IES Antonio Tovar

Curso 2020-2021

Plan de Seguridad y Confianza Digital

(Concreción en el Centro)

COMISIÓN TIC

IES Antonio Tovar

Plan de Seguridad y Confianza Digital

Introducción

Los elementos aquí descritos son un resumen de los aspectos relacionados con la Seguridad y Confianza digital contenidos en el Plan TIC del centro. Su objetivo es informar y dar a conocer a la comunidad educativa la aplicación y concreción en nuestro instituto del Plan de Seguridad y Confianza Digital que las administraciones europeas, nacional y autonómica han impulsado para hacer los centros educativos lugares seguros en la red.

En consecuencia, este plan está en línea con la información contenida, especialmente, en los siguientes documentos:

- Agenda digital para Europa.
- ORDEN EDU/834/2015 que regula el Plan de Seguridad y Confianza Digital en el ámbito educativo» en la Comunidad de Castilla y León.

Como establece dicha orden, la finalidad de este Plan es *"fomentar el uso seguro, crítico y responsable de las tecnologías de la información y la comunicación (en adelante, TIC) entre todos los miembros de la comunidad educativa, en especial en el alumnado".*

Punto de partida

La gestión de riesgos se puede dividir en tres etapas diferenciadas: La identificación, la evaluación y el tratamiento de los riesgos.

El riesgo se deriva de la exposición a amenazas, por tanto, desde la perspectiva de la privacidad, es fundamental entender qué es una amenaza y cómo se pueden identificar escenarios de riesgo para los datos personales a partir de la misma. Una amenaza es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento. Si ponemos el foco en la protección de los datos, las amenazas se pueden categorizar principalmente en tres tipos:

- Acceso ilegítimo a los datos: ¿qué daño causaría que lo conociera quien no debe? confidencialidad

- Modificación no autorizada de los datos: ¿qué perjuicio causaría que estuviera dañado o corrupto? integridad
- Eliminación de los datos: ¿qué perjuicio causaría no tener un dato o no poder utilizarlo? disponibilidad.

La última fase del proceso de gestión de riesgos es tratar los mismos. El objetivo de tratar los riesgos es disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen. El riesgo inherente se puede tratar con el objetivo de reducir o mitigar el mismo, en función de la medida que se adopte, hasta situar el riesgo residual en un nivel que se considere razonable.

Definición de riesgos y medidas:

En cuanto a la definición de riesgos y medidas, derivan principalmente del uso inadecuado en internet, instalación de malware, infección por virus, pirateo de contraseñas, etc. Existen una serie de normas de uso y también de software de seguridad para tratar de paliar estos efectos.

La transferencia de información en el aula virtual se realiza mediante conexiones seguras HTTP y certificados de seguridad proporcionados por empresas certificadoras.

En las aulas de informática mediante el cortafuegos general del que dispone la red.

En todos los ordenadores del Centro mediante un antivirus actualizado.

Hasta la fecha, el mayor riesgo al utilizar Internet se encuentra en el uso que los alumnos hacen de las redes sociales en las que tienen cuenta registrada. En ellas suelen publicar información personal y fotografías sin haber configurado adecuadamente la privacidad, con lo que están expuestos a las miradas de cualquier usuario.

El control de las comunicaciones que los alumnos puedan establecer fuera del horario escolar, a través de las redes sociales, no es responsabilidad del profesorado. Sin embargo, cuando se producen conflictos en las redes sociales entre alumnos, estos se reflejan también dentro del instituto, y entonces se llevan a cabo acciones de información y control por parte de tutores, departamento de orientación y jefatura de estudios, siguiendo el protocolo recogido en el plan de convivencia. No obstante, es preciso que los padres de los alumnos ejerzan un control suficiente del uso que sus hijos hacen de las redes sociales.

Estructura organizativa de seguridad y responsabilidad sobre la seguridad, datos personales, documentos institucionales y recursos de aprendizaje y enseñanza:

Los criterios de seguridad y conservación de datos implican la realización de *backup* diario de los ficheros de la red de Secretaría.

También se informa al nuevo profesorado en cada curso de las normas de uso de la red informática y sus elementos asociados del centro, en cuanto a uso permitido, protección de la información y elección de contraseñas robustas. También se les avisa de las normas de uso de los dispositivos móviles dentro de las aulas.

Los datos de configuración de la red y los nombres de usuario y claves de acceso al Aula virtual y a la intranet son custodiados por el Coordinador TIC.

Al inicio de cada curso académico, el coordinador TIC configura los accesos de todos los usuarios y comunica a los alumnos, a través de los tutores, sus datos de acceso.

