados

- Exposición a contenidos violentos, discriminatorios o pornográficos.
- Desinformación o noticias falsas.
- Contenido que promueva conductas de riesgo (retos virales peligrosos).

Riesgos técnicos y de seguridad informática

- Malware, virus o software malicioso al descargar archivos o aplicaciones.
- Phishing o engaños para obtener datos personales.
- Uso de redes Wi-Fi inseguras.
- Instalación de aplicaciones sin control o autorización.

Riesgos para el bienestar personal

- Uso excesivo o dependencia de dispositivos.
- Problemas de concentración y rendimiento académico.
- Alteraciones del sueño o sedentarismo por uso prolongado de pantallas.
- Impacto emocional por la presión social en redes.

Riesgos legales y de responsabilidad

- Difusión de imágenes sin consentimiento (posible vulneración del derecho a la intimidad).
- Descarga o distribución de contenidos protegidos por derechos de autor.
- Participación en conductas que puedan tener consecuencias disciplinarias o legales.

E. MEDIDAS DE SEGURIDAD

Seguridad técnica

- Uso exclusivo de **plataformas educativas autorizadas por la Junta**.
- Actualización periódica de sistemas y dispositivos.
- Uso obligatorio de **contraseñas seguras**.
- Autenticación institucional del profesorado.
- Control de acceso a redes WiFi del centro.
- Antivirus y cortafuegos actualizados.
- Copias de seguridad periódicas.

Protección de datos

Medidas adoptadas:

- Registro de actividades de tratamiento de datos.
- Autorización familiar para uso de imágenes.
- Minimización de datos personales.
- Los criterios de **seguridad y conservación de datos** implican la realización de backup diario de los ficheros de la red de Secretaría.
- Uso de correos institucionales.
- El acceso físico al **servidor** está restringido en remoto al Equipo Directivo, la administrativa y al coordinador del SIGIE de la dirección provincial.
- En el **Plan de Tratamiento de Datos de Imagen/Voz del IES. Aliste** se reflejan las actuaciones del IES. Aliste para garantizar el tratamiento de estos datos de acuerdo con la normativa vigente y las recomendaciones de la Consejería de Educación
- Con respecto a la **publicación de datos de nuestro alumnado** el IES. Aliste se ajusta a lo explicitado en la tabla (ANEXO I) que aclara que tipo de datos del alumnado se tratan en un centro y cuáles pueden ser publicados (imagen extraída de <https://protecciondatos-lopdp.com/empresas/centros-educativos>)

Se evitará:

- Uso de cuentas personales para comunicación con alumnado.
- Compartir información académica por canales no oficiales.

Uso responsable de dispositivos

Normas generales de uso por parte del alumnado

- Los dispositivos personales solo podrán usarse con fines educativos y con autorización docente.
- Queda prohibido:
 - grabar sin consentimiento

- difundir imágenes de la comunidad educativa
- acceder a contenidos inapropiados

Medidas generales

- Acceder a los ordenadores de las aulas, sala de profesores y departamentos desde el perfil correspondiente (profesor/alumno).
- El perfil de administrador solo será accesible para los técnicos del CAU.
- No se deben usar pen drive en los ordenadores de uso común, pero si se necesitara hacerlo, revisar con un antivirus antes de utilizarlos.
- Al final del último trimestre se solicitará al CAU que en verano vengan a realizar un formateo de los Equipos del Aula de Informática y una revisión de los demás equipos del centro (formateo si fuese preciso, antivirus, aplicaciones, ...)

F. MEDIDAS DE PREVENCIÓN PARA LOS RIESGOS DIGITALES

Medidas preventivas relacionadas con la seguridad y la privacidad

- Formación del alumnado en **protección de datos personales y privacidad digital**, promoviendo el uso responsable de la información personal en internet.
- Educación en **buenas prácticas de seguridad**: creación de contraseñas seguras, no compartir credenciales y uso responsable de las cuentas institucionales.
- Sensibilización sobre los **riesgos de la suplantación de identidad** y sobre la importancia de proteger los perfiles personales en plataformas digitales.
- Establecimiento de **normas claras sobre el uso y difusión de imágenes o vídeos** de miembros de la comunidad educativa.
- Supervisión del uso de las **plataformas educativas del centro** mediante cuentas institucionales y control de accesos.

Medidas preventivas relacionadas con la convivencia digital

- Desarrollo de actividades de **educación en ciudadanía digital y convivencia en línea**, fomentando el respeto y la responsabilidad en la comunicación digital.
- Inclusión en el **Plan de Convivencia del centro** de actuaciones específicas frente al ciberacoso.
- Información al alumnado sobre los **canales de comunicación y denuncia** disponibles en el centro ante situaciones de acoso digital.
- Realización de **acciones de sensibilización y prevención** sobre el ciberacoso dirigidas al alumnado y a las familias.
- Prohibición expresa de **grabar, fotografiar o difundir imágenes de otras personas sin su consentimiento** dentro o fuera del ámbito escolar.

Medidas preventivas ante el acceso a contenidos inapropiados

- Uso de **sistemas de filtrado de contenidos y control de navegación** en la red del centro.
- Desarrollo de actividades educativas orientadas a la **alfabetización mediática y el pensamiento crítico**, para identificar información falsa o manipulada.
- Información al alumnado sobre los **riesgos asociados a retos virales o contenidos peligrosos** difundidos en internet.
- Supervisión del uso de dispositivos digitales durante las actividades educativas.

Medidas preventivas relacionadas con la seguridad informática

- Instalación y mantenimiento de **sistemas de protección informática** en los equipos del centro (antivirus, actualizaciones de seguridad, control de accesos).
- Formación básica del alumnado sobre **riesgos de malware, phishing y fraudes digitales**.
- Restricción de la **instalación de aplicaciones o programas no autorizados** en los dispositivos del centro.
- Uso exclusivo de **redes seguras del centro** para el desarrollo de actividades educativas con dispositivos institucionales.

Medidas preventivas relacionadas con el bienestar personal

- Promoción de **hábitos saludables de uso de la tecnología**, fomentando el equilibrio entre el tiempo de pantalla y otras actividades.
- Desarrollo de actividades educativas sobre **uso responsable y consciente de dispositivos digitales**.
- Sensibilización sobre los **efectos del uso excesivo de pantallas** en la salud, el descanso y el rendimiento académico.
- Inclusión de orientaciones sobre **bienestar digital** en las actividades de tutoría y orientación educativa.

Medidas preventivas relacionadas con la responsabilidad legal

- Información al alumnado sobre las **implicaciones legales del uso inadecuado de las tecnologías**.
- Educación en **respeto a la intimidad, protección de la imagen y derechos de autor** en el entorno digital.
- Inclusión en las **Normas de Organización y Funcionamiento del centro** de normas específicas relativas al uso de dispositivos y recursos digitales.
- Difusión entre alumnado y familias de las **normas de uso responsable de las TIC** del centro.

G. ESTRUCTURA ORGANIZATIVA DE SEGURIDAD, SERVICIOS, REDES Y EQUIPOS.

Seguridad de servicios

Servicios	Estrategias y criterios de seguridad	Responsable
Moodle / Teams	Control de acceso mediante cuentas institucionales	Comisión TIC
Correo	Uso exclusivo para comunicaciones educativas	Equipo Directivo
Herramientas digitales	Instalación de herramientas controlado y realizado des	Comisión TIC/CAU
RRS	Publicación controlada de contenidos	Comisión TIC

Seguridad de red

RED	Estrategias y criterios de seguridad	Responsable
Red de Escuelas Conectadas de Castilla y León	Acceso autenticado con usuario corporativo y red filtrada	CAU

H. CRITERIOS DE ALMACENAMIENTO Y CUSTODIA DE DATOS ACADÉMICOS, DIDÁCTICOS Y DOCUMENTALES

Criterios y procedimientos de almacenamiento

Tipo de dato	Criterios de almacenamiento y custodia	Responsable
Datos académicos del alumnado	Almacenamiento en plataformas oficiales con automatización de copias periódicas (STILUS e IES2000)	Equipo Directivo
Imágenes y vídeos de actividades escolares	Almacenamiento en carpetas protegidas y publicación solo con consentimiento informado	Equipo Directivo
Informes	Archivo digital con encriptación de datos	Delegado de protección de datos
Documentos institucionales de centro	almacenan en los ordenadores de Dirección y Jefatura de Estudios y se envían a inspección, dentro de los plazos requeridos, en el espacio habilitado para ello en el entorno educa, a través de la cuenta de usuario de la directora del centro. Se comparten en la cuenta de ONEDrive del Centro	Equipo Directivo
Documentos de trabajo e interés para los docentes	En la cuenta de ONEDrive del Centro se comparte ○ INFORMACIÓN DEL CURSO ACADÉMICO: ▪ PARTES – JUSTIFICANTES DE ALUMNADO ▪ ELABORACIÓN DE PROGRAMACIÓN DIDÁCTICAS ▪ LEYES Y NORMATIVA ▪ LOGOS Y MEMBRETES ▪ TUTORÍA – RECEPCIÓN DE ALUMNOS EL PRIMER DÍA ○ ACTAS DE REUNIONES ○ PERMISOS Y AUSENCIAS DE DOCENTES ▪ NORMATIVA ▪ SOLICITUD ○ CALENDARIO DE REUNIONES	Equipo Directivo

