Castilla-La Mancha

PROGRAMA CIBERSEGURIDAD

CEIP "LOS OLIVOS"

CABANILLAS DEL CAMPO-GUADALAJARA



CEIP "Los Olivos".
Calle San Juan de la Cruz, nº 2. 19.171
Cabanillas del Campo. Guadalajara.

Tel. y Fax: 949 324457
e-mail: 19008046.cp@edu.jccm.es

http://ceip-losolivos.centros.castillalamancha.es/

ÍNDICE

0. Introducción.

1. Objetivos generales del programa

2. Objetivos específicos.
   a) Para estudiantes.
   b) Para docentes
   c) Para familias
   d) Para el entorno educativo general

3. Áreas clave del Programa de Ciberseguridad Educativa.
   a) Educación y Formación
   b) Políticas y normativas
   c) Herramientas tecnológicas.
   d) Concienciación continua
   e) Evaluación y seguimiento.
   f) Alianzas y recursos externos

0. Introducción.

En la era digital actual, la tecnología se ha convertido en una herramienta fundamental para la educación y el desarrollo personal de los estudiantes. Sin embargo, este entorno digital también presenta riesgos que pueden comprometer la seguridad, la privacidad y el bienestar de los más jóvenes. Conscientes de esta realidad, y con el compromiso de garantizar un entorno educativo seguro y formativo, presentamos el **Programa de Ciberseguridad Educativa**, diseñado específicamente para alumnos de educación infantil y primaria en Castilla-La Mancha.

Este programa nace de la necesidad de preparar a nuestros niños y niñas para interactuar de manera segura y responsable en el entorno digital. A medida que dispositivos como tabletas, ordenadores y smartphones se integran cada vez más en la vida diaria y en el aprendizaje, es fundamental que los estudiantes, junto con sus familias y docentes, adquieran los conocimientos y las habilidades necesarias para prevenir riesgos como el ciberacoso, el acceso a contenidos inapropiados o la suplantación de identidad.

En Castilla-La Mancha, reconocemos la importancia de la educación en valores digitales desde edades tempranas, no solo para proteger a los más pequeños, sino también para fomentar un uso crítico y constructivo de la tecnología. Por ello, este programa abarca una formación integral que combina la sensibilización sobre la ciberseguridad, el desarrollo de competencias digitales y el fortalecimiento de valores como el respeto, la empatía y la responsabilidad en línea.

A través de actividades dinámicas y adaptadas a las distintas etapas educativas, este programa busca empoderar a los estudiantes para que se conviertan en usuarios conscientes y seguros de la tecnología. Además, se incluye una componente de formación específica para el profesorado y las familias, con el objetivo de crear una comunidad educativa preparada para afrontar los retos de la era digital de forma conjunta.

Este proyecto no solo aborda las amenazas tecnológicas actuales, sino que también fomenta una actitud proactiva y resiliente frente a los desafíos futuros. Con ello, pretendemos sentar las bases de una educación digital que prepare a nuestros niños y niñas no solo para protegerse, sino también para aprovechar las enormes oportunidades que el mundo digital les puede ofrecer.

Juntos, trabajaremos por una educación que garantice la seguridad, el bienestar y el desarrollo pleno de nuestros estudiantes en un entorno tecnológico en constante evolución.

1.-Objetivos Generales del Programa de Ciberseguridad Educativa

1. **Promover una cultura de seguridad digital**: Fomentar una actitud responsable, crítica y segura en el uso de las tecnologías digitales entre los estudiantes de educación infantil y primaria.
2. **Prevenir riesgos asociados al entorno digital**: Capacitar a los alumnos, docentes y familias para identificar y mitigar amenazas como el ciberacoso, la exposición a contenidos inapropiados, la pérdida de privacidad y otros riesgos relacionados con la interacción en línea.