Para la confidencialidad de datos se cumple la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD).

La confidencialidad es importante, pero nuestra experiencia nos dice que hay bastantes alumnos que olvidan o pierden sus datos de acceso, por lo que debemos proporcionárselos nuevamente, en ocasiones varias veces. Por otro lado, no existe la posibilidad de que los datos de acceso al aula virtual o al portal de educación, sean migrados automáticamente a la intranet. Estas dos situaciones nos obligan a disponer de un fichero con los datos de acceso de alumnos y profesores, custodiado por el coordinador TIC, a partir del que se puedan suministrar los datos de acceso a los alumnos, cuando sea necesario, y configurarlos en la intranet. No obstante, una vez suministrados los datos, cada usuario puede cambiar su clave de acceso, lo que aumenta la seguridad del sistema.

Descripción del contexto de almacenamiento y custodia de datos académicos, didácticos y documentales

Los servicios integrados en la plataforma educativa del centro disponen de los elementos de seguridad configurados de forma centralizada por los servicios informáticos de la Junta de Castilla y León.

El Centro cuenta con un sistema de protección y seguridad, y antivirus en el servidor.

El servicio de Intranet que proporciona el centro se basa en una estructura de estrella que permite el acceso libre a ciertos contenidos y el acceso identificado a otros. No obstante, los alumnos solo pueden acceder desde los equipos conectados directamente a la red del centro, mientras que se permite el acceso a los profesores tanto desde el centro como desde cualquier otra ubicación. Este servidor dispone de antivirus y se hacen copias de seguridad diarias de la información.

El Centro posee un servidor FTP Filezilla, software utilizado para gestionar la transferencia de archivos a través del protocolo FTP, permitiendo entre otras cosas el crear usuarios, asignarles permisos para acceder sólo a determinadas carpetas, así como permitirles no tan sólo la descarga de archivos sino también la posibilidad de subir archivos al propio servidor FTP, eliminarlos, crear y

eliminar carpetas o directorios, etc. Todo ello con contraseñas personales gestionadas por el coordinador de las TIC y el Equipo Directivo del Centro.

Estrategias de seguridad de servicios, redes y equipos

A) OBJETIVOS:

- ✓ Definir, generar y estructurar las medidas de seguridad que garanticen la protección de datos especialmente sensibles y la confidencialidad en el centro.
- ✓ Informar y formar a los diferentes sectores de la comunidad educativa del uso correcto y seguro de las nuevas tecnologías.

B) CRITERIOS DE SEGURIDAD Y CONFIDENCIALIDAD:

- **Criterios de seguridad:** Para mejorar la seguridad y el uso de contenidos poco apropiados, se ha configurado un cortafuegos en el servidor para no permitir el acceso determinadas páginas web. Así mismo en las aulas de informática se utiliza el cortafuegos general del que dispone la red. Además, cada ordenador dispone de un antivirus actualizado.

- **Criterios de confidencialidad:** Con respecto a la confidencialidad de datos se cumple la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD). Como ya se ha señalado en apartados anteriores:
  - ✓ Se realiza un backup diario de los ficheros de la red de Secretaría.
  - ✓ Se informa al nuevo profesorado en cada curso de las normas de uso de la red informática y sus elementos asociados del centro, en cuanto a uso permitido, protección de la información y elección de contraseñas robustas. También se les avisa de las normas de uso de los dispositivos móviles dentro de las aulas.
  - ✓ Los datos de configuración de la red y los nombres de usuario y claves de acceso al Aula virtual y a la intranet son custodiados por el Coordinador TIC, encargado de configurar los accesos y comunicarlos a los alumnos. Posteriormente cada usuario cambia la clave, para mejorar la seguridad.

C) ESTRATEGIAS CON SERVICIOS, REDES Y EQUIPOS:

C1) Criterios y procesos establecidos en caso de un uso inadecuado y/o incidencias en materiales y servicios:

Siguiendo el mismo proceso que se indica en **nuestro reglamento de régimen interno** el alumnado que realice desperfectos en los equipos informáticos por el uso inadecuado del mismo, tendrá que pagar o reponer el sistema afectado y, dependiendo de la intencionalidad, puede ir acompañado de la correspondiente sanción académica.

