BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN

Este es un **documento de buenas prácticas** de seguridad de la información dirigido al personal del **Colegio P. Andrés de Urdaneta** con el fin de que tenga conocimiento sobre cuestiones de protección de datos que puedan surgir en su día a día, y así conocer los procedimientos de actuación a la hora de tratar datos de carácter personal.

El centro, como cualquier otra organización que trate datos de carácter personal, debe cumplir con la normativa de protección de datos, y en caso de incumplimiento, puede llegar a enfrentarse a considerables sanciones.

El Reglamento General de Protección de Datos (en adelante, RGPD) introduce nuevos planteamientos que deben ser interiorizados por todo el centro, por lo que éste **ha decidido implantar una serie de medidas de seguridad** y al mismo tiempo comunicarlas e impartir el conocimiento para que la organización cumpla con la legislación relativa a la protección de datos.

Mediante el conocimiento se incrementa el cumplimiento de la legislación, evitando correr riesgos innecesarios y aumentando la protección de la información personal. Por ello, con el fin de evitar actuaciones erróneas o negligentes es necesario ser conocedor de las medidas técnicas y organizativas apropiadas a aplicar por el centro.

Hoy en día, son muchos los activos que se gestionan en un centro educativo (ordenadores personales, teléfonos móviles corporativos, tabletas, portátiles, proyectores, servidores, aplicaciones software, monitores, etc.). De igual modo, la asiduidad con la que se utilizan las plataformas educativas, la página web del centro, redes sociales etc. es cada vez mayor. Es por ello, que se debe prestar especial atención a las buenas prácticas de seguridad de la información.

La concienciación, el sentido común y las buenas prácticas son las mejores defensas para prevenir y detectar contratiempos en la utilización de sistemas de las Tecnologías de la Información y la Comunicación (TIC). Por lo tanto, con el fin de implementar la seguridad de la información y minimizar riesgos es necesario determinar **medidas de seguridad**, así como la observación continua de las mismas.

A continuación, se detallan las medidas de seguridad a adoptar por todo el personal del centro:

SEGURIDAD BÁSICA

- ✓ **Utiliza contraseñas robustas** (que tengan más de ocho caracteres y aparezcan mayúsculas, minúsculas, símbolos especiales (*/-+&%$) y números) **y cámbialas con la periodicidad establecida por el centro** o cuando sospeches que tu sistema ha podido ser comprometido. No reveles nunca tus contraseñas a nadie. (Recuerda que **tu identificador es único y personal**). Usa un gestor de contraseñas.

- ✓ Observa los criterios establecidos por el centro para el **almacenamiento de la información,** de manera que permita la realización periódica de **copias de seguridad de la información que gestionas**, garantizando la recuperación de los datos y la continuidad del negocio en caso de que se materialice alguna amenaza que afecte a los mismos.

- ✓ **Mantén actualizado el antivirus** para que se realicen correctamente los análisis periódicos de los equipos, para así evitar infecciones. **En ningún caso lo desactives**.

- ✓ **No dejes documentos con información delicada a la vista**.
- ✓ **Destruye la información de forma segura** cuando ya no sea necesaria (ej.: mediante proceso de triturado cuando se trate de soporte papel).
- ✓ Recoge los documentos de impresoras compartidas rápidamente y **evita imprimir en impresoras que no tengas controladas visualmente**.
- ✓ Haz un buen uso de los dispositivos móviles asignados (Portátiles, Smartphones, Tablets, etc.) y **separa las comunicaciones personales de las profesionales**.
- ✓ Si detectas cualquier incidente de seguridad **ponte inmediatamente en contacto con los Servicios Informáticos del centro** (SSII), abriendo una incidencia a la mayor brevedad, para mitigar los posibles efectos.

APLICACIONES

La instalación de software puede afectar al rendimiento y la seguridad de tu equipo. Hazlo sabiendo lo que haces.