3. **Fortalecer las competencias digitales**: Proporcionar a los participantes habilidades esenciales para desenvolverse de manera segura y efectiva en el entorno digital, incluyendo el manejo de contraseñas seguras, la gestión de la información personal y el reconocimiento de prácticas sospechosas.
4. **Desarrollar valores éticos en el entorno digital**: Fomentar principios como el respeto, la empatía, la responsabilidad y la solidaridad en las interacciones en línea, contribuyendo al uso ético y constructivo de la tecnología.
5. **Impulsar la participación de la comunidad educativa**: Integrar a docentes, familias y estudiantes en el diseño e implementación de estrategias de ciberseguridad, promoviendo un enfoque colaborativo para garantizar un entorno digital seguro.
6. **Preparar a los estudiantes para los retos del futuro digital**: Ofrecer herramientas y conocimientos adaptados a su edad para que sean capaces de afrontar los desafíos tecnológicos presentes y futuros con confianza y autonomía.
7. **Promover el uso positivo y creativo de la tecnología**: Orientar a los participantes hacia el aprovechamiento de las oportunidades educativas, sociales y culturales que ofrece el entorno digital, destacando su potencial como herramienta de aprendizaje y desarrollo.

2.- Objetivos Específicos del Programa de Ciberseguridad Educativa

Para los estudiantes:

1. Aprender a identificar y evitar enlaces maliciosos, sitios web inseguros y aplicaciones sospechosas.
2. Comprender la importancia de mantener la privacidad en línea, incluyendo la protección de datos personales y contraseñas.
3. Reconocer señales de ciberacoso y saber cómo actuar ante situaciones de acoso digital.
4. Desarrollar habilidades para evaluar la veracidad de la información encontrada en Internet, evitando la desinformación y las noticias falsas.
5. Adoptar hábitos seguros en el uso de dispositivos tecnológicos, como evitar el uso excesivo de pantallas y aplicar configuraciones de seguridad básicas.
6. Participar en actividades lúdicas y didácticas que fomenten un uso responsable y creativo de las tecnologías digitales.

Para los docentes:

1. Capacitar al profesorado en el uso de herramientas tecnológicas seguras y adaptadas al entorno educativo.
2. Proveer estrategias para la detección temprana de riesgos de ciberseguridad entre los estudiantes, como el ciberacoso o la exposición a contenido inadecuado.
3. Desarrollar materiales pedagógicos que integren la educación en ciberseguridad en el currículo escolar.
4. Facilitar el acceso a recursos y protocolos de actuación ante incidentes relacionados con la ciberseguridad en el entorno escolar.
5. Promover el uso de plataformas educativas seguras y la integración de buenas prácticas digitales en el aula.

Para las familias:

1. Sensibilizar a las familias sobre la importancia de supervisar y guiar el uso de dispositivos tecnológicos en el hogar.
2. Ofrecer talleres prácticos para enseñar a configurar controles parentales y aplicar medidas de seguridad en dispositivos y aplicaciones.
3. Fomentar el diálogo familiar sobre los riesgos y oportunidades del entorno digital, fortaleciendo la confianza y la comunicación entre padres e hijos.
4. Proporcionar recursos para identificar señales de alerta relacionadas con el uso inadecuado de Internet por parte de los niños.
5. Crear una red de apoyo entre familias para compartir experiencias, inquietudes y buenas prácticas en el ámbito de la ciberseguridad.

Para el entorno educativo en general:

1. Establecer un protocolo de actuación ante incidentes de ciberseguridad, incluyendo planes de respuesta a ciberacoso y brechas de privacidad.
2. Implementar un plan de formación continua en ciberseguridad para toda la comunidad educativa, adaptado a las necesidades de cada grupo.
3. Crear campañas de sensibilización periódicas sobre el impacto del uso irresponsable de la tecnología.
4. Realizar evaluaciones periódicas del nivel de ciberseguridad en el centro educativo, identificando áreas de mejora.
5. Promover alianzas con instituciones especializadas en ciberseguridad para enriquecer el programa con recursos actualizados y especializados.

3.- Áreas Clave del Programa de Ciberseguridad Educativa

a) Educación y Formación

Este eje se centra en proporcionar conocimientos y habilidades esenciales a todos los miembros de la comunidad educativa para fomentar un uso seguro y responsable de las tecnologías.

Estudiantes:

- **Talleres prácticos**: Actividades interactivas sobre temas como la creación de contraseñas seguras (actividad en la que los alumnos aprender a crear contraseñas robustas utilizando combinaciones de letras, números y símbolos), la gestión de privacidad en línea y el uso adecuado de las redes sociales. Impartidos por profesionales en la materia. (Taller de Sensibilización sobre ciberseguridad y desinformación: el juego online impartido por Unitel Formación, 1 sesión 6ºEP)
- **Sensibilización sobre ciberacoso**: Sesiones adaptadas por edades para identificar, prevenir y actuar frente al ciberacoso, promoviendo un uso respetuoso y ético de las plataformas digitales. Impartidos por profesionales en la materia. (1 sesión 5º y 6º EP Pto.Omega y Plan Director) (1 sesión para 4º EP Cibervoluntarios).
- **"Ciberacoso**: ¿Qué harías tú?: dinámicas de rol para que los alumnos identifiquen situaciones de acoso en línea y practiquen cómo actuar o buscar ayuda.
- **Formación en ciberseguridad básica**: Enseñanza de conceptos como la detección de fraudes digitales (phishing, malware) y los peligros de descargar contenido desde fuentes no confiables. Impartidos por profesionales en la materia. (Pto.Omega, Plan Director, Cibervoluntarios)

- **Desarrollo de habilidades críticas**: Ejercicios para aprender a evaluar la veracidad de la información en línea y evitar la propagación de noticias falsas.

Docentes:

- **Formación especializada**: Formación en herramientas de control y supervisión de contenido, como configuraciones de seguridad en navegadores y plataformas educativas. .
- **Capacitación en incidentes digitales**: Estrategias o charlas para identificar y abordar casos de ciberacoso, suplantación de identidad o exposición a contenido inapropiado.
- **Recursos pedagógicos**: Acceso a materiales y guías para integrar temas de ciberseguridad en el currículo escolar de manera transversal. Orientaciones sobre el uso de herramientas digitales en el ámbito educativo desde la perspectiva de la protección de datos - INTEF Criterios de selección de recursos didácticos : Evaluar Recursos Educativos - INTEF

  Guía sobre el uso de la inteligencia artificial en el ámbito educativo: Guía sobre el uso de la inteligencia artificial en el ámbito educativo.

  Amibox Atresmedia: Amibox Aula | Cómo funciona

  Code.org Currículo gratuito de informática e inteligencia artificial (K-12) | Code.org

Familias:

- **Charlas informativas**: Encuentros que aborden los riesgos digitales, la importancia de supervisar el uso de dispositivos en casa y estrategias para fomentar un uso equilibrado de la tecnología. Impartidos por profesionales en la materia. (Plan Director u otras promovidas por AMPA y Ayuntamiento).Formación para familias del INCIBE: FORMACIÓN PARA MENORES Y FAMILIAS | Menores | INCIBE. Buscador global - INTEF
- **Guías prácticas**: Materiales didácticos sobre la configuración de controles parentales, el manejo seguro de redes sociales y la protección de datos personales en dispositivos familiares. Familias | Menores | INCIBE (Mediación parental, Ciberseguridad para familias, herramientas de control parental). AseguraTIC - Seguridad del menor en Internet - Buscador - INTEF (Stop abuso a menores, Sexting, vida digital sana…..) Buscador global - INTEF (Guía seguridad en redes sociales, Guía conéctate contra la violencia de género….)
- **Fomento del diálogo familiar**: Actividades diseñadas para fortalecer la comunicación entre padres e hijos sobre el uso responsable de la tecnología. Familias | Menores | INCIBE (Organizador digital familiar, Pactos familiares para el buen uso, Vales de tiempo)

b) Políticas y Normativas

Un conjunto de directrices claras que establecen las bases para un uso seguro y responsable de las tecnologías en el centro.

- **Normas sobre comunicación digital**: Reglas para las interacciones entre estudiantes, docentes y familias a través de canales digitales, fomentando un respeto mutuo y profesionalismo. (Plan de comunicación de centro).



- **Política de privacidad**: Medidas específicas para proteger los datos personales de los estudiantes y garantizar que la información sensible no sea expuesta o utilizada indebidamente.

Carteles visuales para aulas: Infografías con normas claras y atractivas sobre el uso de dispositivos en el centro (por ejemplo: "No fotos sin permiso", "Mantén tus contraseñas privadas").