I. ACTUACIONES DE FORMACIÓN Y CONCIENCIACIÓN RELACIONADAS CON EL PSCD

Se realizarán acciones formativas dirigidas a:

Profesorado

- seguridad digital
- protección de datos
- prevención del ciberacoso

Alumnado

- talleres de ciudadanía digital
- uso responsable de redes sociales
- prevención de delitos digitales

Familias

- charlas informativas
- guías de control parental
- acompañamiento digital

Que se concretarán en las siguientes actuaciones:

Perfil	Actuación de formación	Responsable
Profesorado	Educación y Tecnología Segura: Difusión de las herramientas/cursos del INCIBE para EDUCADORES en relación con aulas con ciberseguridad, ciberconvivencia y ciberseguridad	Responsable de formación
Alumnado	Riesgos de internet	Plan Director y PSCD
Familias	Jornadas de apoyo TIC para familias	PSCD / Equipo Directivo

J. PROTOCOLO DE ACTUACIÓN ANTE INCIDENTES DIGITALES

INCIDENTES DIGITALES GENERADOS POR EL ALUMNADO

En caso de incidente:

1. Comunicación inmediata al equipo directivo.
2. Registro del incidente.
3. Análisis del caso.
4. Aplicación del protocolo de convivencia.
5. Comunicación a familias.
6. Si procede, comunicación a autoridades competentes.

FALLO DE INTERNET

- RED WIFI
 - Comunicación inmediata al Coordinador TIC o al Equipo Directivo.
 - Registro de la incidencia y análisis del caso.
 - Contactar con el CAU y actuar según las indicaciones de los técnicos de este servicio.
 - Recurrir al cableado mientras se resuelve la incidencia.
 - Fomentar entre el profesorado el hábito de contar con recursos TIC que no precisen de la conexión constante a internet (OFF LINE), por ejemplo, contar con archivos descargados de Internet, presentaciones, ...
- CABLEADO
 - Contactar con el CAU y actuar según las indicaciones de los técnicos de este servicio.
 - Recurrir a la red WIFI para poder continuar con la actividad en la medida de lo posible.

- Fomentar entre el profesorado el hábito de contar con recursos TIC que no precisen de la conexión constante a internet (OFF LINE), por ejemplo, contar con archivos descargados de Internet, presentaciones, ...

FALLO RED ELÉCTRICA:

Preventivas:

- Inspecciones periódicas de la red eléctrica del centro a cargo de una auditoría externa.
- Inspecciones periódicas del sistema de Pararrayos del Centro.

Actuación:

Determinar si el fallo en la red es a causa de factores internos o externos al centro.

- Si el **fallo es externo** solo cabe esperar al restablecimiento de la red por parte de empresa licitadora de la red.
- Si el **fallo es interno**:
 - La secretaria del centro coordinará a las conserjes del centro a fin de determinar cuál es la zona de la red que causa la caída del sistema, para a continuación mantener aislada esa fase sin energía y continuar trabajando con el resto de fases si fuese posible.
 - Contactar con un servicio de reparación eléctrica.

CIBERATAQUE:

A la hora de detectar un ciberataque y responder, entran en juego dos tipos de medidas:

- **Técnicas y tecnológicas:**
 1. Desconectar los dispositivos atacados (desconexión de Internet y red eléctrica).
 2. Contactar con el CAU y actuar según las indicaciones de los técnicos de dicha institución.
- **Organizativas.**
 1. Una vez detectada la vulnerabilidad de un equipo, el coordinador TIC lo aislará.
 2. El coordinador TIC comunica a la Comisión TIC y a la Secretaria del centro el incidente detectado para que se inicien actuaciones.
 3. La Secretaria del Centro comunica la incidencia al CAU.
 4. El coordinador TIC comunicará el incidente al personal del centro y alertará de los riesgos.
 5. La Comisión TIC auditará el resto de equipos del centro para detectar posibles casos de equipos vulnerables y aislarlos.
 6. Comunicación de todos los casos al técnico del CAU encargado de la gestión.

K. DIFUSIÓN

El plan se difundirá mediante:

- página web del centro
- reuniones con familias
- sesiones informativas con alumnado
- claustro de profesores

L. EVALUACIÓN Y REVISIÓN

El plan será evaluado anualmente mediante:

- análisis de incidentes digitales
- cuestionarios a alumnado y profesorado (ANEXO II. Cuestionario de evaluación del PSCD del IES. Aliste para el profesorado)
- revisión del equipo directivo

Se introducirán mejoras para adaptarlo a **nuevos riesgos tecnológicos**.

ANEXO I:

DATOS PERSONALES EN CENTROS EDUCATIVOS

TIPOS DE DATOS TRATADOS

ORIGEN Y AMBIENTE FAMILIAR

INFORMACIÓN SOBRE LA
SITUACIÓN FAMILIAR
DEL ALUMNO Y SUS PADRES

CONDICIONES PERSONALES

EN LA MATRICULACIÓN, ASPECTOS
FÍSICOS Y PSICOLÓGICOS

DURANTE EL CURSO ESCOLAR,
TRATAMIENTOS MÉDICOS DEL CENTRO

DESARROLLO Y RESULTADO DE SU ESCOLARIZACIÓN

NOTAS ALUMNOS, ASIGNATURAS
ELEGIDAS, QUE PERFILAN AL ALUMNO

CIRCUNSTANCIAS NECESARIAS PARA EDUCAR

CONOCER LA SITUACIÓN FAMILIAR
DEL ALUMNO PARA SU BUEN
DESARROLLO EDUCATIVO

DATOS AJUSTADOS A LA FINALIDAD

NO SE PODRÁN RECABAR DATOS
QUE EXCEDAN LA FINALIDAD



TIPOS DE DATOS QUE PUEDEN PUBLICAR

LISTA ADMITIDOS

SIN ACCESO INDISCRIMINADO
SÓLO RESULTADO FINAL

EN CASOS DE VIOLENCIA DE GÉNERO SE
DEBERÁ PROTEGER AL MENOR

BENEFICIARIOS DE BECAS

ANONIMIZACIÓN DE LOS DATOS
PARA SU PUBLICACIÓN

CAPTACIÓN Y PUBLICACIÓN DE IMÁGENES

NO SERÁ NECESARIO RECABAR DE NUEVO
EL CONSENTIMIENTO SI SE REALIZA CON
FINES EDUCATIVOS

GRABACIÓN DE IMÁGENES SÓLO ACCESIBLE
PARA LOS ALUMNOS Y PADRES

DATOS EN LA WEB

SI LA WEB DEL CENTRO ES PÚBLICA SE
NECESITARÁ CONSENTIMIENTO

EN WEB RESTRINGIDA SE PUEDE PUBLICAR SI
SE INFORMA A LOS AFECTADOS

DATOS EN REDES SOCIALES

RECABAR EL CONSENTIMIENTO INEQUÍVOCO
DEL AFECTADO

SI LA RS ES PARTICULAR DEL PROFESOR,
ESTE SERÁ EL RESPONSABLE DE LOS DATOS

ANEXO II: Cuestionario de evaluación del PSCD del IES. ALISTE

DESCRIPTORES	No planteado	En desarrollo	Sistematizado
--------------	--------------	---------------	---------------

PROTECCIÓN DE DATOS Y CONFIDENCIALIDAD

1. El centro emplea o dispone de ficheros diferentes a los registrados por la Junta de Castilla y León en el Registro General de Protección de Datos.	☐	☐	☐
2. El centro dispone de medidas de registro de las personas que acceden a los ficheros de datos de carácter personal de nivel básico	☐	☐	☐
3. El centro dispone de un documento de planificación y organización de los procesos básicos de protección de datos.	☐	☐	☐
4. Existe un responsable de gestión de la protección de datos que aborda las incidencias relativas a la información y los datos.	☐	☐	☐
5. El centro tiene un plan de auditorías de seguridad para la protección de datos.	☐	☐	☐
6. Existe un reglamento claro con directrices específicas respecto a la disposición de imágenes y fotografías en la red.	☐	☐	☐
7. Tanto el profesorado como los padres y la comunidad escolar están informados y se les recuerda de forma regular dicho reglamento de centro sobre protección de datos.	☐	☐	☐
8. El centro solicita consentimiento en el uso de fotografía de los alumnos a los padres si es menor de 14 años y en el caso de mayores de 14 años al propio interesado. En todo caso se explicita el lugar de difusión y el tiempo de uso/fecha de retirada.	☐	☐	☐

ALMACENAMIENTO Y CUSTODIA DE DATOS

1. El centro tiene un procedimiento sistematizado de la realización periódica de copias de respaldo y está documentado.	☐	☐	☐
2. Las copias de seguridad se custodian en un lugar diferente a los equipos informáticos y están resguardados de incidencias (protección eléctrica, inundaciones,...)	☐	☐	☐
3. Se verifica periódicamente la lectura de copias anteriores.	☐	☐	☐
4. Existe una relación e identificación de equipos y dispositivos en los que se encuentran datos protegidos.	☐	☐	☐
5. Existe una relación de recursos compartidos en red con datos de carácter personal.	☐	☐	☐
6. Existe una relación de usuarios con acceso físico a los equipos con datos.	☐	☐	☐
7. Existe relación de personas ajenas al centro con acceso a equipos con datos de carácter personal, y mantienen acuerdos por escrito de confidencialidad.	☐	☐	☐
8. Existen criterios establecidos para la eliminación segura/definitiva de datos de dispositivos de almacenamiento (borrado seguro, destrucción física, inutilización...)	☐	☐	☐
9. La instalación de datos de carácter personal en otros equipos o dispositivos diferentes a los destinados a tal efecto, se lleva a cabo con consentimiento del responsable e identificación del equipo	☐	☐	☐

