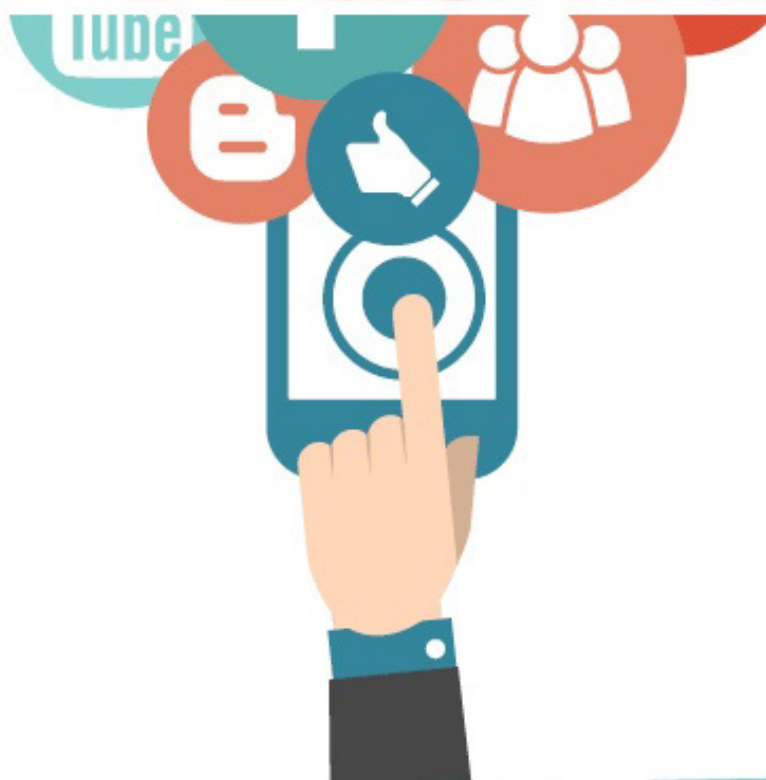




Protocolo de uso de Internet



PROTOCOLO DE USO DE INTERNET

ÍNDICE

1. Introducción	<u>3</u>
2. Ámbitos de aplicación	<u>3</u>
3. Principios generales	<u>3</u>
4. Derechos y deberes de los usuarios	<u>4</u>
5. Directrices de seguridad	<u>5</u>
6. Uso de redes sociales	<u>9</u>
7. Sanciones	<u>10</u>
8. Formación	<u>10</u>
9. Revisión	<u>10</u>

PROTOCOLO DE USO DE INTERNET

Curso 2025/26

1. INTRODUCCIÓN

El presente protocolo establece las normas y pautas que deben seguir todos los miembros de la comunidad educativa del IES Eduardo Linares Lumeras (alumnos, profesores, personal administrativo, entre otros) en relación con el uso de internet dentro de las instalaciones del centro.

El objetivo principal es fomentar un uso seguro, responsable y educativo de las Tecnologías de la Información y la Comunicación (TIC) y de las Tecnologías de Aprendizaje y Conocimiento (TAC), garantizando así un entorno digital que favorezca el aprendizaje, la creatividad y el respeto mutuo.

2. ÁMBITO DE APLICACIÓN

Este protocolo es de aplicación para todos los usuarios de internet en el centro educativo, sin importar el dispositivo que se utilice o el tipo de conexión (red interna o wifi).

3. PRINCIPIOS GENERALES

PRINCIPIOS GENERALES

USO EDUCATIVO

El uso principal de internet debe estar orientado a fines educativos y de apoyo a las actividades académicas. Se debe priorizar el acceso a recursos y herramientas que fomenten el aprendizaje y el desarrollo de habilidades digitales.

RESPETO

Todos los usuarios deben actuar con respeto hacia los demás, evitando cualquier forma de discriminación, acoso, *ciberbullying*, o comportamientos que puedan dañar la dignidad de otros miembros de la comunidad educativa. Esto incluye el respeto por las opiniones, creencias y diversidad cultural de todos.