Para localizar con mayor facilidad este tipo de incidencia, los profesores se asegurar y comprueban que los alumnos ocupan un mismo puesto en sus clases. Existen dos modelos de recogida de dicha información:

- Para los usuarios habituales de un aula con equipos informáticos, el profesor responsable cumplimenta el modelo de usuarios de cada puesto a comienzo de curso. Estos listados se recogen en Secretaría.
- Para los usuarios puntuales, en cada aula de informática existen estos mismos modelos que se rellenarán con el listado de puestos de cada clase. Estos listados son recogidos periódicamente por Secretaría.

Este sistema permite identifica al alumno que haya podido hacer un mal uso, siempre que se comunique con rapidez la incidencia.

C2) Riesgos y medidas en redes e internet ante un uso inadecuado:

Los riesgos más destacables del acceso a internet y las medidas que se llevan a cabo para evitarlos son:

- ✓ Acceso a contenidos inadecuados en internet. Como medida para evitarlo el cortafuego del servidor del centro está configurado para no permitir la conexión a páginas web con contenido relacionado con la violencia, pornografía, de carácter sexual, etc.
- ✓ Mal uso de las redes sociales. Se realiza una labor de concienciación del uso responsable de las redes sociales en las reuniones de inicio de curso con padres/madres/ tutores y estudiantes.
- ✓ Información poco fiable. Los profesores dirigen las búsquedas en internet en sus asignaturas, y se facilitan direcciones (URL) como recurso didáctico a los estudiantes.
- ✓ Operaciones de descarga de archivos. Esta operación puede utilizarse para que se instale en el equipo un software malicioso con diferentes finalidades: borrado de datos, ralentización del sistema, robo de datos de contraseñas y de datos personales, seguimiento de los sitios web visitados, etc. Para evitarlo se utilizan dos medidas: de manera global, el cortafuegos; y de manera local, un software de antivirus y de seguridad específico en cada uno de los equipos.
- ✓ Posibles riesgos de intrusión en los servicios utilizados por el Centro:

  Sitios web, blog, redes sociales, etc. Para evitarlos, el acceso a la configuración actualización y mantenimiento de éstos se hará a través de un usuario y una contraseña personales de los responsables de las TIC del centro. Además, en todos los servicios se utilizan políticas de privacidad adecuadas para un centro educativo.

  Software de gestión de la biblioteca, ABIES. El acceso al equipo de la biblioteca, en la cual está instalado, está habilitado con dos tipos de usuarios: profesores y biblioteca. Sólo las personas encargadas de la Biblioteca del centro tienen acceso a la contraseña de este último.

  Equipos informáticos de la red de la Consejería de Educación de la Junta de Castilla y León: Servidor, Dirección, Jefatura de estudios, Secretaría y administración. Sólo los miembros del equipo conocen la contraseña de acceso a dichos ordenadores.

- ✓ Publicación de información sin autorización de los alumnos. Todos los estudiantes del Centro presentan, en el momento de formalizar la matrícula, un documento de autorización de datos personales del alumno. En dicho documento el Padre, Madre o Tutor legal o el propio alumno (si es mayor de edad) autoriza la captación de imágenes y grabaciones audiovisuales; la publicación de datos personales simples (nombre, apellidos, grupo); la publicación de trabajos escolares, para su difusión en cualquiera de los medios impresos, audiovisuales o espacios web del centro con fines estrictamente educativos, no lucrativos, divulgativos y de información, durante el período de escolarización del alumno/a en el Centro. En el caso de alumnos menores de edad dicho impreso debe de ser firmado por el padre, madre o tutor. Al inicio de cada curso escolar se registra dicha situación en el software IES2000, y se comunica por correo electrónico (a través del grupo de la sala de profesores del aula virtual) a todo el profesorado del centro los nombres, apellidos, curso y nivel de estudios de los estudiantes que no han autorizado para que procedan en consecuencia.

C3) Criterios de seguridad, conservación de datos y confidencialidad:

Al inicio de cada curso académico el técnico informático (empresa externa) realiza las siguientes acciones:

- ✓ Formatea todas las unidades de red de los alumnos. Al inicio de cada nuevo curso se advierte a los estudiantes de que esta circunstancia. Tendrá lugar al inicio del siguiente curso académico, de manera que deberán de guardar en un USB o unidad externa la información que consideren que deben conservar.
- ✓ Elimina todos los usuarios-alumnos del curso anterior y da de alta a todos los usuarios-alumnos (alumnos matriculados en el centro) para permitir el acceso a los ordenadores, y se facilita una clave genérica que cada uno de ellos deberá de personalizar en su primer acceso. Los usuarios se agrupan por niveles de estudios y son facilitados por el responsable TIC del centro.
- ✓ Da de baja los correos electrónicos de los profesores que no permanecen en el centro y da de alta los de las nuevas incorporaciones. Así mismo da de baja sus usuarios de acceso. Esto mismo se lleva a cabo con los profesores que cubren alguna suplencia. También se crea un usuario y contraseña para cada uno de ellos que permitan el acceso a los ordenadores.
- ✓ A pesar de que existe la posibilidad de utilizar herramientas para la gestión de las contraseñas, el equipo directivo decidió que no existiera un registro de las contraseñas, de manera que el alumno o el docente fueran los únicos conocedores de la misma. En el caso de olvido o extravío se solicita al responsable de las TIC del centro, y éste lo comunica a su vez al responsable del mantenimiento informático que inicia de nuevo el proceso. Este sistema garantiza la confidencialidad e integridad de las contraseñas.