REDES LOCALES

- | | | | |
|--|--------------------------|--------------------------|--------------------------|
| 1. El centro tiene segmentadas las redes del centro en redes administrativas, redes educativas (de profesores y alumnos) y no son accesibles entre ellas | ☐ | ☐ | ☐ |
| 2. Están establecidos los criterios de uso, perfiles de usuario, configuración y acceso a cada una de las redes. | ☐ | ☐ | ☐ |
| 3. Las redes tienen sistemas de filtrado de acceso y bloqueo de aplicaciones en función de los usuarios de la red. | ☐ | ☐ | ☐ |
| 4. En las distintas redes de alumnos existe algún sistema de control parental o protección de acceso a lugares inapropiados. | ☐ | ☐ | ☐ |
| 5. El centro dispone de un gráfico con el esquema de la estructura física de las redes de centro en la que se muestren la ubicación de dispositivos de red y asignación de IP. | ☐ | ☐ | ☐ |
| 6. Existen protocolos para el control de la descarga de materiales ilegales. | ☐ | ☐ | ☐ |
| 7. El centro tiene implementados cortafuegos de red. | ☐ | ☐ | ☐ |
| 8. Existe en el centro un protocolo sobre el acceso a las redes de centro de equipos o dispositivos personales por parte del personal docente, no docente y alumnos. | ☐ | ☐ | ☐ |
| 9. Existe un responsable para el mantenimiento de la seguridad de las redes locales de centro. | ☐ | ☐ | ☐ |
| 10. Existe un registro sobre incidencias relativas a la seguridad de la red | ☐ | ☐ | ☐ |

REDES INALÁMBRICAS

- | | | | |
|---|--------------------------|--------------------------|--------------------------|
| 1. Los dispositivos de red (router, wifis, plc,...) tienen claves de acceso a la gestión registradas y suficientemente seguras, y son solamente accesibles desde la red local del centro. | ☐ | ☐ | ☐ |
| 2. Los puntos wifi y routers de aulas se apagan en periodos no lectivos. | ☐ | ☐ | ☐ |
| 3. Los dispositivos wifi disponen de un cifrado del tipo WPA2 con AES como mínimo. | ☐ | ☐ | ☐ |
| 4. El centro realiza un control periódico de los dispositivos que incorporan wifis virtuales. | ☐ | ☐ | ☐ |
| 5. Se realizan revisiones periódicas de configuración de wifis cobertura, claves de acceso y protocolo. | ☐ | ☐ | ☐ |
| 6. La potencia de los puntos wifi es adecuada al espacio que se desea utilizar (en el caso de wifis de aula o de administración). | ☐ | ☐ | ☐ |
| 7. En los periodos vacacionales se cierran los dispositivos de red prescindibles. | ☐ | ☐ | ☐ |
| 8. Existen limitaciones al acceso a los puntos wifi en función de la red de centro (filtrado de MAC, portales cautivos, claves de uso restringido...). | ☐ | ☐ | ☐ |
| 9. Se realizan revisiones periódicas de configuración de wifis cobertura, claves de acceso y protocolo. | ☐ | ☐ | ☐ |
| 10. El centro dispone de documentación sobre la organización tecnológica de las redes y servicios. | ☐ | ☐ | ☐ |

SEGURIDAD DE EQUIPOS Y DISPOSITIVOS

1. El centro tiene asignadas contraseñas de administrador y usuario con perfil de administración, y profesor y alumno con perfil estándar en los ordenadores y dispositivos de centro.
2. Existe un registro y criterios de centro para el uso de equipos personales y/o privados que acceden las redes del centro.
3. Se revisa la seguridad y uso de los equipos con periodicidad.
4. Los ordenadores del centro están inventariados, registrados, identificados y localizados.
5. Se dispone de inventario de software básico de los equipos, en general, con las licencias pertinentes
6. Se dispone de estrategias para la restauración de los equipos a estados anteriores (congeladores, recuperadores) o clonación de los mismos.
7. Todos los equipos disponen de programas de antivirus y control de malware adecuados a las características de los dispositivos.
8. En los dispositivos móviles del centro se tienen activadas las opciones de geolocalización antirrobo.
9. Los equipos y dispositivos de centro tienen activados los cortafuegos.
10. Las contraseñas de los usuarios son siempre de al menos 8 caracteres alfanuméricos
11. El software es instalado únicamente por responsables específicos, teniendo en cuenta las licencias disponibles y de seguridad para equipos y datos.
12. El alumno firma el compromiso de uso adecuado y seguro de los dispositivos de centro y de las redes del mismo.
13. Existen normas de buen uso de los equipos y dispositivos en los espacios en los que se utilizan.
14. Los navegadores están configurados para eliminar los datos al cerrar la sesión.
15. En los momentos de uso de los equipos y dispositivos en el centro por parte de los alumnos, siempre hay personal responsable.

☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐

SERVICIOS DE INTRANET

1. Existe un registro con indicación de características, definición de funciones y usuarios de servicios de intranet de centro (NAS, servidores de centro, nubes privadas de centro,...).
2. El centro tiene establecidos perfiles de usuario protegidos con contraseñas de seguridad en los servicios de intranet de centro: Administrador, profesorado, alumnado e invitados.
3. Se realizan copias de seguridad de datos con periodicidad de los documentos depositados en la intranet.
4. Los servicios de intranet están separados de los servicios de internet.
5. Se realiza un seguimiento del uso y la seguridad de los servicios de intranet.

☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐

SERVICIOS DE INTERNET Y REDES SOCIALES

1. Se analizan los datos antes de almacenarlos o subirlos a servicios de internet.

☐	☐	☐
--------------------------	--------------------------	--------------------------

2. El centro tiene registrados todos los servicios de internet que utiliza, e identificado el responsable de cada servicio, así como registro de las cuentas y contraseñas del centro.
3. Se conocen los contratos y las condiciones de los servicios que se utilizan el centro y es aplicable en la legislación española.
4. El centro tiene registrados todos los servicios de internet que utiliza, e identificado el responsable de cada servicio, así como registro de las cuentas y contraseñas del centro.
5. La localización del almacenamiento físico de los datos se encuentra preferentemente en el Espacio Económico Europeo, o en empresas que han suscrito los principios del Puerto Seguro.
6. Los servicios de internet garantizan la integridad de los datos, y evitan el acceso de personal no autorizado.
7. Se ha comprobado que datos proporcionados a un servicio de internet no son cedidos a terceros proveedores.
8. Los servicios de internet permiten recuperar toda la totalidad de los datos en caso de que se produzcan incidencias de seguridad.
9. Los servicios de internet garantizan el borrado seguro de datos.
10. Las plataformas de aprendizaje que utiliza el centro permiten controlar los datos que se visualizan de los alumnos y en caso contrario se ha solicitado el consentimiento de los usuarios.
11. Se han solicitado permiso a los alumnos o padres para proporcionar los datos de carácter personal que permiten el acceso a las plataformas de aprendizaje o servicios de internet de terceros
12. En períodos vacacionales se revisan los perfiles, se eliminan permisos y servicios que no se utilicen.
13. Se hace un seguimiento de los servicios de internet en momentos vacacionales para controlar las posibles incidencias.
14. Los datos de carácter personal dispuestos en servicios de internet se suben encriptados.
15. El centro controla los materiales depositados en servicios de internet, y se respetan los derechos de autor y de distribución.
16. El centro tiene documentados los criterios de uso y los perfiles de los usuarios de los distintos servicios, así como las funciones de cada una de ellos.

☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐

FORMACIÓN Y CONCIENCIACIÓN

1. El centro desarrolla planes de formación y concienciación sobre el uso seguro de los equipos, redes y servicios de internet para el profesorado y personal no docente.
2. El centro integra objetivos y procesos de aprendizaje sobre el uso seguro de las tecnologías en el currículo escolar.
3. El Reglamento de Régimen Interior recoge los procesos y actuaciones a aplicar en el caso de uso inadecuado e incidencia en dispositivos y servicios.
4. El Reglamento de Régimen Interior contempla protocolos de actuación para hacer frente a las incidencias de seguridad.
5. El centro dispone de un Plan TIC de centro coordinado, evaluado, actualizado y aplicado actualmente en el centro.

☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐
☐	☐	☐

6. El Plan TIC de centro hace referencia a la incorporación de la seguridad digital en el currículum. De este modo, el profesorado toma conciencia de su responsabilidad compartida.
7. Se informa anualmente a todo el profesorado sobre las novedades en seguridad digital.
8. Se insta a los padres a adoptar un papel activo en materia de seguridad digital y a reforzar los mensajes clave.
9. En caso de duda sobre seguridad, el profesorado sabe dónde solicitar orientación.
10. El centro cuenta con un profesor de referencia al que los alumnos pueden consultar sobre temas relacionados con Internet.