PRINCIPIOS GENERALES

RESPONSABILIDAD

Cada usuario es responsable de sus acciones en internet y debe ser consciente de las posibles consecuencias de un uso inadecuado de la misma. Esto implica hacer un uso consciente y crítico de la información que se encuentra en la red, verificando la veracidad de las fuentes y evitando la difusión de información falsa.

SEGURIDAD

Es fundamental garantizar la seguridad de los datos personales y evitar el acceso a contenido inapropiado o peligroso. Esto implica el uso de contraseñas seguras, no compartir información personal sin autorización, y estar alerta ante posibles amenazas como *phishing* o *malware*.

PRIVACIDAD

Se debe respetar la privacidad de los demás usuarios y proteger la información personal. Está prohibida la difusión de datos personales de terceros sin su consentimiento explícito. Además, se debe ser consciente de los derechos de privacidad y confidencialidad en el entorno digital.

4. DERECHOS Y DEBERES DE LOS USUARIOS

DERECHOS Y DEBERES DE LOS USUARIOS

DERECHOS

Los usuarios de internet en el centro educativo tienen derecho a:

1. Acceder a la información y los recursos educativos disponibles en internet, siempre que estos sean apropiados y estén autorizados por el centro.
2. Utilizar las herramientas informáticas y digitales proporcionadas por el centro para el desarrollo de sus actividades académicas.
3. Expresar sus ideas y opiniones de manera respetuosa y constructiva en los espacios digitales habilitados por el centro para tal fin.
4. Recibir formación y orientación adecuadas para el uso seguro y responsable de internet y las tecnologías de la información y la comunicación.
5. Que se respete su privacidad y la confidencialidad de sus datos personales, de acuerdo con la normativa vigente.

DERECHOS Y DEBERES DE LOS USUARIOS

DEBERES

Los usuarios de internet en el centro educativo tienen el deber de:

1. Utilizar internet de forma responsable, ética y acorde con los fines educativos establecidos por el centro.
2. Respetar y cumplir las normas, políticas y directrices del centro respecto al uso de las tecnologías de la información y la comunicación.
3. Proteger sus datos personales y los de los demás, actuando con cautela en la divulgación de información en línea y respetando la privacidad de otros usuarios.
4. Abstenerse de utilizar internet para actividades ilegales, perjudiciales o que puedan comprometer la integridad de otras personas o los sistemas informáticos del centro.
5. Informar de inmediato a un responsable del centro si se encuentra con contenido inapropiado o cualquier situación de riesgo en internet.
6. Hacer un uso eficiente y responsable de los recursos tecnológicos del centro, evitando su deterioro o uso indebido.
7. Respetar los derechos de autor y la propiedad intelectual en todas las actividades que impliquen el uso de internet.
8. Colaborar en la creación de un entorno digital seguro y positivo para toda la comunidad educativa.

5. DIRECTRICES DE SEGURIDAD

DIRECTRICES DE SEGURIDAD

USO EDUCATIVO

El uso principal de internet debe estar orientado a fines educativos y de apoyo a las actividades académicas. Se debe priorizar el acceso a recursos y herramientas que fomenten el aprendizaje y el desarrollo de habilidades digitales.

DIRECTRICES DE SEGURIDAD

CONTRASEÑAS

- Es esencial utilizar combinaciones seguras que incluyan mayúsculas, minúsculas, números y símbolos.
- Las contraseñas deben cambiarse regularmente, al menos cada tres meses, y nunca deben compartirse con nadie, ni siquiera con amigos cercanos.
- Es importante usar contraseñas diferentes para cada cuenta o servicio y activar la autenticación de dos factores siempre que sea posible.

PROTECCIÓN CONTRA MALWARE

- Todos los dispositivos deben contar con software antivirus actualizado.
- Se debe evitar abrir archivos adjuntos de correos electrónicos sospechosos o de remitentes desconocidos, así como descargar software de fuentes no confiables.
- Es recomendable realizar escaneos periódicos de los dispositivos en busca de *malware*.