- ✓ Instala siempre **software autorizado** y proporcionado directamente por el fabricante, **siempre que lo autorice el centro** y siguiendo en todo momento las instrucciones de las personas responsables de los sistemas de información.
- ✓ **Instala las actualizaciones de seguridad** en el sistema operativo y en las aplicaciones, con especial atención en aquellas de carácter crítico.
- ✓ **No ejecutes nunca programas de origen dudoso o desconocido**.
- ✓ **Trabaja habitualmente en el sistema como usuario sin privilegios**, no como Administrador.

NAVEGACIÓN SEGURA

Un alto porcentaje de los usuarios no es consciente de la cantidad de información que, de forma inadvertida e involuntaria, está revelando a terceros al hacer uso de Internet.

Algunas **recomendaciones** para mantener una **navegación segura** son:

- ✓ Accede únicamente a **sitios de confianza**.
- ✓ **Mantén actualizado el navegador** a la última versión disponible del fabricante.
- ✓ **Descarga los programas desde sitios oficiales** para evitar suplantaciones maliciosas, **siempre que lo autorice el centro** y siguiendo en todo momento las instrucciones de las personas responsables de sistemas.
- ✓ **Configura el navegador** para evitar ventanas emergentes.

CORREO ELECTRONICO

Actualmente el correo electrónico sigue siendo una de las herramientas más utilizadas para el intercambio de información y con ello también ha incrementado el número de engaños a usuarios por este medio.

Algunas **recomendaciones** para utilizar el correo electrónico de forma segura:

- ✓ **No pulses en ningún enlace ni descargues ningún archivo adjunto** de un mensaje de correo electrónico que presente cualquier **indicio o patrón fuera de lo habitual**.
- ✓ **No confíes únicamente en el nombre del remitente**. Comprueba que el propio dominio del correo recibido es de confianza. Si un correo procedente de un contacto conocido solicita información inusual, contacta con ese contacto por teléfono u otra vía de comunicación para corroborar la legitimidad del mismo.
- ✓ Antes de abrir cualquier archivo descargado desde el correo, **comprueba la extensión** y no te fíes del icono asociado al mismo.
- ✓ **No pulses en ningún enlace que solicite datos personales o bancarios**.
- ✓ **Evita pulsar directamente en cualquier enlace desde el propio cliente de correo**. Si el enlace es desconocido, es recomendable buscar información del mismo en motores de búsqueda como Google o Bing.
- ✓ **Cifra los mensajes** de correo que contengan información sensible. Es la mejor opción.
- ✓ **Utiliza contraseñas robustas** para el acceso al correo electrónico. Las contraseñas deberán ser periódicamente renovadas.

REDES SOCIALES

El uso masivo de las redes sociales hoy en día es evidente, por lo que se debe prestar mucha atención a la hora de emplear las mismas. La escasa concienciación y el exceso de confianza hacen que el uso de las redes sea inadecuado.

Los **principales consejos** que se pueden dar como buenas prácticas en el uso de redes sociales son:

- ✓ **Cumple de forma estricta las normas e instrucciones** que establezca el Colegio sobre el uso de redes sociales.
- ✓ **Crea el perfil y configura la privacidad** de forma cuidadosa. No te bases en la configuración por defecto que proporcionan las plataformas.
- ✓ Reflexiona sobre todo lo que se publica. Sobre todo, se debe tener especial precaución en el caso de **los alumnos menores de edad** a la hora de publicar sus datos o imágenes/videos en las redes, **debiendo solicitar en todo caso el consentimiento de los mismos** (a partir de los 14 años) **o de sus representantes legales** (hasta los 14 años).

- ✓ Respeta en todo momento la **intimidad de las personas** que aparezcan en las publicaciones.
- ✓ Utiliza las imágenes y/o videos para un **fin legítimo, didáctico e informativo**.
- ✓ Da por sentado que todo lo que se sube en una red social es **permanente**, aunque se elimine la cuenta.
- ✓ Revisa la información publicada. **Elude dar excesiva información**.

BUENAS PRÁCTICAS EN RELACIÓN AL TRATAMIENTO DE DATOS PERSONALES, IMÁGENES Y VIDEOS DE LOS ALUMNOS DE CENTROS EDUCATIVOS

La Agencia Española de Protección de Datos (AEPD) ha editado una guía sobre la normativa de protección de datos adecuada al sector educativo, en la que establece el modo de actuación de los centros docentes respecto al tratamiento de los datos personales de alumnos, profesores, padres o tutores.