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

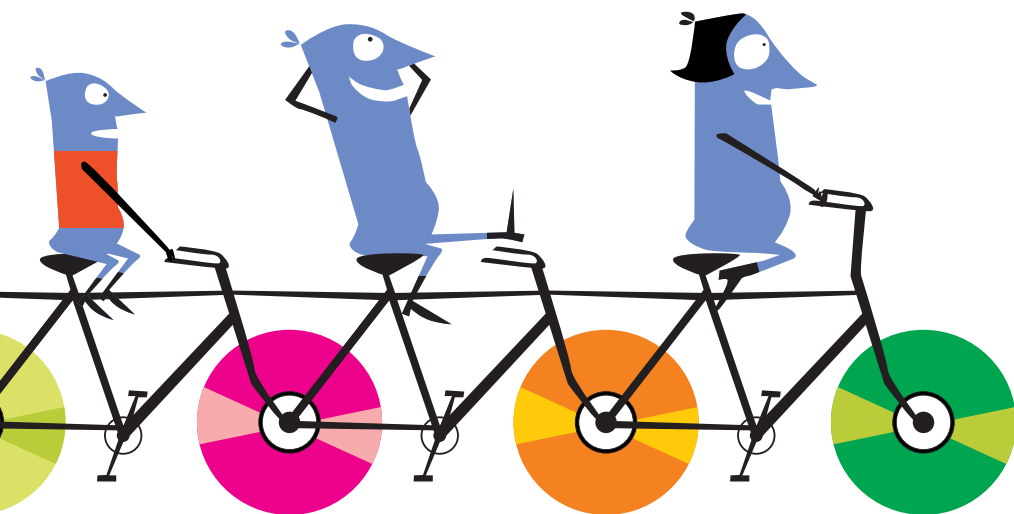
ANEXO III. Protocolos en caso de CIBER ACOSO

PROTOCOLO CIBERACOSO FAMILIAS _____	2
PROTOCOLO CIBERACOSO PROFESORES Y CENTROS ESCOLARES _____	16
PROTOCOLO CIBERACOSO ALUMNOS _____	34



PLAN DE PREVENCIÓN
DEL CIBERACOSO
Y PROMOCIÓN DE LA
NAVEGACIÓN SEGURA
EN CENTROS
ESCOLARES

Guía de la familia.



Junta de
Castilla y León

Miembros del Equipo Interdisciplinar:

Fernando Sánchez-Pascuala Neira (Coordinador)
Viceconsejería de Educación Escolar

Teresa Barroso Botrán
Secretaría General

Jaime Álvarez Rodríguez
D.G. de Planificación, Ordenación e Inspección Educativa

José Luis Martín Sanz
Secretaría General

Antonio Pérez Cano
D.G. de Infraestructuras, Equipamiento y Servicios

Javier Fernández Sáez
D.G. de Calidad, Innovación y Formación del Profesorado

José Ignacio Recio Rivas
D.G. de Planificación, Ordenación e Inspección Educativa

Colaboradores externos:

Francisco Javier Gómez González

Cristina Durlan

Departamento de Sociología y Trabajo Social. Universidad de Valladolid

Apoyo y asistencia: Oficina Técnica Viceconsejería de Educación Escolar

Diseño y creación: Soldegato Laboratorio de Ideas S.L.L.



PLAN DE PREVENCIÓN
DEL CIBERACOSO
Y PROMOCIÓN DE LA
NAVEGACIÓN SEGURA
EN CENTROS
ESCOLARES

Guía de la familia.





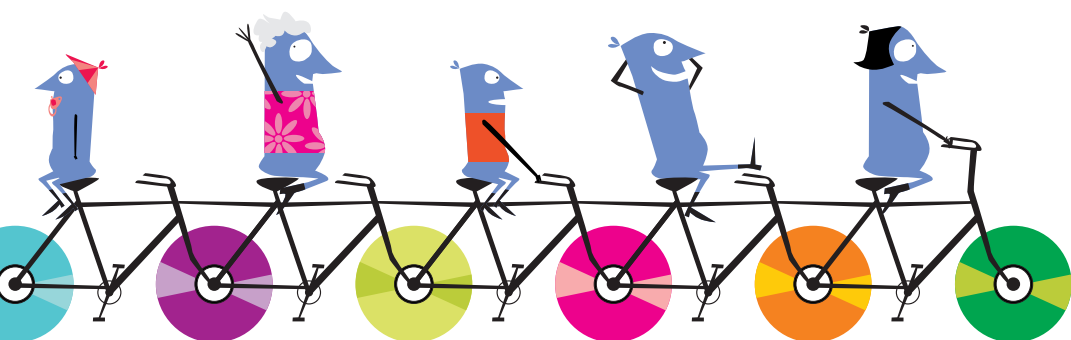
Internet es un tesoro de la información. De hecho, el desarrollo de Internet ha hecho que el mundo sea un sitio más pequeño. Hoy en día, Internet es una ventana al mundo que facilita la búsqueda y el intercambio de información, pero también de ideas y mensajes con personas de distintos sitios del mundo. Y, sin embargo, a pesar de sus múltiples beneficios, como cualquier otra cosa, también tiene sus puntos malos. Los contenidos inapropiados y las facilidades de contacto que ofrece a potenciales infractores son algunas de las desventajas de esta gran herramienta, que afectan, en mayor medida, a los más vulnerables: nuestros hijos/as. Pero prohibirles el acceso a Internet sería cerrarles el acceso a la información.

Por ello, para nosotros, los padres y las madres, es importante conocer y comprender bien esta herramienta para poder entender los riesgos que conlleva y guiar a nuestros hijos/as en su exploración en Internet. A continuación os presentamos, de forma sintética, unas recomendaciones básicas para que, tanto nosotros, como nuestros hijos/as, podamos disfrutar de Internet y sus beneficios.





PLAN DE PREVENCIÓN
DEL CIBERACOSO
Y PROMOCIÓN DE LA
NAVEGACIÓN SEGURA
EN CENTROS
ESCOLARES



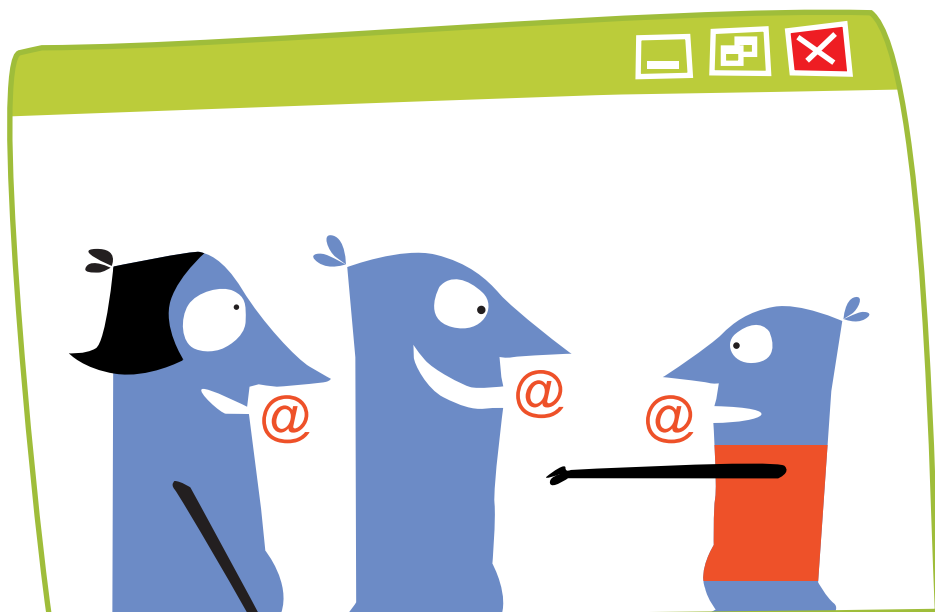
Recomendaciones de carácter general.



■ Aprender a conocer Internet.

Es importante que nosotros mismos nos acerquemos a Internet, aprendiendo a utilizar de manera eficaz y segura esta herramienta. Lo podemos hacer junto a nuestros hijos/as, ya que es la mejor manera de descubrir Internet y de comunicarnos con ellos. Esto ayuda a que establezcamos una relación de confianza mutua.





■ El fomento del diálogo y la comunicación.

Es fundamental fomentar una relación de dialogo con nuestros hijos/as sobre los beneficios y los peligros de Internet. Esto les ayudará a discriminar entre los distintos tipos de información que ofrece esta realidad, y también a respetar a los demás usuarios.





■ La importancia de los datos personales.

Enséñale a tu hijo/a la importancia de sus datos personales y de la privacidad de los mismos, ya que representan una información de carácter muy vulnerable que puede ser utilizada en su contra.





■ La seguridad de tu equipo informático.

Tener una buena seguridad informática en el equipo es una de las reglas esenciales. El antivirus, los filtros de control de acceso a la red y los programas de control parental están entre las herramientas informáticas más utilizadas en este sentido. También es recomendable hablar con el centro educativo sobre la política de prevención que se sigue y pedir consejo sobre cómo actuar.





■ La importancia de las normas de utilización.

