Plan de seguridad y confianza digital

IES Vía de la Plata

Contenido

1. Datos de identificación del Centro

Nombre del Centro: IES Vía de la Plata
Dirección: Avda. General Benavides, 51
Código del Centro: 24000679
Localidad: La Bañeza
Código Postal: 24750
Teléfono: 987 64 17 50
Correo electrónico: 24000679@ educa.jcyl.es

2. Justificación

A nivel europeo, en 2010, la Comisión Europea puso en marcha "la estrategia Europa 2020" que contempla la creación de la Agenda Digital Europea para conseguir convertir a la Unión Europea en una potencia tecnológica y digital, garantizando la confianza y seguridad en el uso de las Tecnologías de la Información y la Comunicación (TIC).

A nivel estatal, de acuerdo con este marco europeo, España aprobó en 2013 la creación de una Agenda Digital con seis objetivos prioritarios entre los que se incluye el refuerzo de la confianza y seguridad en el ámbito digital. La Ley Orgánica 8/2013, de 9 de diciembre, para la mejora de la calidad educativa (LOMCE) destaca el papel de la TIC en el cambio metodológico necesario para la mejora de la calidad educativa y como su uso responsable debe abordarse en nuestro sistema educativo. También la Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación, incluye entre los objetivos de la ESO, desarrollar las competencias tecnológicas y avanzar en la reflexión sobre su funcionamiento y utilización y entre los objetivos de Bachillerato, utilizar con solvencia y responsabilidad las tecnologías de la información y la comunicación.

A nivel regional, la Conserjería de Educación de la Junta de Castilla, pone en marcha en 2014-15 el Plan de Seguridad y Confianza Digital en el ámbito educativo para impulsar el uso seguro y responsable de internet por parte de la comunidad educativa. Este proyecto se afianza y regula en Castilla y León en 2015 con la Orden Edu/834/2015.

A nivel de centro, se persigue sistematizar intervenciones educativas que fomenten el uso seguro, crítico y responsable de las TIC entre toda la comunidad educativa.

3. Objetivos

Este plan pretende lograr los siguientes objetivos:

1. Formar sobre el uso seguro de internet en todos los niveles educativos que se imparten en el centro
2. Informar y sensibilizar sobre las situaciones de riesgo más habituales que se pueden encontrar los menores al navegar por internet
3. Impulsar la alfabetización digital y el uso seguro de las TIC

4. Actuaciones

Objetivo 1.-
Formar sobre el uso seguro de internet en todos los niveles educativos que se imparten en el centro

ACTIVIDADES	RESPONSABLES	TEMPORALIZACIÓN
Realizar actividades formativas con el alumnado sobre el uso seguro de internet el día de internet segura CYL	Tutores y profesorado	Curso escolar
Dar instrucciones básicas en cada curso académico para el uso seguro y responsable de las TIC	Tutores	Primer trimestre

Objetivo 2.-
Informar y sensibilizar sobre las situaciones de riesgo más habituales que se pueden encontrar los menores al navegar por internet

ACTIVIDADES	RESPONSABLES	TEMPORALIZACIÓN
Publicación en la página web del centro de recursos sobre seguridad y confianza digital	Coordinador página web	Cada curso escolar
Realización de trabajos por parte del alumnado sobre información y prevención de situaciones de riesgo en internet	Profesores	Curso escolar
Informar a las familias a través de nuestra página web sobre los talleres ofertados en el portal de educación de Castilla y León	Coordinador página web	Cada curso escolar

Objetivo 3.-
Impulsar la alfabetización digital y el uso seguro de las TIC

ACTIVIDADES	RESPONSABLES	TEMPORALIZACIÓN
Participación del alumnado en concursos y/o proyectos específicos sobre confianza y seguridad digital	Profesores	Curso escolar
Realización de actividades de formación del profesorado sobre competenciaa digital y uso seguro de las TIC	Coordinador de formación	Curso escolar
Organización de visitas o participación en talleres presenciales o a distancia del INCIBE	Jefe departamento extraescolares	Curso escolar

