Normativa y Seguridad del Entorno de Trabajo Digital en Escuelas Pías de S. Fernando

Características del Entorno:

El entorno de trabajo digital del colegio está amparado bajo el ecosistema Google Workspace for Education Plus. Dicho ecosistema es específico para educación, de modo que hace que el entorno de trabajo sea adecuado a usuarios en edad escolar, en lo referente especialmente a la Protección de Datos[1] y a la capacidad de proteger a los alumnos de un uso no adecuado a su cometido educativo o su edad.

El entorno de trabajo está dirigido al uso de herramientas con impacto educativo que permiten el trabajo colaborativo, la indagación, investigación y el desarrollo de las competencias educativas en las diferentes áreas.

Las herramientas de uso escolar con impacto educativo son las ofrecidas por el propio entorno de Google Workspace for Education, así como las herramientas de terceros que el claustro de profesores considere apropiadas conforme a la asignatura y la edad de los alumnos.

Usuario del dominio @epsfernando.org

Para poder hacer uso del entorno digital del colegio cada alumno disfrutará de un usuario dentro del dominio, *alumno.nombre.apellido@epsfernando.org*

---

1 Google Workspace for Education cumple estrictos estándares educativos en materia de privacidad y seguridad.

Nos sometemos a varias auditorías externas e independientes con regularidad. Las auditorías, evaluaciones y certificaciones de Google incluyen:

- ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 y SOC 3, BSI C5 (Alemania), PCI DSS, Cumplimiento de las directrices del FISC, Esquema Nacional de Seguridad (ENS) (España)

Google Workspace for Education se puede usar para cumplir los requisitos de conformidad y de informes estipulados en el: Reglamento General de Protección de Datos (RGPD), Cláusulas Contractuales Tipo de la UE

https://cloud.google.com/privacy/gdpr/?hl=es#tab1

El uso de dicho usuario lleva asociadas una serie de consecuencias y por lo tanto responsabilidades en su uso.

El alumno se compromete a hacer un uso exclusivamente educativo de dicho usuario del dominio y conforme a las directrices dadas por los profesores de las diferentes asignaturas.

Toda actividad realizada con dicho usuario, ya sea de páginas visitadas, aplicaciones utilizadas, registros, *login o signin,* deja rastro en la red y en los sistemas. De este modo si un alumno realiza algún tipo de actividad no adecuada, ésta dejará como parte del rastro al propio colegio, con las consecuencias y responsabilidades que ello conlleva.

Por todo ello, será el alumno[2] el responsable del uso indebido de dicho usuario. Si un alumno tiene dudas acerca de un uso, aplicación, página web, etc. deberá ponerlo en conocimiento de sus profesores o de sus familiares o tutores, de modo que pueda ser aconsejado a este respecto.

No está permitido el uso de dicho usuario para hacer *Sign in with Google,* u otro tipo de registros en aplicaciones no autorizadas por el colegio. Hay que tener especial cuidado con este tema puesto que en ocasiones el perfil está asociado a teléfonos móviles y si no nos percatamos de que dicho perfil puede estar activo podemos llegar a registrarnos en aplicaciones de terceros con dicho perfil. Una buena práctica sería no dar de alta la cuenta del colegio en teléfonos móviles.

El uso de la cuenta del colegio es personal e intransferible. El usuario se compromete a hacer un buen uso de la contraseña y mantenerla a buen recaudo.

El colegio se reserva el derecho de suspender las cuentas de usuario en periodos largos de vacaciones o cuando lo crea conveniente. No está permitido anunciar la cuenta del colegio como correo de contacto a otras personas ajenas al colegio sin el consentimiento del colegio.

El usuario de cuentas @epsfernando.org utilizará los datos sensibles, mediante las herramientas asociadas al dominio, siempre conforme a las leyes de Protección de Datos (LOPD-RGPD), y la Ley de la Sociedad de la Información y el Comercio Electrónico (LSSI), así como la Ley de Propiedad Intelectual, vigentes en cada momento, y en lo que respecta a su uso y está en su mano como usuario y no como administrador del servicio.

[2] O sus padres/tutores si el alumno es menor de 14 años.

Los alumnos no podrán compartir fuera del dominio del colegio documentos pertenecientes al mismo o con membretes y sellos del colegio.

Uso del chromebook

Los alumnos, desde 6º de Primaria hasta 2º de Bachillerato tendrán a su disposición un chromebook como herramienta educativa. Dicho dispositivo presenta enormes ventajas en cuanto a su uso en un entorno de enseñanza y aprendizaje y de trabajo colaborativo.