Para asegurar un buen uso de Internet, es importante que establezcamos con nuestros hijos/as unas normas básicas y claras sobre la utilización de Internet, especialmente respecto al tiempo de uso (de día y no de noche). Es fundamental que Internet no se convierta en una actividad extraescolar predominante. Hay que fomentar un uso equilibrado de esta herramienta, y no olvidar las otras actividades. Por otro lado, es necesario habilitar una zona de uso común de Internet, para facilitar la supervisión del tiempo de uso, pero también de las situaciones de ciberacoso.



■ ¿Qué hacer en situaciones de ciberacoso?



Acude al centro escolar en cuanto tengas indicios, o simplemente sospechas, de que tu hijo/a está sometido a actuaciones de maltrato o agresiones.

Intenta hablar con tu hijo/a e indaga sobre los indicios que observas. Explícale que vas a acudir al centro escolar y que tu intención es buscar una colaboración con el centro para intervenir en el cese del maltrato.

Si existe un alto riesgo para tu hijo/a, dirígete al centro educativo y ponte en contacto con el tutor o, en su caso, con la jefatura de estudios, la dirección o el departamento de orientación del centro e infórmales de tus inquietudes.

En caso de que tu hijo/a sea víctima de una agresión muy grave, si observas que aumenta su miedo, o que se produce un rebrote de las agresiones o que éstas no cesan a pesar de la intervención escolar, comunícalo al centro y, dependiendo del nivel de riesgo, indícales tu intención de denunciarlo en otras instancias. Los incidentes constitutivos de delito pueden ser denunciados a la policía, a la guardia civil o en la línea de denuncia anónima www.protegeles.com.

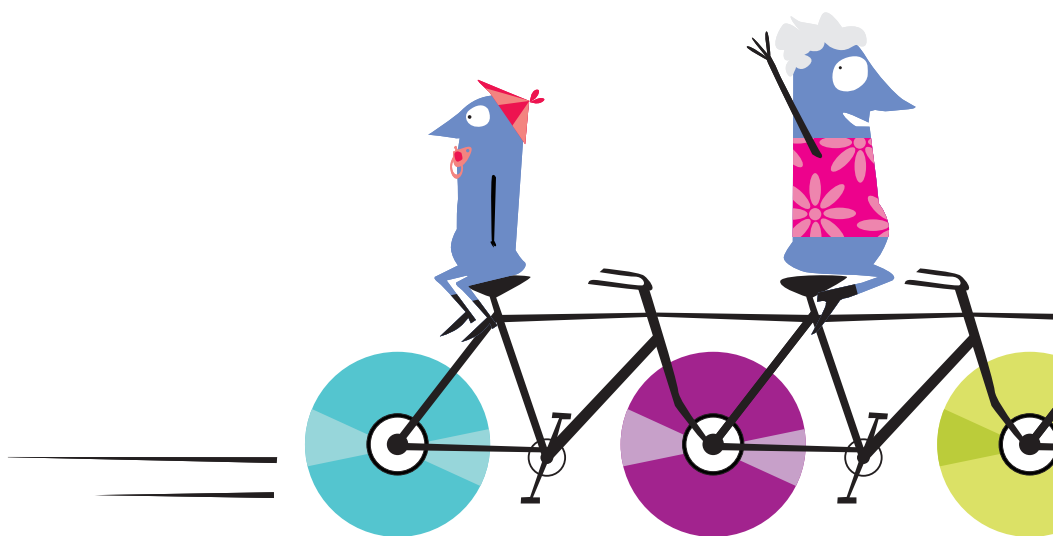




Recuerda que Internet tiene muchas facetas positivas. Es un instrumento que puede ser muy divertido y muy útil.

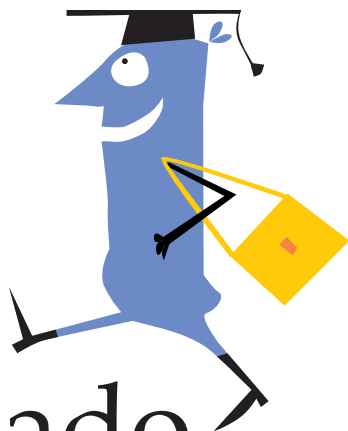
A través de él nuestros hijos/as buscan información para realizar trabajos escolares, conocen gente de lugares distintos del mundo y aprenden cosas nuevas. Es, por excelencia, la herramienta del progreso social hoy en día. Por ello, estas recomendaciones deben representar una pequeña parte de su educación con respecto al buen uso de los medios informáticos. Todo ello se debe complementar con el trabajo de los centros educativos y, por tanto, de los docentes, para asegurar una utilización apropiada de las Nuevas Tecnologías.







PLAN DE PREVENCIÓN
DEL CIBERACOSO
Y PROMOCIÓN DE LA
NAVEGACIÓN SEGURA
EN CENTROS
ESCOLARES



Guía para profesorado y centros escolares.



Junta de
Castilla y León

Miembros del Equipo Interdisciplinar:

Fernando Sánchez-Pascuala Neira (Coordinador)
Viceconsejería de Educación Escolar

Teresa Barroso Botrán
Secretaría General

Jaime Álvarez Rodríguez
D.G. de Planificación, Ordenación e Inspección Educativa

José Luis Martín Sanz
Secretaría General

Antonio Pérez Cano
D.G. de Infraestructuras, Equipamiento y Servicios

Javier Fernández Sáez
D.G. de Calidad, Innovación y Formación del Profesorado

José Ignacio Recio Rivas
D.G. de Planificación, Ordenación e Inspección Educativa

Colaboradores externos:

Francisco Javier Gómez González

Cristina Durlan

Departamento de Sociología y Trabajo Social. Universidad de Valladolid

Apoyo y asistencia: Oficina Técnica Viceconsejería de Educación Escolar

Diseño y creación: Soldegato Laboratorio de Ideas S.L.L.



PLAN DE PREVENCIÓN
DEL CIBERACOSO
Y PROMOCIÓN DE LA
NAVEGACIÓN SEGURA
EN CENTROS
ESCOLARES

Guía para profesorado y centros escolares.



La utilización de Internet como herramienta educativa conlleva una gran diversidad de beneficios. Hoy en día, la clave de la educación radica, por un lado, en el fomento de la competencia digital tanto de los alumnos, como de los profesores. Por ello, los profesores tienen una doble responsabilidad a la hora de educar en el uso correcto de las Nuevas Tecnologías: mantenerse informados y siempre actualizados en esta materia y fomentar un uso seguro de las Nuevas Tecnologías en los centros educativos.

Por ello, a continuación se presenta unas recomendaciones básicas para el uso de las Nuevas Tecnologías en los centros educativos:

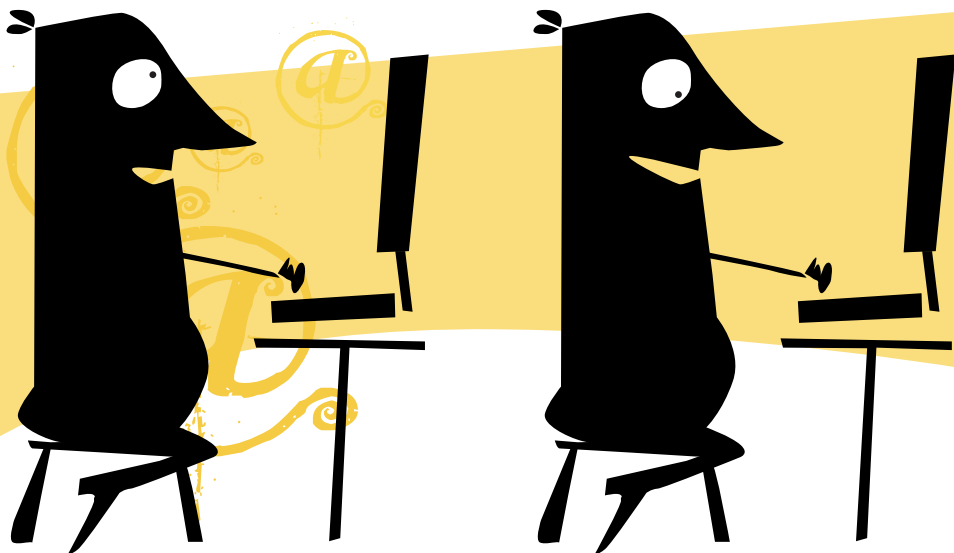




PLAN DE PREVENCIÓN
DEL CIBERACOSO
Y PROMOCIÓN DE LA
NAVEGACIÓN SEGURA
EN CENTROS
ESCOLARES



Recomendaciones para el centro educativo.



■ La importancia de la formación.

Es importante que en el centro educativo exista una política de formación permanente en esta materia, tanto de los alumnos, como de los profesores. Esta formación ayuda a conocer todos los conceptos relacionados con los riesgos en la red, sus consecuencias y la forma de actuar frente a estos peligros.



■ La necesidad de un plan de educación en seguridad informática.



Es recomendable que se cuente con un plan de educación en seguridad informática. De esta forma, al tiempo que se aprende a utilizar las Nuevas Tecnologías, se toma conciencia de los beneficios y los potenciales peligros que existen en la red.



■ El plan de seguridad de los equipos informáticos.

Es importante contar con un buen plan de seguridad de los equipos informáticos, ya que es uno de los pasos básicos para una utilización segura de las Nuevas Tecnologías.