5. Recursos

Coordinador de seguridad

Responsable #CompDigEdu. Enrique González Alonso

Materiales externos de las siguientes webs

Portal de Educación de CYL(Educacyl):. Plan de Seguridad
https://www.educa.jcyl.es/plandeseguridad/es

- Guías de enseñanza con TIC (Consejos para docentes, familias y alumnado sobre enseñanza con TIC)
- Consejos y recomendaciones (Información de interés sobre el uso seguro de Internet) Material multimedia (Vídeos de corta duración sobre información, difusión y promoción del uso seguro de Internet)
- Propuesta de talleres para centros, familias y alumnado
- Vídeos premiados en el concurso de Plan de Seguridad y Confianza Digital

Internet segura for kids

https://www.is4k.es/

INCIBE

https://www.incibe.es/

OSI

https://www.osi.es/es

6. Evaluación

La verificación de la seguridad y confianza digital en el centro educativo se hace en el tercer trimestre del curso académico a través de la siguiente herramienta de autoevaluación, basada en la autoevaluación CODICE TIC.

INDICADOR	INICIADO	DESARROLLO	SISTEMATIZADO
1. El centro tiene establecidas estrategias y responsabilidades explícitas para la gestión de la seguridad de datos, servicios, redes y equipos.			
2. El centro tiene recogidos en sus documentos institucionales las normas, procesos y actuaciones a aplicar en las situaciones que afecten a la seguridad, garantía de los derechos digitales, uso inadecuado de equipamiento y servicios y a la convivencia en red de la comunidad educativa.			
3. El centro tiene establecidos criterios y procedimientos sistematizados para el almacenamiento, copia de seguridad, custodia de datos, documentos y recursos digitales de centro.			
4. El centro desarrolla actuaciones de formación y concienciación sobre la propiedad intelectual, los derechos de autor y la propiedad industrial.			
5. El centro desarrolla actuaciones de formación y concienciación sobre el uso seguro de los equipos, servicios y convivencia en la red.			
6. El centro desarrolla periódicamente procesos de evaluación y auditoría de la seguridad de equipamientos y servicios y de aplicación de las normativas de protección de datos			

ANEXOS

CUESTIONARIO DETALLADO DE AUTOEVALUACIÓN

El protocolo de mantenimiento de equipos incluye apartado dedicado a la seguridad informática y privacidad.

PROPUESTA-APOYO PARA LA VERIFICACIÓN SEGURIDAD Y CONFIANZA DIGITAL EN LOS CENTROS EDUCATIVOS. HERRAMIENTA DE AUTOEVALUACIÓN

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 centros dispone de medidas de registro, autentificación personalizada con límite de intentos para ficheros de carácter personal que contengan datos de características personales, penales, financieras, tributarias...	☐	☐	☐
4. El centro dispone de medidas de registro, autentificación con límite de intentos y cifrado para los datos referidos a ideología, religión, origen racial, salud, psicológicos, etc., de los miembros de la comunidad educativa.	☐	☐	☐
5. El centro dispone de un documento de planificación y organización de los procesos básicos de protección de datos.	☐	☐	☐
6. Existe un responsable de gestión de la protección de datos que aborda las incidencias relativas a la información y los datos.	☐	☐	☐
7. El centro tiene un plan de auditorías de seguridad para la protección de datos.	☐	☐	☐
8. Existe un reglamento claro con directrices específicas respecto a la disposición de imágenes y fotografías en la red.	☐	☐	☐
9. 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.	☐	☐	☐
10. 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 ☐ ☐ ☐
10. Los datos o información de carácter personal en dispositivos móviles o en la nube, se mueven encriptados o con las medidas de seguridad adecuadas al nivel del fichero. ☐ ☐ ☐

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 *wifis* 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. l 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 estos. ☐ ☐ ☐
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 de este. ☐ ☐ ☐
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 subscrito los principios del Puerto Seguro. ☐ ☐ ☐
6. 5. Los servicios de internet garantizan la integridad de los datos, y evitan el acceso de personal no autorizado. ☐ ☐ ☐
7. 6. 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. ☐ ☐ ☐