- **Acuerdos de uso**: Contratos formales entre el centro, los estudiantes y las familias para garantizar el compromiso con las normas establecidas. .(Decálogo del buen uso de dispositivos digitales enmarcado dentro de las NCOF del centro:

- DECÁLOGO DEL BUEN USO DE LOS DISPOSITIVOS DIGITALES

1. Sólo se utilizará la tableta con el conocimiento y permiso del profesor/a.
2. La tableta vendrá cargada cada mañana de casa.
3. No se traerán al centro accesorios, ni periféricos (cascos, altavoces, etc.) salvo que lo autorice el profesor.
4. Cada tableta vendrá identificada, tanto en el propio dispositivo como en la carcasa, de manera clara y visible.
5. El dispositivo no vendrá con código de desbloqueo, ni patrón, ni pin, particular.
6. Las cámaras de las tabletas se utilizarán solo cuando el profesor lo determine necesario para el cumplimiento de la tarea.
7. Queda prohibido hacer cualquier tipo de grabación de vídeo, audio, así como cualquier tipo de foto, salvo que lo autorice el profesor/a. La LGPD prohíbe expresamente la grabación y publicación de cualquier persona sin su consentimiento. Llevarlo a cabo es un delito.
8. Las tabletas sólo tendrán descargadas las aplicaciones de las editoriales y aquellas autorizadas por el equipo docente.
9. La tableta sólo se utilizará en el aula. Durante los recreos, comedor, extraescolares… permanecerá dentro de la mochila y en los lugares habilitados para ello.
10. En casa utilizaremos la tableta solo con carácter escolar y siempre bajo la supervisión de los adultos y el dispositivo de control parental.

CARTEL PARA LAS AULAS:



Toda estas actividades en el centro se engloban dentro de la normativa existente en CLM relacionada con el ámbito de la ciberseguridad escolar, y que es la siguiente:

Normativa Nacional:

- **Código de Derecho de la Ciberseguridad:** Este compendio, disponible en el Boletín Oficial del Estado (BOE), reúne leyes y reglamentos fundamentales en materia de ciberseguridad, incluyendo la Ley de Seguridad Nacional y el Esquema Nacional de Seguridad. boe.es
- **Esquema Nacional de Seguridad (ENS):** Establece los requisitos mínimos para la protección de los sistemas de información en el ámbito de la Administración Pública, aplicables también a entidades que gestionan servicios públicos.
- **Reglamento General de Protección de Datos (RGPD):** Regula el tratamiento de datos personales y la privacidad, aspectos esenciales en el entorno educativo. BOE.es - DOUE-L-

2016-80807 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Iniciativas Regionales en Castilla-La Mancha:

- **Centro Regional de Innovación Digital (CRID):** En febrero de 2025, el CRID inauguró un laboratorio de formación avanzada en ciberseguridad en Talavera de la Reina. Este espacio está destinado a formar y sensibilizar tanto a profesionales de la tecnología como a la ciudadanía en general sobre prácticas seguras en el entorno digital. cadenaser.com
- **Prohibición del Uso de Teléfonos Móviles en Centros Educativos:** Castilla-La Mancha, junto con Madrid y Galicia, ha implementado restricciones al uso de teléfonos móviles en las escuelas. Esta medida busca mejorar la convivencia escolar y reducir casos de ciberacoso. lacronica.net

Recursos y Recomendaciones:

- **Recomendaciones para la Ciberconvivencia:** El Instituto Nacional de Ciberseguridad (INCIBE) ofrece guías detalladas para trabajar la ciberconvivencia en los centros educativos, abarcando aspectos como la información al alumnado sobre líneas de ayuda y protocolos de actuación. incibe.es
- **Formación y Sensibilización:** La Universidad de Castilla-La Mancha ha organizado cursos y seminarios enfocadas en la ciberseguridad y su relevancia en el sector educativo, destacando la importancia de la protección de datos y el uso responsable de las tecnologías. uclm.es
- **Guía para centros educativos de la Agencia Española de Protección de datos. JCCM. Guía para centros educativos de la Agencia Española de Protección de Datos | Portal de Educación de la Junta de Comunidades de Castilla - La Mancha**

Estas iniciativas y normativas reflejan el compromiso de Castilla-La Mancha con la creación de un entorno educativo seguro y protegido en el ámbito digital.

c) Herramientas Tecnológicas

Implementación de soluciones tecnológicas avanzadas para garantizar un entorno digital seguro y funcional.