■ Los códigos de buenas prácticas de utilización de los equipos informáticos.

Es fundamental elaborar y utilizar un código de buenas prácticas de utilización de los equipos informáticos en los centros. Estas normas de uso se deberían utilizar tanto como material didáctico, como reglamento básico de uso de los equipos en las aulas de informática.





■ Las formas de respuesta ante las situaciones de ciberacoso.

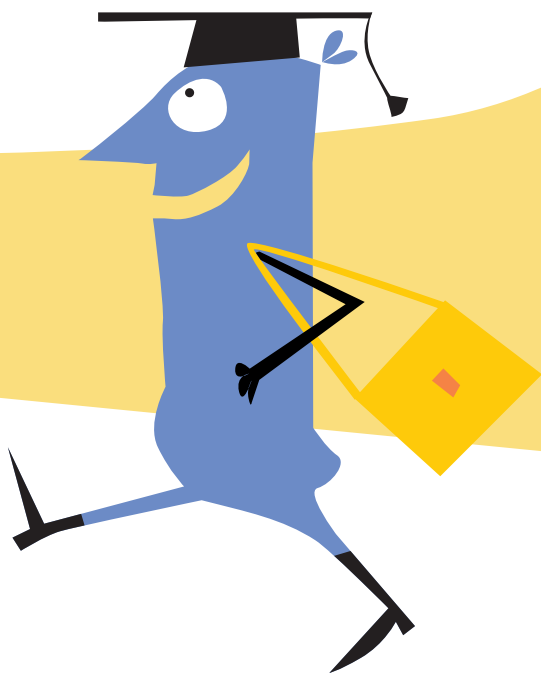
El ciberacoso es una nueva forma de acoso escolar y se refiere a diferentes tipos de acoso (racista, homofóbico, o acoso relacionado con discapacidades, etc.). La diferencia es que el acoso se realiza a través de las Nuevas Tecnologías. En este sentido, las formas de respuesta ante las situaciones de ciberacoso se guían a través de la normativa específica de convivencia escolar en la comunidad de Castilla y León. Por ello, es importante que todos los colectivos de la comunidad educativa conozcan el procedimiento sancionador de aplicación para el desarrollo del DECRETO 51/2007, de 17 de mayo, por el que se regulan los derechos y deberes de los alumnos y la participación y los compromisos de las familias en el proceso educativo, y se establecen las normas de convivencia y disciplina en los Centros Educativos de Castilla y León.

En el portal de Educación de la Junta de Castilla y León, se ha puesto a disposición de la comunidad educativa información, por una parte, sobre los procedimientos de actuación de acuerdo con dicho Decreto y, por otra, sobre los diferentes programas de apoyo, incluida la asistencia legal, para el profesorado y alumnado que pueda estar sufriendo alguna situación de posible ciberacoso.





PLAN DE PREVENCIÓN
DEL CIBERACOSO
Y PROMOCIÓN DE LA
NAVEGACIÓN SEGURA
EN CENTROS
ESCOLARES



Recomendaciones para los profesores.

■ La importancia de los datos personales.



Intercambiar nombres, fotos, direcciones y teléfonos, etc. es a veces necesario, pero también es arriesgado y debes tomar muchas precauciones.

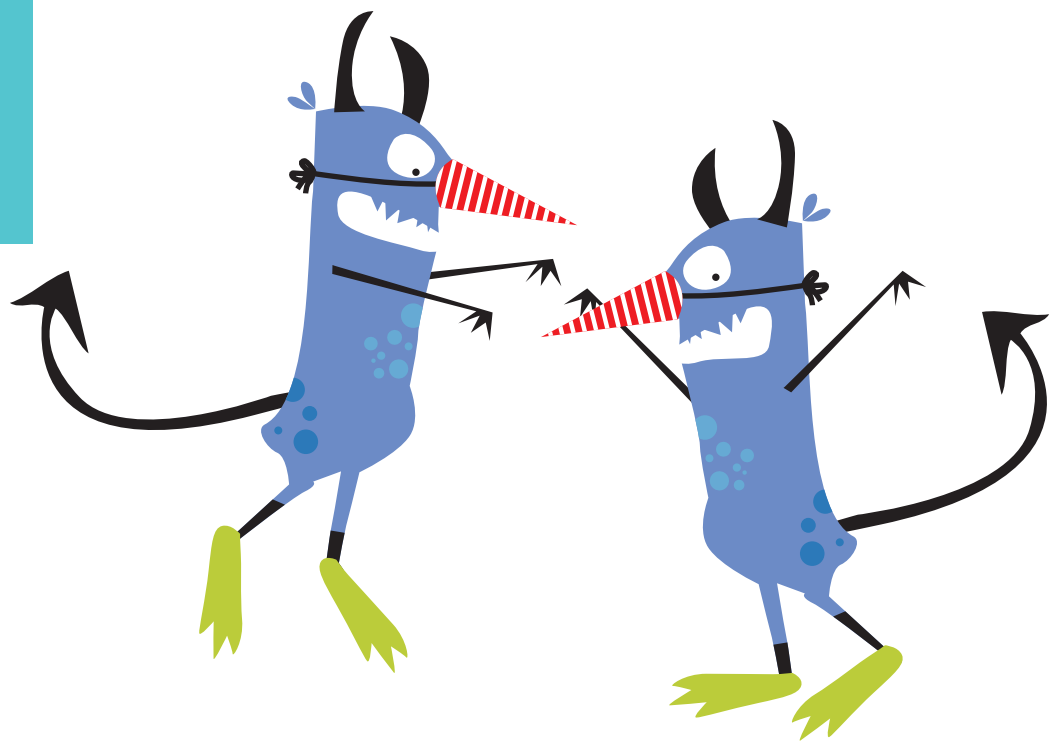


■ Ignora el spam.



El spam, ya sabes, correo basura, sms basura, mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades, cada vez es más frecuente. Escapa del spam, huye, es una pesadilla que puedes evitar, por ejemplo, no pinchando nunca en los correos electrónicos publicitarios no solicitados.





■ Los virus acechan constantemente.

Además de escapar del spam, no accedas a programas ni archivos de desconocidos. Si lo haces tienes grandes posibilidades de que los virus y programas espía accedan a tu ordenador y, además, puedes propagar la infección a otros.



■ ...además de todo lo anterior...

Es importante tener en cuenta las normas de uso que haya dispuesto el centro y especialmente las de control de los procesos de inicio y finalización del trabajo con los alumnos.

Los ordenadores son una herramienta básica para trabajar en las actividades didácticas y de apoyo al aula.

Es esencial ayudar a los alumnos y orientarles sobre el uso adecuado de Internet.

Si no existen en el reglamento de régimen interior del centro, debes establecer unas pautas de uso de los equipos informáticos por parte de cualquier miembro de la comunidad educativa, especialmente por el profesorado y alumnado.

Presta ayuda y colaboración a los profesores y orientales sobre el uso adecuado de Internet.



■ Enlaces de interés.

Agencia de Calidad de Internet

www.iqua.net

Asociación ACPI

www.asociacion-acpi.org

Asociación de Clasificación de Contenidos de Internet (ICRA)

www.fosi.org/icra

Asociación dedicada a la seguridad infantil en Childnet International

www.childnet-int.org

Brigada de Investigación Tecnológica

www.policia.es/bit

Ciberbullying: Acoso entre menores por medio de Nuevas Tecnologías

www.ciberbullying.net

International Association of Internet Hotlines (INHOPE)

www.inhope.org/en/index.html

Internet sin Acoso

www.internetsinacoso.com

Internet Sin Riesgos.