El alumno se compromete a un uso adecuado de dicho dispositivo, y sólo para sus necesidades escolares y académicas. Hasta 4º de ESO sólo es posible el uso del chromebook con el usuario del dominio @epsfernando.org con lo cual aplica a su uso todo lo mencionado en el punto anterior.

El alumno es el responsable y se compromete al cuidado del dispositivo tanto a nivel físico (golpes, recomendación de funda protectora, manipulación del mismo, uso de cargadores y periféricos adecuados) como en cuanto a su uso y a hacer un uso responsable que no impacte negativamente en su salud (excesivo tiempo de exposición a la pantalla, máx 2h diarias, uso de filtro de luz azul, iluminación adecuada de la ubicación para su uso, actitud postural en su uso, limitación en el uso de auriculares y volumen adecuado)

Protección del entorno digital

El colegio pone en juego todos los medios que tiene a su alcance para proteger el entorno digital usado por los alumnos y docentes. Entre las medidas puestas en juego se encuentran las siguientes:

- Elección del entorno Google Workspace for Education Plus:

  Se trata de un entorno pensado para entornos educativos y que cumple con la Regulación Europea en Protección de datos, permitiendo incluso trasladar la región de datos a Europa.

  Dicho entorno permite el seguimiento y control de la actividad realizada por los alumnos, donde todo deja rastro en la red o los sistemas. De este

modo podemos detectar situaciones o comportamientos anómalos o indebidos y tomar las medidas necesarias.

A este respecto el colegio se reserva el derecho de suspender cuentas de usuario, auditar tráfico o datos de usuarios desde la cuenta @epsfernando.org cuando haya fundados sospechas de un uso indebido y con el fin de aclarar lo ocurrido.

El entorno permite adecuar aplicaciones como gmail o youtube a la edad de los alumnos, no permitiendo su uso o uso indebido en función de la edad.

El resto de aplicaciones del ecosistema como Google Classroom, Google Meet, Google Docs, etc. están pensadas para su uso educativo y contienen medidas de seguridad y preventivas de un mal uso adecuadas al entorno.

- Filtrado de tráfico y de aplicaciones.

  El colegio uso filtrado de tráfico para proteger el acceso indebido a contenidos o aplicaciones no apropiadas para la edad de los alumnos o ajenas a un uso académico.
  Dicho filtrado se realiza en función de la edad de los alumnos y de los requisitos recomendados por los docentes en las diferentes materias, de forma que permita el acceso a los recursos que éstos consideran necesarios.

  En ocasiones se personaliza dicho filtrado en función de las características concretas o especiales de los alumnos.

  A este respecto cabe mencionar que el colegio pone a disposición de las familias, a través de la plataforma del colegio y de forma sencilla e intuitiva, el control parental, de modo que los padres o tutores de los alumnos pueden dar preferencia a las políticas por ellos definidas cuando el dispositivo esté fuera del colegio. Este control parental les permite incluso el corte de internet o apagado del equipo según su conveniencia.

- Protección del chromebook

  El chromebook queda protegido de modo que:

  - Queda enrolado en la organización del colegio.

- No admite el uso de usuarios diferentes a la cuenta @epsfernando.org del colegio. De este modo no es posible el uso de cuentas personales ni la navegación en modo incógnito.
- No admite la instalación de aplicaciones no autorizadas por el colegio.
- El control físico de puertos USB, bloqueo de cámara, etc. puede ser operado por parte del colegio si las circunstancias lo aconsejan.
- El chromebook es un sistema muy seguro, no habiéndose detectado a día de hoy ningún ataque ransomware a este tipo de dispositivos.

- FW perimetral del colegio

  Además del filtrado software mencionado anteriormente, el colegio cuenta con un FW perimetral en el acceso a internet de modo que aumenta los niveles de seguridad de todos los equipos que trabajan en la red del colegio.

- Supervisión por parte del profesorado

  El uso del chromebook en las instalaciones del colegio está supervisado por los profesores presentes en el aula, de modo que se evite el uso inadecuado del mismo.

  Los profesores cuentan, además con la posibilidad de imponer normas específicas de filtrado para sus propias clases.

- Supervisión de la seguridad del alumno

  El colegio cuenta con herramientas, apoyadas en IA, que son capaces de rastrear de forma proactiva el tráfico y detectar imágenes o mensajes que pueden afectar a la seguridad de los alumnos, desde búsquedas realizadas en la red que son inadecuadas a la edad o entorno escolar o puedan ir contra la salud, hasta vocabulario usado en los mensajes o imágenes utilizadas.