C3) Elementos de seguridad y protección de los servicios (servidores, servicios P2P, proxy, controles parentales,…).

Como se ha detallado anteriormente el equipo firewall del servidor gestiona el trafico ascendente y descendente desde internet. Así mismo, permite controlar y filtrar los contenidos descargados en la red, permitiendo o bloqueando los mismos.

Todos los datos de usuarios almacenados en el data server está protegidos por copia de seguridad diaria.

C4) Protección, confidencialidad, conservación y seguridad de los datos de carácter académico:

Desde el centro se llevan a cabo las siguientes tareas relacionadas con esta cuestión:

- Control de acceso a los datos:
- Gestión de contraseñas.
- Realización de copias de seguridad:
- Difusión y extensión de datos personales dentro y fuera del centro:
  - ✓ Registro de las redes sociales con acceso autorizado desde el centro: las que el equipo Directivo determina, bajo la supervisión del responsable de las TIC y del profesor en clase.
  - ✓ Elaborar estrategias para crear la identidad digital del centro: difusión de la página WEB del Centro.
  - ✓ Elaborar estrategias para formar y concienciar a los alumnos sobre el uso correcto de los datos y la tecnología: Durante todo el curso.
    - Imágenes, difusión de datos personales en Internet, acceso a contenidos inapropiados en la red. Control a través de la Dirección del Centro.

C5) Medidas de seguridad en la red:

Aspectos generales:

- Equipo responsable: Responsable de las TIC, HV Consulting
- Tareas:
  - ✓ Establecer criterios de uso, configuración y acceso a los sistemas (usuario, contraseña…).
  - ✓ Gestión de contraseñas: Administrador TIC, cambio por el propio usuario
  - ✓ Comprobar si están funcionando las medidas de seguridad previstas.
    - Garantizar que no se interrumpan los servicios.
    - Detectar y solucionar en primera instancia las incidencias de seguridad detectadas.
  - ✓ Crear y registrar las directivas de grupo utilizadas para definir las configuraciones de los equipos y usuarios.
    - Evitar que personas no autorizadas accedan el sistema.
    - Evitar que los usuarios realicen operaciones involuntarias que puedan dañar el sistema.
  - ✓ Informar y educar a los usuarios sobre el uso seguro de los sistemas.
  - ✓ Definir los posibles riesgos y las medidas a tomar.
  - ✓ Llevar a cabo la auditoria de los sistemas.

Seguridad inalámbrica:

Criterios establecidos por la Conserjería de Educación dentro del proyecto de Escuelas Conectadas.

Acceso a Internet:

- Establecer criterios de responsabilidad de uso (buenas prácticas). Sí
- Establecer criterios de control de acceso, que permitan identificar incidencias de seguridad o mal uso, identificando riesgos y estableciendo posibles medidas de respuesta.

Seguridad de los equipos:

- Comprobar que las herramientas de seguridad funcionan y se actualizan correctamente: al comenzar la clase
- Escanear los equipos con antivirus y antimalware con la periodicidad que se considere conveniente: diariamente
- Detectar incidencias y aplicar medidas en respuesta a ellas.
- Fijar criterios de acceso y configuración: Usuario, contraseña, perfiles.
- Fijar criterios de responsabilidad de uso (buenas prácticas) e informar a los alumnos.

Registro de aplicaciones de seguridad instaladas:

- Antivirus: Avast, bitdefender
- Antimalware: Malwarebytes
- Control parental: Configuración de control parental de Windows 7 y Windows 10.
- Cortafuegos: firewall de Windows 7, Windows 10 o del propio antivirus.

Programas de gestión académica: Administración.

Regulado mediante Instrucción de 27 de mayo de 2013, de la Dirección General de Política Educativa Escolar.