www.internetsinriesgos.es/index.html

Insafe

www.saferinternet.org/ww/en/pub/insafe/index.htm

Instituto Nacional de Tecnologías de la Comunicación

www.inteco.es

Pantallas Amigas

www.pantallasamigas.net

Programa Safer Internet de la Unión Europea

ec.europa.eu/information_society/activities/sip/index_en.htm

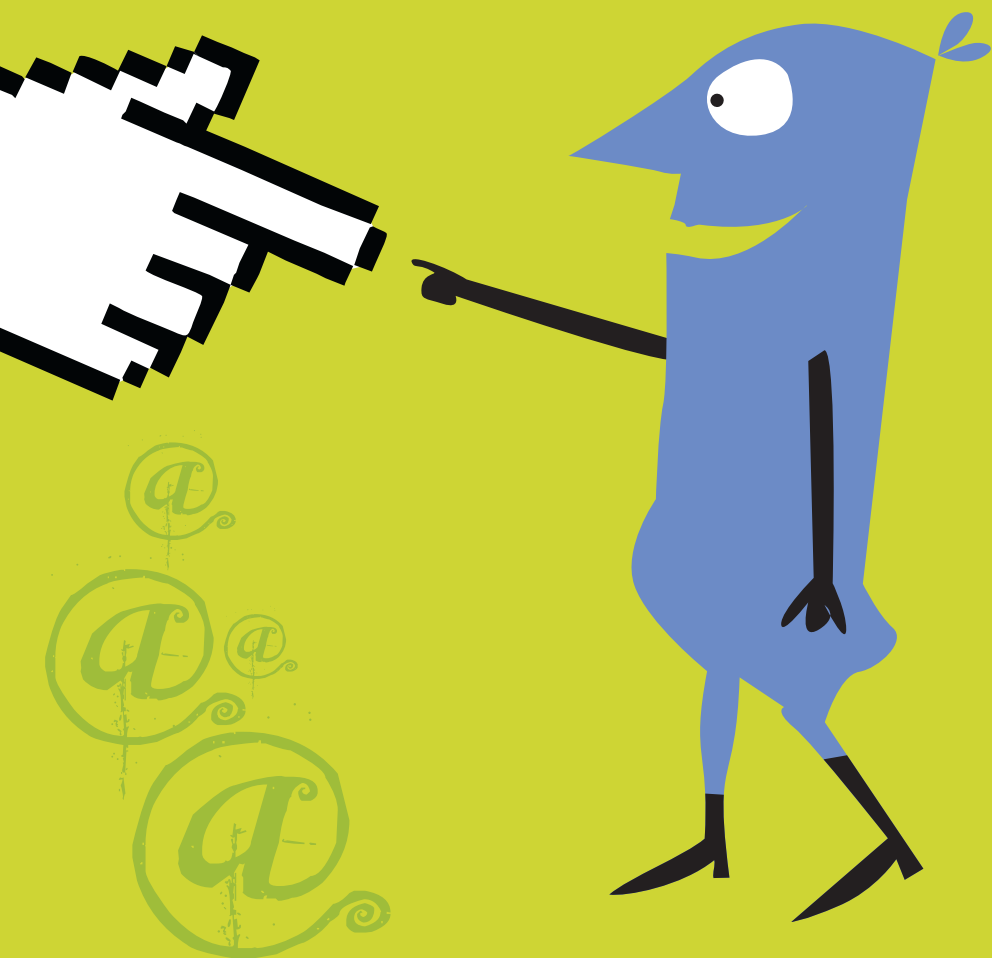
Protégeles: Línea de denuncia

www.protegeles.com

Safer Internet Programme (Comisión Europea):

ec.europa.eu/information_society/activities/sip/index_en.htm









PLAN DE PREVENCIÓN
DEL CIBERACOSO
Y PROMOCIÓN DE LA
NAVEGACIÓN SEGURA
EN CENTROS
ESCOLARES

Guía de los alumnos.



Junta de
Castilla y León



Miembros del Equipo Interdisciplinar:

Fernando Sánchez-Pascuala Neira (Coordinador)
Viceconsejería de Educación Escolar

Teresa Barroso Botrán
Secretaría General

Jaime Álvarez Rodríguez
D.G. de Planificación, Ordenación e Inspección Educativa

José Luis Martín Sanz
Secretaría General

Antonio Pérez Cano
D.G. de Infraestructuras, Equipamiento y Servicios

Javier Fernández Sáez
D.G. de Calidad, Innovación y Formación del Profesorado

José Ignacio Recio Rivas
D.G. de Planificación, Ordenación e Inspección Educativa

Colaboradores externos:

Francisco Javier Gómez González

Cristina Durlan

Departamento de Sociología y Trabajo Social. Universidad de Valladolid

Apoyo y asistencia: Oficina Técnica Viceconsejería de Educación Escolar

Diseño y creación: Soldegato Laboratorio de Ideas S.L.L.



PLAN DE PREVENCIÓN
DEL CIBERACOSO
Y PROMOCIÓN DE LA
NAVEGACIÓN SEGURA
EN CENTROS
ESCOLARES

Guía de los alumnos.



Internet es una herramienta muy divertida y útil, ya que a través de ella puedes:

Buscar información para hacer tus trabajos.

Divertirte jugando.

Aprender muchas cosas nuevas.

Conocer y comunicarte con personas de lugares distintos.

Y, sin embargo, **Internet** es también un sitio al que tiene acceso todo el mundo, tanto buenas como malas personas.

Por ello, existen unas reglas que tienes que tener siempre en la mente y respetar a la hora de utilizar **Internet**.



PLAN DE PREVENCIÓN
DEL CIBERACOSO
Y PROMOCIÓN DE LA
NAVEGACIÓN SEGURA
EN CENTROS
ESCOLARES



¿Qué debes hacer
cuando navegas
en Internet?



- Siempre utilizar un nombre secreto. Tus datos personales son sólo tuyos.

A pesar de que sea muy interesante intercambiar nombres, fotos, direcciones y teléfonos, tienes que tener en cuenta que también es muy peligroso y debes tomar muchas precauciones. Lo mejor es no intercambiar tus datos personales por Internet. Por supuesto que esto debes aplicarlo también para tus amigos: no des nunca sus datos sin su permiso.



■ Habla con tus padres.



Aprende junto a tus padres más sobre Internet y sus beneficios.

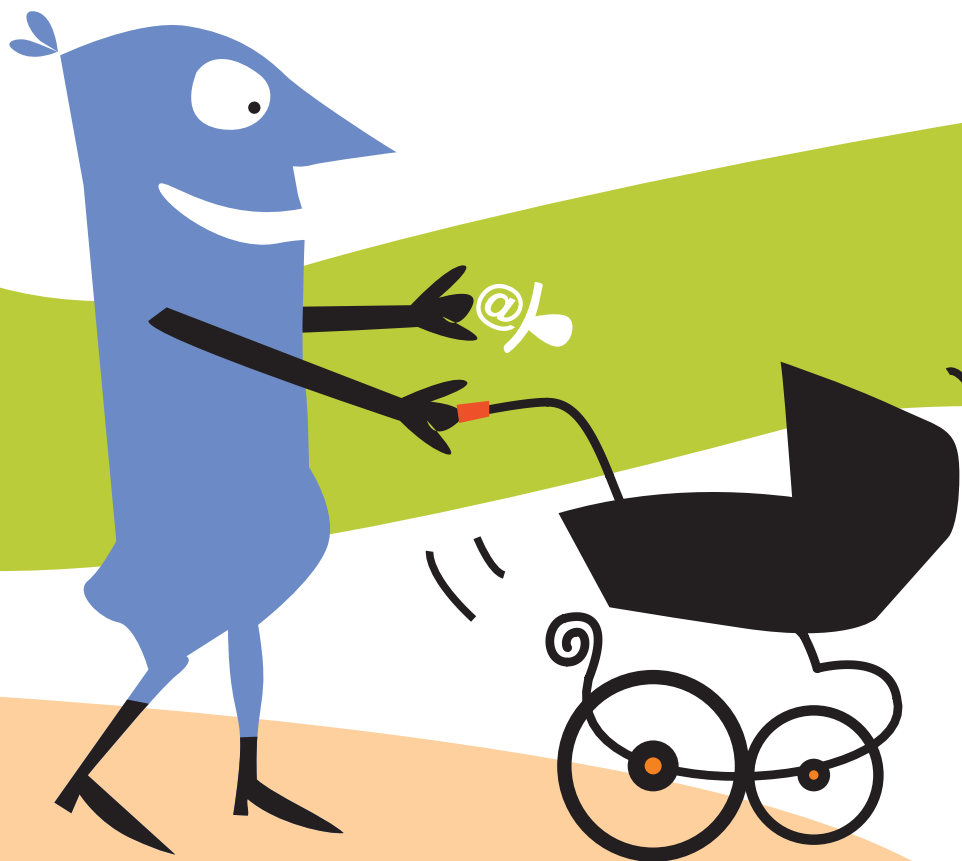
Si hay alguna situación que te molesta, coméntalo con tus padres.

Preséntales los nuevos amigos que has conocido a través de Internet.

Si quieres hacer alguna compra por Internet, coméntalo con ellos.

■ Cuida de tu ordenador.

Utiliza siempre el antivirus para la seguridad de tu ordenador y analiza con él cualquier fichero que descargues.





■ Ignora el spam.

Ya sabes, correo basura, sms basura, mensajes no solicitados (habitualmente de tipo publicitario) enviados en grandes cantidades. Escapa del spam, huye, es una pesadilla que puedes evitar no pinchando nunca en los correos electrónicos publicitarios no solicitados.

- Demuestra que sabes utilizar Internet.



Demuestra tu inteligencia y educación. No provoques o insultes a otros usuarios. No te dejes influir por otros, aceptando cosas que te proponen y que están mal. Recuerda las normas de uso de Internet: no escribir en mayúsculas (equivale a gritar), no publiques datos falsos, no utilices tacos, etc.



PLAN DE PREVENCIÓN
DEL CIBERACOSO
Y PROMOCIÓN DE LA
NAVEGACIÓN SEGURA
EN CENTROS
ESCOLARES



¿Qué
NO debes hacer
cuando navegas
en Internet?

- Nunca te fíes de los extraños. Un desconocido no es tu amigo o tu amiga.



Las apariencias engañan, al menos a veces. Si mantienes relación con un desconocido por Internet, seguirá siendo sólo eso: un desconocido. No te fíes a pesar de que te pueda parecer que es tu amigo o amiga.

■ No acuerdes nunca citas con desconocidos a través de Internet.

Si conoces a alguien en la Red, recuerda el punto anterior: es un desconocido, no quedes nunca a solas con él. Si tienes mucho interés en hacerlo que te acompañe tu madre o tu padre.



■ Recuerda que
Internet no
es un medio
para insultar o
molestar a la gente.

