PLAN DE SEGURIDAD Y CONFIANZA DIGITAL

CURSO 2024- 2025

INTRODUCCIÓN

En la era digital actual, las tecnologías de la información y la comunicación (TIC) se han integrado profundamente en todos los aspectos de la vida cotidiana, incluida la educación. Los centros educativos de Castilla y León no son ajenos a este fenómeno, y su compromiso con la formación integral de los estudiantes incluye el uso adecuado y responsable de las herramientas digitales. Sin embargo, junto con los beneficios que el uso de las TIC ofrece, también surgen retos significativos relacionados con la seguridad digital y la confianza de los usuarios.

Un entorno educativo seguro no solo debe facilitar el acceso a la información y a los recursos digitales, sino también garantizar la protección de los datos personales y la privacidad de todos los miembros de la comunidad escolar.

El Plan de Seguridad y Confianza Digital que aquí se presenta tiene como objetivo establecer un marco integral para proteger los sistemas, dispositivos y datos de la institución educativa, al tiempo que promueve una cultura de uso responsable de las tecnologías.

Este plan, alineado con las normativas nacionales y europeas sobre protección de datos y seguridad en línea, busca minimizar los riesgos asociados con ciberamenazas, fraudes digitales, y el uso inadecuado de la red.

A través de la educación y la sensibilización de los estudiantes, docentes, personal administrativo y familias, el centro educativo podrá fomentar un ambiente digital seguro y confiable, propiciando un uso adecuado de las herramientas digitales para mejorar el aprendizaje y el desarrollo integral de los estudiantes.

De esta manera, el Plan de Seguridad y Confianza Digital se convierte en un instrumento clave para garantizar que las tecnologías sigan siendo un aliado en el proceso educativo, respetando la privacidad, la seguridad y el bienestar de todos los involucrados en la comunidad educativa.

OBJETIVOS

• Cumplir con las leyes y regulaciones aplicables a la protección de datos personales y la ciberseguridad.

• Proteger los datos personales y la privacidad de los estudiantes, docentes y familias.

• Fomentar una cultura de seguridad digital entre la comunidad educativa.

• Garantizar el uso seguro y ético de las tecnologías en el entorno escolar.

• Prevenir y gestionar incidentes de seguridad digital como ciberacoso, phishing o acceso no autorizado.

• Fomentar la colaboración con instituciones y organizaciones para llevar a cabo acciones encaminadas a mejorar la Seguridad y Confianza Digital del centro y del alumnado.

ACCIONES

• **Formación:** Organizar talleres y sesiones formativas para estudiantes, docentes y familias sobre ciberseguridad, privacidad y comportamiento digital responsable.

• **Políticas claras:** Establecer políticas de uso aceptable de dispositivos y recursos digitales.

• **Actualización tecnológica:** Mantener sistemas operativos, software antivirus y firewalls actualizados en todos los dispositivos del centro.

• **Control de acceso:** Implementar contraseñas seguras y autentificación en dos pasos en todas las cuentas institucionales.

• **Comunicación proactiva:** Difundir consejos y buenas prácticas de seguridad digital a través de boletines y redes sociales.

• **Supervisión:** Monitorizar el uso de internet en el centro mediante herramientas de control parental y filtrado de contenido.

• **Denuncia segura:** Crear un canal de comunicación confidencial para reportar problemas de seguridad o confianza digital.

• **Netiqueta:** Establecer reglas claras sobre el uso de la tecnología en el colegio. (**Anexo I**).

INDICADORES DE LOGRO

- **Capacitación:**

Porcentaje de estudiantes, docentes y familias que han participado en formaciones sobre ciberseguridad.

- **Incidentes reportados:**

Número de incidentes gestionados y resueltos de manera eficaz.

- **Conformidad:**

Nivel de cumplimiento de las políticas de seguridad digital entre la comunidad educativa.

- **Evaluaciones:**

Mejoras en los resultados de encuestas de percepción sobre seguridad digital.

PROTOCOLO DE ACTUACIÓN ANTE PROBLEMAS DE SEGURIDAD Y CONFIANZA DIGITAL

• **Identificación:** Detectar y registrar el problema (ej. acceso no autorizado, ciberacoso, phishing).

• **Notificación:** Informar a los responsables del centro (equipo directivo y coordinador TIC).

• **Contención:** Tomar medidas inmediatas para minimizar el daño (bloqueo de cuentas, desconexión de sistemas).

• **Análisis:** Investigar las causas del problema y los datos o usuarios afectados.

• **Comunicación interna:** Informar al personal relevante (profesores, familias) sobre el incidente.

• **Apoyo a afectados:** Brindar asistencia a las personas involucradas (psicológica, técnica o jurídica según corresponda).

• **Resolución:** Aplicar soluciones técnicas y administrativas para resolver el incidente.

• **Reporte oficial:** Documentar el incidente y las acciones tomadas en un informe.

• **Aprendizaje:** Implementar medidas preventivas basadas en lo aprendido (mejoras tecnológicas o formativas).

• **Seguimiento:** Realizar un monitoreo posterior para asegurar la eficacia de las medidas implementadas.