NAVEGACIÓN SEGURA

- Para una navegación segura, es importante verificar que las conexiones sean seguras (<https://>) antes de introducir datos personales o contraseñas.
- Se debe ser cauteloso al hacer clic en enlaces, especialmente en correos electrónicos o mensajes de texto.
- Al usar dispositivos compartidos, es aconsejable utilizar el modo de navegación privada y cerrar sesión en todas las cuentas al terminar.

ACTUALIZACIONES DE SOFTWARE

Las actualizaciones de software son fundamentales para la seguridad. Se debe mantener el sistema operativo y todas las aplicaciones actualizadas con las últimas versiones de seguridad, configurando las actualizaciones automáticas siempre que sea posible.

PHISHING Y ESTAFAS EN LÍNEA

Es crucial estar alerta ante intentos de *phishing* y estafas en línea. Hay que verificar la autenticidad de los remitentes antes de proporcionar cualquier información y no responder a solicitudes de información personal por correo electrónico o mensajes de texto.

GESTIÓN DE LA INFORMACIÓN

La gestión adecuada de la información incluye realizar copias de seguridad regulares, utilizar servicios de almacenamiento en la nube aprobados por el centro y eliminar de forma segura los archivos y datos confidenciales cuando ya no sean necesarios.

DIRECTRICES DE SEGURIDAD

DISPOSITIVOS MÓVILES

Para los dispositivos móviles, se debe configurar un código de acceso o huella dactilar, activar la opción de borrado remoto en caso de pérdida o robo, y no dejarlos desatendidos y sin bloquear.

COMUNICACIÓN DE INCIDENTES

Es importante comunicar de inmediato a jefatura de estudios o al responsable designado cualquier incidente de seguridad, pérdida de datos o comportamiento sospechoso en línea.

FORMACIÓN CONTINUA

La formación continua es esencial. Todos los miembros de la comunidad educativa deben participar en las sesiones de formación sobre seguridad en línea proporcionadas por el centro y mantenerse informados sobre las últimas amenazas y mejores prácticas de seguridad en internet.

El cumplimiento de estas medidas de seguridad es responsabilidad de todos los usuarios y es esencial para mantener un entorno digital seguro en el centro educativo.

6. USOS PERMITIDOS Y NO PERMITIDOS

USOS PERMITIDOS Y NO PERMITIDOS

USOS PERMITIDOS

Se considera uso permitido de internet en el centro educativo:

1. **Realización de tareas académicas e investigación.** Utilización de internet para buscar información, realizar trabajos escolares y acceder a plataformas educativas autorizadas por el centro.
2. **Consulta de recursos educativos.** Acceso a bibliotecas digitales, enciclopedias en línea y otros recursos digitales que contribuyan al aprendizaje y al desarrollo académico.
3. **Comunicación institucional.** Utilización de correos electrónicos institucionales, foros educativos y plataformas autorizadas para la interacción y colaboración en proyectos académicos.
4. **Acceso a plataformas educativas.** Uso de sistemas de gestión de aprendizaje, aplicaciones educativas y otros recursos digitales proporcionados o autorizados por el centro.
5. **Uso de herramientas colaborativas.** Participación en proyectos grupales utilizando herramientas como *Google Workspace for Education*, *Microsoft Teams* u otras similares, siempre bajo la supervisión docente y con fines estrictamente educativos.

USOS PERMITIDOS Y NO PERMITIDOS

USOS NO PERMITIDOS

Queda expresamente prohibido el uso de internet en el centro educativo para:

1. **Acceso a contenido inapropiado.** Queda terminantemente prohibido acceder a sitios web que contengan material pornográfico, violento, discriminatorio o que inciten al odio o a conductas ilegales.
2. **Descarga o distribución de material ilegal.** No se autoriza la descarga, distribución o compartición de software, contenido multimedia o cualquier otro tipo de material protegido por derechos de autor sin la debida autorización.
3. **Ciberacoso o conductas intimidatorias.** No se tolera ninguna forma de acoso, amenaza o comportamiento que genere un entorno hostil o intimidante en el espacio digital.
4. **Difusión de información falsa o engañosa.** No se admite la propagación de rumores, noticias falsas o información no verificada que pueda causar confusión o perjuicio a la comunidad educativa.
5. **Suplantación de identidad.** Queda prohibido utilizar las credenciales o la sesión abierta de otro usuario para acceder a sus cuentas, enviar mensajes o realizar cualquier acción en su nombre. Cada usuario es responsable de cerrar su sesión al terminar de usar los equipos informáticos y de mantener la confidencialidad de sus contraseñas.
6. **Acceso no autorizado.** Queda prohibido el intento de acceso no autorizado a sistemas, redes o cuentas ajenas, así como cualquier actividad que pueda comprometer la seguridad de los sistemas informáticos del centro.
7. **Uso de software malicioso.** No se autoriza la creación, uso o distribución de software diseñado para dañar o acceder de forma no autorizada a sistemas informáticos.
8. Utilización de navegadores en modo incógnito, redes privadas (VPN) o cualquier otro método que impida la supervisión del uso de internet.
9. Acceso a contenidos que no estén relacionados con las actividades académicas propuestas.
10. Empleo de herramientas digitales para falsear la identidad, el origen de la conexión o el uso real del dispositivo.

El incumplimiento de estas normas puede conllevar la aplicación de medidas disciplinarias conforme a las normas internas del centro, sin perjuicio de otras responsabilidades legales que pudieran derivarse de dichas acciones.

7. USO DE REDES SOCIALES

USO DE REDES SOCIALES

USO GENERAL

El uso de redes sociales no está permitido en el centro educativo, salvo en casos específicos autorizados y siempre con fines educativos.

USO CON FINES EDUCATIVOS

En ocasiones excepcionales, los profesores pueden proponer el uso de redes sociales como parte de una actividad educativa específica. En estos casos:

- La actividad debe ser aprobada previamente por la dirección del centro.
- Se requiere el consentimiento explícito y por escrito de los padres o tutores legales de los estudiantes participantes.
- El uso se limitará estrictamente a la actividad educativa propuesta y durante el tiempo establecido para la misma.

INTERACCIÓN ENTRE PROFESORES Y ALUMNOS

Se desaconseja la interacción entre profesores y alumnos en redes sociales personales. Es conveniente que cualquier comunicación necesaria se realice a través de los canales oficiales establecidos por el centro educativo.

INCIDENTES FUERA DEL HORARIO ESCOLAR

El centro educativo no tiene competencia directa sobre los conflictos que puedan surgir entre alumnos en redes sociales fuera del horario escolar. Sin embargo:

- Se insta a los padres, madres y tutores legales a supervisar y orientar el uso de redes sociales por parte de sus hijos.
- En caso de detectar situaciones de ciberacoso, amenazas o comportamientos inapropiados que puedan afectar la convivencia en el centro, se recomienda a las familias:
 - a. Documentar la evidencia del incidente.
 - b. Abordar la situación directamente con los padres del otro alumno involucrado, si es posible.
 - c. En casos graves, considerar la posibilidad de denunciar el incidente ante las autoridades competentes.

Si estos comportamientos tienen un impacto directo en la convivencia escolar, el centro podrá tomar medidas educativas y disciplinarias de acuerdo con las normas establecidas en el NOF (Normas de Organización y Funcionamiento)

8. SANCIONES

El incumplimiento de este protocolo puede derivar en sanciones, que se aplicarán según lo establecido en las NOF (Normas de Organización y Funcionamiento) del centro educativo. Las sanciones pueden variar según la gravedad de la infracción, desde una advertencia verbal hasta la adopción de medidas disciplinarias adicionales, incluida la expulsión del centro.

9. FORMACIÓN

El centro educativo se compromete a fomentar la formación continua de todos los miembros de la comunidad educativa en el uso seguro y responsable de internet. Esta formación podrá incluir talleres, charlas y recursos didácticos sobre seguridad digital, privacidad, comportamiento en línea y las herramientas educativas disponibles.

10. REVISIÓN

Este protocolo será revisado de manera periódica para asegurar que se mantiene actualizado con respecto a los avances tecnológicos y las necesidades cambiantes de la comunidad educativa. Cualquier modificación será comunicada a todos los miembros del centro, quienes podrán sugerir mejoras o expresar sus inquietudes durante el proceso de revisión.