**Internet nos permite
hacer cosas que no nos
atreveríamos a hacer "a
la cara". Sin embargo,
no olvides que el
anonimato no existe. De
todo lo que ocurre en
Internet queda algún
rastros y, ya sabes,
tirando del hilo...**



- No te creas los regalos y los chollos.

Nadie da nada a cambio de nada, en Internet tampoco ocurre esto, no lo olvides.

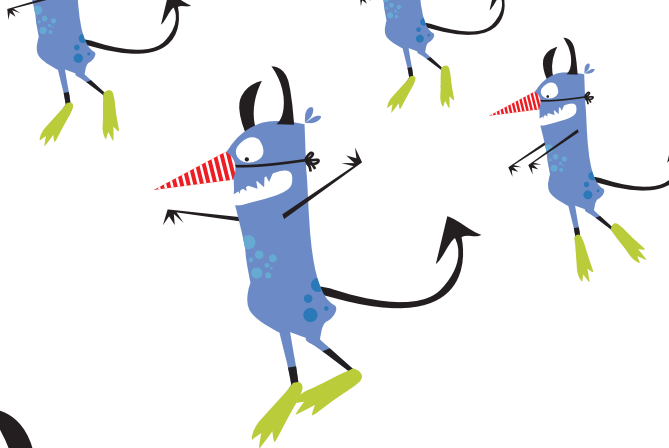
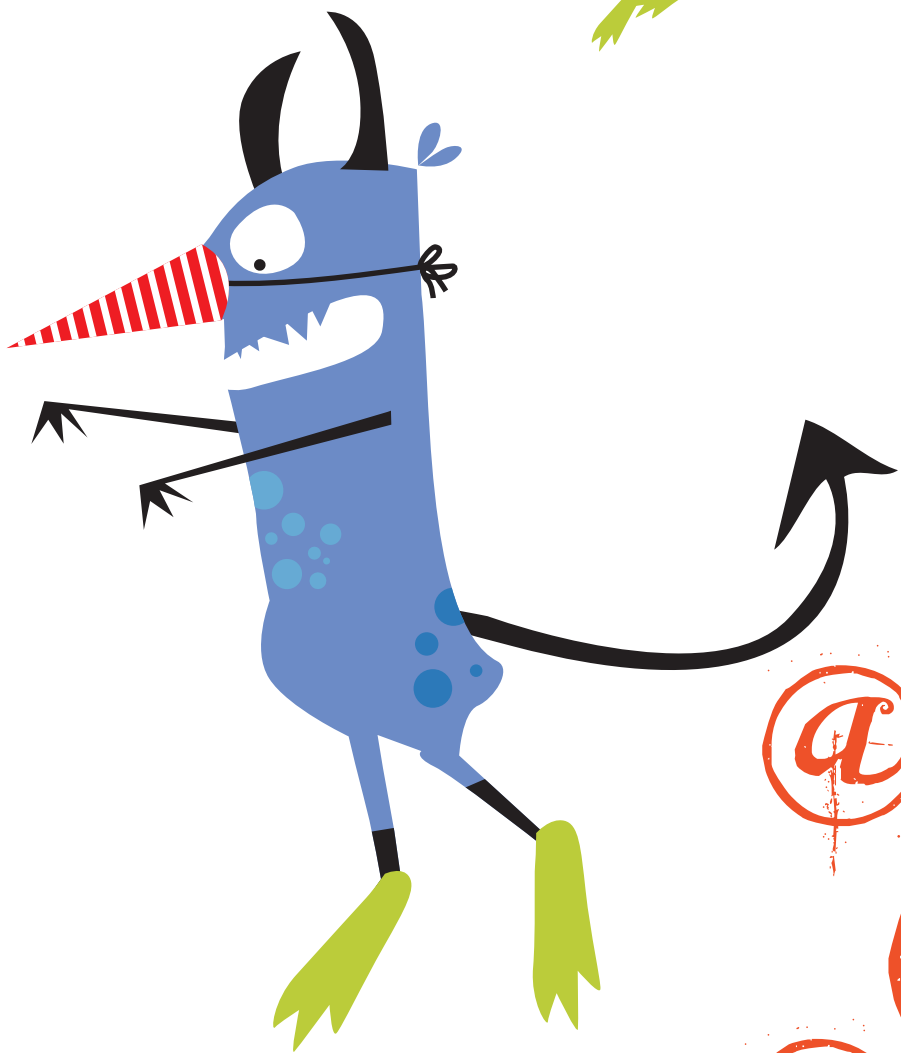


■ Recuerda que los virus acechan constantemente.



Además de escapar del spam, no accedas a programas ni archivos de desconocidos.

Si lo haces tienes grandes posibilidades de que los virus y programas espía accedan a tu ordenador y, además, puedes propagar la infección a todos tus amigos.



Declaración de



Tengo el derecho de sentirme seguro y estar seguro en Internet.

Tengo el derecho de explorar, aprender y disfrutar de todo el contenido dirigido a mí en Internet.

Tengo el derecho de guardar en secreto toda la información sobre mí.

derechos de Internet.

Tengo el derecho de no ser molestado o acosado por los otros.

Tengo el derecho de ignorar los correos y los mensajes de personas que no conozco o en las que no confío.

Tengo el derecho de no rellenar formularios o responder preguntas que encuentro en Internet.

Tengo el derecho de pedir ayuda a mis padres o a un adulto, SIEMPRE.

Tengo el derecho de informar sobre cualquier persona que pienso que está actuando de forma rara o que hace preguntas extrañas.

Tengo el derecho de no sentirme culpable si, mientras utilizo Internet, aparecen cosas molestas en la pantalla.

Tengo el derecho de que la gente me respete en Internet.

■ Enlaces de interés

Estas páginas web te pueden ayudar a descubrir más sobre cómo puedes aprender y divertirte en Internet:

www.educa.jcyl.es

Escritorio virtual con actividades, juegos y recursos educativos.

www.pantallasamigas.net

Iniciativa para la promoción del uso seguro y saludable de Internet y las nuevas tecnologías.

www.enredate.org

Recursos curriculares organizados por bloques de contenido, para todas las edades.

www.ciencianet.com

Diviértete y encuentra cosas curiosas y extrañas sobre la ciencia.

www.disney.es

La página de Disney en español.

www.curiosos.com

Buscador específico

www.wildwebwoods.org

Juego diseñado para entender el funcionamiento de Internet y para enseñarte unas nociones técnicas que te ayudarán a convertirte en un internauta prudente.



www.internetsinriesgos.es/index.html

Te enseña sobre los riesgos de Internet y las formas básicas de protegerte ante cualquier riesgo.

www.educared.net/

Página web de recursos educativos.

www.exprimelared.com/

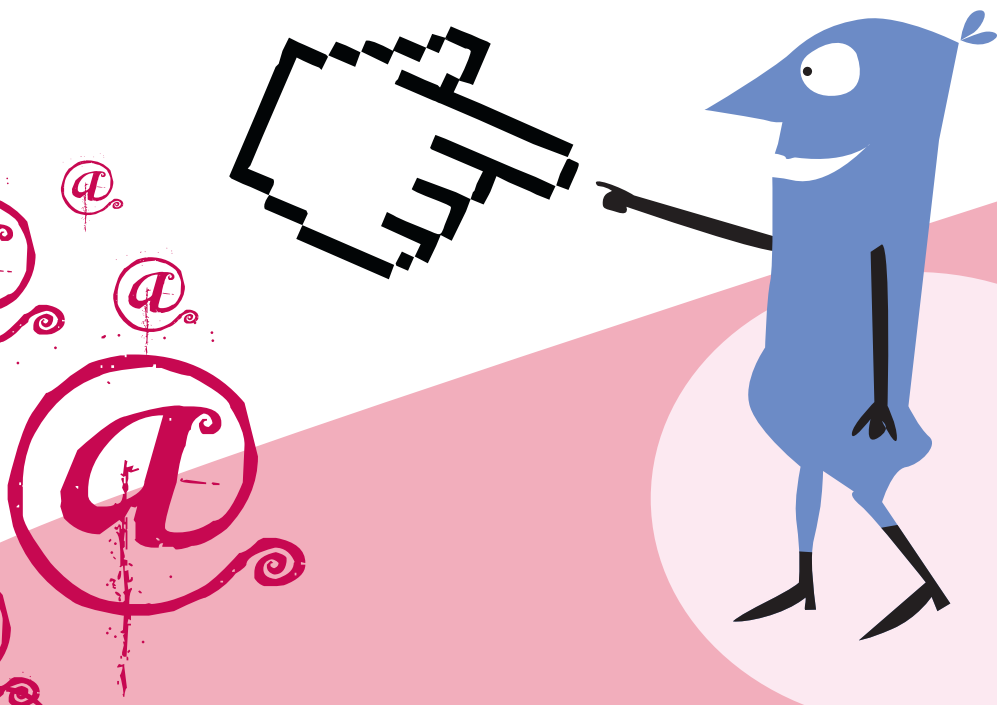
Página web que te enseña como disfrutar de todas las ventajas que te ofrece Internet.

chaval.red.es/index.jsp

Página web con información específica dirigida a los jóvenes.

www.micueva.com/

Aprende a crear tu propio espacio en Internet.





**Junta de
Castilla y León**