EVALUACIÓN

La comisión TIC realizará una evaluación anual al finalizar el curso con el objetivo de realizar propuestas de mejora en el Plan Códice TIC del colegio para el curso siguiente. Para dicha evaluación se tendrá como referencia los indicadores de logro para completar la siguiente rúbrica:

Criterio	Nivel Excelente (4)	Nivel Bueno (3)	Nivel Aceptable (2)	Nivel Insuficiente (1)
Definición de objetivos	Los objetivos son claros, específicos, medibles y completamente alineados con las necesidades del centro.	Los objetivos son claros y relevantes, pero podrían ser más específicos o medibles.	Los objetivos son generales y no abarcan todas las áreas críticas de seguridad digital.	Los objetivos son confusos, irrelevantes o inexistentes.
Ejecución de acciones	Las acciones están bien definidas, implementadas y alineadas con los objetivos planteados.	Las acciones están implementadas, aunque faltan detalles o no están completamente alineadas.	Las acciones están parcialmente implementadas o son insuficientes para cubrir todos los objetivos.	No se han implementado acciones relevantes o estas son inadecuadas.
Indicadores de logro	Los indicadores son claros, específicos y miden el impacto de manera efectiva.	Los indicadores son relevantes, pero podrían ser más específicos o mejor diseñados.	Los indicadores son básicos y no reflejan adecuadamente el impacto de las acciones.	No se definieron indicadores o estos son irrelevantes para evaluar los logros del plan.
Protocolo de actuación	El protocolo es claro, detallado y aplicable a una variedad de incidentes	El protocolo es adecuado, pero podría incluir más pasos o mayor detalle	El protocolo es básico y no contempla todos los posibles	No se definió un protocolo o este es insuficiente para gestionar incidentes.

	de seguridad digital.	en ciertos casos.	problemas de seguridad digital.	
Formación y sensibilización	El plan incluye formación regular, bien diseñada y participativa para toda la comunidad educativa.	La formación está presente, pero no es regular o no alcanza a toda la comunidad educativa.	La formación es limitada y no cubre todos los temas clave de seguridad digital.	No se incluyen actividades de formación o sensibilización en el plan.
Evaluación y mejora continua	El plan incluye una evaluación detallada y acciones concretas para la mejora continua.	La evaluación está presente, pero le faltan detalles o no incluye un plan de mejora claro.	La evaluación es básica y no garantiza una mejora continua.	No se contempla ningún tipo de evaluación ni mejora continua.

Este plan busca garantizar un entorno digital seguro y confiable, con protocolos claros y un enfoque en la prevención, gestión y aprendizaje continuo.

ANEXO I

Netiqueta del CEIP Rafael Alberti (Urbanización El Encinar).

Reglas de Netiqueta

1. **Respeto mutuo**: Usa un lenguaje amable y respetuoso en todas las comunicaciones.
2. **Uso adecuado del lenguaje**: Evita las expresiones ofensivas, insultos o lenguaje vulgar.
3. **Identificación clara**: Usa tu nombre real y mantén tu perfil actualizado en las plataformas.
4. **Cuidado con las mayúsculas**: No escribas mensajes en mayúsculas completas; equivale a gritar.
5. **Responde con prontitud**: Contesta los correos y mensajes relevantes en un plazo razonable.
6. **Estructura los mensajes**: Usa saludos, cuerpo del mensaje claro y una despedida cordial.
7. **Evita el spam**: No envíes mensajes innecesarios o repetitivos.
8. **Protege la privacidad**: No compartas información personal o fotos de otros sin su consentimiento.
9. **Sé inclusivo**: Usa un lenguaje que no discrimine por razones de género, cultura, o creencias.
10. **Cita correctamente**: Da crédito a las fuentes al compartir información o material ajeno.
11. **No interrumpas**: En reuniones virtuales, espera tu turno para hablar y utiliza las funciones de levantar la mano.
12. **Revisa antes de enviar**: Lee los mensajes antes de enviarlos para evitar errores o malentendidos.
13. **Sigue las normas tecnológicas**: Usa las plataformas del centro de manera apropiada y respeta los límites establecidos.
14. **Actúa con profesionalidad**: Recuerda que tu comportamiento en línea refleja tu actitud como estudiante o educador.

Aplicación de la Netiqueta

1. **Correo electrónico**:
   - Usa el asunto del correo para resumir el contenido.
   - Mantén un tono formal y profesional.
   - Firma con tu nombre y, si aplica, tu rol dentro del centro.

2. **Redes sociales**:
   - Publica contenido relacionado con actividades educativas, evitando temas personales o controversiales.
   - Responde comentarios o mensajes directos con cortesía y dentro del horario establecido por el centro.

3. **TEAMS (y otras plataformas virtuales)**:
    - Conéctate a las reuniones puntualmente y asegúrate de tener configurado tu micrófono y cámara correctamente.
    - Usa fondos neutros y evita distracciones visuales o sonoras.
    - Utiliza los canales asignados para cada tema o grupo y evita mensajes fuera de contexto.

Comportamientos que no son Netiqueta

1. **Enviar mensajes ofensivos** o que ataquen a otros usuarios.
2. **Compartir contenido inadecuado**, como memes ofensivos, información falsa o material no relacionado con las actividades educativas.
3. **Interrumpir reuniones virtuales** con comentarios fuera de lugar o sin relevancia.
4. **Hacer spam** en los canales de comunicación del centro.
5. **Ignorar las respuestas** o preguntas de otros usuarios, mostrando falta de interés o compromiso.
6. **Usar un lenguaje excesivamente informal** en contextos donde se espera formalidad, como correos o mensajes a docentes.

Adoptando estas reglas de netiqueta, garantizamos un entorno digital respetuoso y productivo para todos los miembros del centro educativo.