Actuaciones de formación y concienciación de usuarios de los servicios centro:

Con el profesorado, en las sesiones de coordinación y formación docente de inicio de curso siempre hay sesiones dedicadas a las TIC del centro y entre otros puntos se hace hincapié en la responsabilidad en el uso de internet. Además, para evitar uno de los principales riesgos: el acceso a contenidos inadecuados, se configurará el cortafuegos del servidor del centro para no permitir la conexión a páginas web con contenido relacionado con la violencia, pornografía, de carácter sexual, etc. El resto de posibles riesgos se describe en su correspondiente apartado.

Las pautas de uso de los equipos informáticos para el alumnado y el profesorado vienen expresadas en las normas del Reglamento de Régimen Interno del Centro y en las normas de uso de las aulas de Informática y Tecnología.

Las estrategias para formar y concienciar a los alumnos en el uso correcto y seguro de las nuevas tecnologías se trabajan a lo largo de cada curso en las tutorías a través de talleres, charlas de orientación, día de internet seguro, etc., donde se tratarán temas relacionados con la seguridad en

Internet: Suplantación de identidad, redes sociales, uso de dispositivos móviles, riesgos en internet (Ciberbullying, Grooming, Sexting), etc.

El coordinador de convivencia y la orientadora del centro utilizan el programa SOCIOESCUELA para evaluar las relaciones interpersonales en el centro, ciberbulling, acoso…

Para las familias también hay formación en tecnología a través de la "Escuela de Padres" que se impulsa en colaboración con el departamento de Orientación y la AMPA. Igualmente, se les da información sobre iniciativas formativas en este campo puestas en marcha por la Consejería de Educación, la Dirección Provincial...

En la Web del instituto hay un enlace permanente de Seguridad Digital para promover un uso seguro y responsable de internet orientado a familias, alumnado y profesorado en el que se facilitan accesos a recursos de autoridad en buenas prácticas e internet seguro, como el Plan de Seguridad y Confianza Digital Educacyl o a Internet segura for Kids isk4:

- ***http://iesantoniotovar.centros.educa.jcyl.es/sitio/index.cgi?wid_item=587&wid_seccion=1***

Criterios de evaluación de seguridad de datos, redes y servicios y su adecuación a la normativa de protección de datos y seguridad:

Evaluar un riesgo implica considerar todos los posibles escenarios en los cuales el riesgo se haría efectivo. La evaluación de riesgos consiste en valorar el impacto de la exposición a la amenaza, junto a la probabilidad de que esta se materialice. El impacto, por su parte, se determina en base a los posibles daños que se pueden producir si la amenaza se materializa, por ejemplo, un impacto sería despreciable si no tuviera consecuencias sobre el interesado o, por el contrario, un impacto sería significativo si el daño ocasionado sobre los derechos y libertades del interesado fuese crítico. Según la probabilidad y el impacto, asociados a las amenazas, es posible determinar el nivel de riesgo inherente.

CRITERIOS:

- Gestión de las incidencias que se produzcan para resolverlas lo antes posible, dando parte al Coordinador o directamente al Servicio de mantenimiento, siempre con conocimiento del Equipo directivo.
- Configuración de usuarios y contraseñas para los equipos que por la seguridad de sus datos lo requieran.
- En el caso de uso inadecuado e incidencias en materiales y servicios, el centro aplicará el RRI.
- En el supuesto de incidencias de seguridad o mal uso de información, documentación o datos se dará parte inmediato a la Dirección Provincial de Educación para actuar de la forma adecuada.
- Mantenimiento actualizado de la Web para evitar amenazas.

ACTUACIONES CONCRETAS Y PROPUESTAS DE MEJORA E INNOVACIÓN:

- Instalación de mayores medidas de seguridad y protección en los equipos destinados al uso de los alumnos y profesores.
- Mejora de la accesibilidad y seguridad de la red wifi.
- Aumento de la partida presupuestaria destinada a la adquisición de equipamiento informático
- Elaboración de un Plan de Reciclado de Equipos y Consumibles, en la actualidad se hace, pero no existe una sistemática de actuación al respecto.
- Estructurar las medidas de seguridad que garanticen la protección de datos especialmente sensibles integrándolas en el plan de confidencialidad y protección de datos del centro.
- Asesoramiento en seguridad informática.
- Instalación de programas actualizados de control de acceso a los equipos para mejorar la seguridad y la protección de datos.
- Aumento del nivel de alerta ante los mensajes y contenidos recibidos, valorando de quién los recibe, finalidad y seguridad.
- Establecimiento en el centro del día de Internet seguro.
- Charlas de concienciación en ciberseguridad.