- **Filtros de contenido**: Instalación de sistemas que bloqueen el acceso a sitios web con contenido inapropiado, violento o peligroso. El centro está integrado en la red de conexiones de CLM, lo que impide el acceso a contenidos y plataformas no adecuados a través de la conexión WIFI del centro escolar. Además, los ordenadores destinados a la digitalización en el centro, utilizados por los alumnos, cuentan con un sistema de control y un cortafuegos gestionado por el servicio de CLM. En cuanto al uso de tabletas personales por parte del alumnado en el tercer ciclo, se propone a las familias la adquisición del control parental IMT Lazarus, que permite tanto al profesorado como a las familias gestionar el control escolar y doméstico durante el periodo escolar
- **Plataformas educativas seguras**: Uso de sistemas de gestión del aprendizaje (LMS) que prioricen la privacidad y seguridad de la información. Orientaciones sobre el uso de herramientas digitales en el ámbito educativo desde la perspectiva de la protección de datos

- INTEF. Empleo de aulas virtuales, Lumio u otras plataformas sensibles con la protección al alumnado.
- **Monitorización remota**: Software que permita al centro educativo supervisar el uso de dispositivos conectados a la red escolar para detectar amenazas. Se ofrece a las familias de 3º ciclo la posibilidad de emplear en los dispositivos personales de los alumnos una aplicación de "control parental" El resto de dispositivos del centro cuenta con "red de centro conectadas" y servicio remoto del CAU.

d) Concienciación Continua

Actividades regulares diseñadas para mantener la atención y el compromiso de la comunidad educativa con la ciberseguridad.

- **Campañas temáticas**: Celebraciones periódicas, como el Día de la Internet Segura, con actividades enfocadas en promover prácticas digitales responsables.
- **Campamento digital,** en colaboración con las **AMPAS** o **Ayuntamientos:** se trata de una propuesta de actividades presenciales extraescolares dirigidas a jóvenes de 9 a 17 años para que amplíen su conocimiento en competencia digital. Es una iniciativa impulsada por Fundación Cibervoluntarios, dentro del Programa de Competencias Digitales para la Infancia, CODI, puesto en marcha por el Ministerio de Juventud e Infancia, financiado por la Unión Europea-Next Generation EU. Campamento Digital
- **Semana de la Ciberseguridad:** una serie de actividades educativas y eventos que se centren en enseñar a los ciudadanos sobre los riesgos de la ciberseguridad, como el phishing, el robo de identidad y la protección de datos personales, con el fin de mejorar la seguridad digital de los usuarios.
- **Día Internacional contra el Ciberacoso (8 de noviembre):** actividades para educar sobre los riesgos del ciberacoso y proporcionar recursos para prevenir y actuar ante situaciones de acoso en línea. Podría incluir charlas, campañas de sensibilización en redes sociales, y talleres en colegios y universidades.
- **Actividades gamificadas**: Uso de juegos de rol, escape rooms digitales y dinámicas interactivas para enseñar conceptos clave de forma atractiva.
- **Materiales visuales**: Difusión de carteles, infografías y vídeos educativos en aulas y espacios comunes para reforzar los mensajes de seguridad digital.

e) Evaluación y Seguimiento

- **Encuestas periódicas**: Formularios para estudiantes, familias y docentes que evalúen la percepción y efectividad del programa.
- **Encuesta o cuestionario final de alumnos 5º y 6º EP sobre seguridad digital personal:** https://forms.office.com/Pages/DesignPageV2.aspx?lang=es-es&subpage=design&FormId=GALCiT482kuDLf9RVylcO7o1igMroDlLn4jrqX4lq2xUNFBPVzIxMzJVVEZHUzFVV0o0UTZXNFRXTCQlQCN0PWcu&Token=e17dbb2e80674514ae29e74f92c2337e
- **Simulaciones de incidentes**: Ejercicios prácticos para evaluar la capacidad de respuesta ante situaciones de ciberseguridad, como un ataque de phishing o un intento de suplantación de identidad.
- **Reuniones de revisión**: Encuentros trimestrales con representantes de docentes, familias y alumnos para analizar avances y ajustar estrategias.

f) Alianzas y Recursos Externos

- **Colaboración con expertos**: Invitar a profesionales de ciberseguridad para impartir talleres o charlas.
- **Acceso a recursos gubernamentales**: Aprovechar materiales y programas proporcionados por entidades como el Instituto Nacional de Ciberseguridad (INCIBE).
- **Creación de una biblioteca digital de ciberseguridad**: Repositorio en línea con guías, vídeos, actividades y materiales educativos para toda la comunidad.

Finalizamos así, la redacción y actualización de nuestro programa de ciberseguridad con la intención de que esté en vigor durante los próximos cursos, con las incorporaciones y mejoras que creamos pertinentes a lo largo de este tiempo y siempre en arreglo a la normativa vigente.

Aprobado en Claustro y Consejo escolar a 30 de junio de 2025