  En el caso de que un comportamiento de este tipo sea detectado es remitido a la Comisión de Coordinación Pedagógica la que conjuntamente con el Departamento TIC valorarán la situación aplicando, en su caso el RRI.

Sesiones sobre el uso correcto del entorno a los alumnos

Cada curso, desde el centro, se imparten sesiones a los alumnos con el fin de enseñarles a hacer un uso correcto del entorno. Se hace especial mención del uso que se espera del entorno, así como de los peligros asociados a un mal uso del mismo y las responsabilidades asociadas.

Esto forma parte de la Competencia Digital que por ley debemos proporcionar a los alumnos.

Reglamento de Régimen Interior

Como parte de las medidas de seguridad, el colegio contempla dentro de su RRI las sanciones correspondientes al uso indebido del entorno. Dicho uso indebido está categorizado en función de la gravedad de las acciones.

Son especialmente graves las acciones conscientes por parte del alumno cuyo fin es romper las medidas de seguridad para hacer un uso ilícito del entorno así como aquellas que tienen relación con actitudes de acoso o comportamientos agresivos o vejatorios hacia otras personas a través de la red.

Uso de servidores Proxy/VPN

El uso de servidores proxy es frecuente en Internet. Su origen está en la necesidad de proteger servidores web y controlar el tráfico de los usuarios. Se trata de un uso lícito, en su origen, pero que en muchos casos ha derivado en un uso fraudulento o inadecuado.

Concretamente, el uso de servidores proxy puede servir para enmascarar el tráfico IP en Internet. De este modo un usuario puede acceder a un servidor proxy (aparentemente inofensivo) y desde éste saltar, de forma enmascarada y por lo tanto no rastreable o bloqueable, a la página o contenido deseado.

En ocasiones se ha llegado a poder encapsular tráfico IP desde menús de aplicaciones.

Para paliar esta situación el colegio pone en marcha las siguientes medidas:

- Filtrado de servidores proxy:

  Tanto a nivel de FW perimetral como a nivel de filtrado web, son bloqueados los servidores proxy que ambos sistemas de protección detectan como tales.

- Rastreo de tráfico periódico para detectar uso de servidores proxy.
- Políticas específicas gestionadas por cada docente, por grupo/aula/asignatura para permitir sólo aquel tráfico necesario para la clase en curso.
- Evitar aplicaciones desde las cuales se pueda dar el salta a un servidor proxy

No obstante, y a pesar de las medidas anteriores, los sistemas de seguridad empleados no son capaces de mantener actualizada la base de datos de servidores proxy. Surgen nuevos servidores proxy cada día y con nombres o dedicación aparentemente inofensiva que los sistemas no detectan.

Por este motivo la protección total frente al uso de proxy no es posible. No obstante y por dicho motivo permanecemos vigilantes ante su posible uso.

Seguridad del entorno

Conforme a lo expuesto en los puntos anteriores podemos decir que el entorno cuenta con una gran cantidad de medidas de protección para salvaguardar el uso correcto del entorno digital. Sin embargo, no es lo mismo hablar de protección que de seguridad.

El entorno está protegido, pero no podemos asegurar la seguridad del mismo al 100%. Hay factores que se escapan a nuestro control entre los cuales se encuentran:

- **El uso inadecuado del dispositivo y del entorno por parte del alumno:** Esta es la principal medida de seguridad y el alumno o sus responsables legales son los responsables de que dicho uso sea el adecuado. A pesar de todas las medidas empleadas por parte del colegio, siempre es posible que una manipulación inadecuada del dispositivo, del software o simplemente un uso inadecuado por parte del usuario pongan en peligro la seguridad del entorno.

- **Uso de servidores proxy/VPN:** Como hemos comentado anteriormente no tenemos un control total del uso de los mismos, a pesar de que ponemos todos los medios a nuestro alcance para minimizar su impacto. No obstante el uso de estos servidores o túneles a través de menús de aplicaciones, se debe a un mal uso o un uso inadecuado por parte del alumno, que utiliza estos sistemas con el fin de acceder a contenidos no permitidos.

En los dos casos anteriores el colegio declina toda responsabilidad, la cual corresponde al usuario correspondiente y su responsabilidad en el uso del entorno.

Consentimiento informado

Es necesario, por parte de los padres/tutores de los alumnos, el consentimiento informado de toda la normativa anterior.

Se puede acceder a la aceptación de dicha normativa en el siguiente formulario.

Para el acceso es necesaria una cuenta de gmail, en caso de no tenerla, se puede acceder mediante la cuenta @epsfernando.org de sus hijos.

El Equipo Directivo