A continuación, brevemente se señala a modo pregunta / respuesta una gama de cuestiones que se presentan en el día a día de un centro educativo que pueden resultar de vuestro interés a la hora de que surjan dudas sobre cómo proceder ante determinadas situaciones en las que están presentes datos de carácter personal:

- **¿Pueden los centros educativos captar imágenes de los alumnos durante las actividades escolares?**

Cuando el centro toma imágenes como parte de la función educativa está legitimados para ello. En cambio, cuando la toma de imágenes y/o videos no corresponde a dicha función educativa (por ejemplo, la difusión o promoción del centro) se deberá disponer del **consentimiento** de los interesados o sus padres o tutores.

Asimismo, es posible captar imágenes en eventos desarrollados en el entorno escolar para la única finalidad de que los padres tengan acceso a dichas imágenes. El acceso debe llevarse a cabo con **la previa identificación y autentificación de los alumnos**, padres o tutores (por ejemplo, en la Intranet). Quienes acceden a las imágenes no pueden proceder a su divulgación de forma abierta.

- **¿Puede un profesor grabar imágenes de los alumnos para una actividad escolar?**

Sí, siempre que grabe en el desarrollo de la programación y enseñanza de las áreas, materias y módulos que tengan encomendados. Sin embargo, esto no supone que la imagen y/o video se pueda difundir de forma abierta en internet, ya que solamente deberán estar accesibles para los alumnos involucrados en la actividad, sus padres o tutores y el profesor correspondiente.

- **¿Pueden los familiares de los alumnos que participan en un evento abierto a las familias grabar imágenes del evento?**

Sí, siempre que las imágenes captadas sean **exclusivamente para su uso personal y doméstico**. En el caso de que las imágenes captadas por los familiares se difundieran, por

ejemplo, mediante una publicación en internet, serían los familiares quienes asumirían la responsabilidad.

Es conveniente que el centro informe a los familiares de dicha responsabilidad.

- **¿Si unos padres se niegan a que se tomen imágenes de su hijo en un <u>evento en el centro educativo</u>, ¿se ha de cancelar dicho evento?**

No. Se debe informar a los padres que la toma de fotografías y/o videos es posible como actividad exclusiva para uso personal y doméstico.

- **¿Pueden los centros escolares prohibir la toma de imágenes en sus instalaciones?**

Si. El centro escolar puede establecer el criterio de no permitir que las familias graben en los eventos escolares.

- **¿Es posible la grabación de imágenes de actividades desarrolladas fuera del centro escolar?**

Requiere el consentimiento de los interesados o de sus padres o tutores, siempre que no se realice en ejercicio de la función educativa. En el caso de que la grabación se realice por terceros (por ejemplo, los responsables de una empresa, un museo que estén visitando), será obligación de estos terceros disponer del consentimiento.

- **¿Se puede publicar en el comedor del centro el menú de los alumnos?**

Si, ya que puede haber alumnos con necesidades alimentarias especiales. Sin embargo, no hay necesidad de que exista un listado público con nombre y apellidos en relación al menú que le corresponde, pudiendo disponer el centro de esos listados para el servicio de comedor.

En caso de que la **necesidad sea imperiosa, la salud del menor prevalece** sobre la protección de datos.

- **¿Pueden los centros colocar en los tablones de anuncios o a las puertas de las aulas la relación de alumnos por clases y/o actividades?**

Si, durante un tiempo razonable para informar a los interesados sobre la distribución. Si el centro educativo dispone de una plataforma para la gestión educativa, se recomienda acceder a dicha información a través de ella (mediante identificación de usuario y contraseña).

- **¿Se pueden hacer públicas las calificaciones escolares?**

Las calificaciones de los alumnos se deben facilitar a los mismos y a sus padres. Se pueden notificar a través de **plataformas educativas siendo accesibles mediante usuario y contraseña**. No obstante, es posible también mostrar la calificación en el entorno de la clase mostrándolas o enunciándolas oralmente, siempre y cuando se eviten los comentarios adicionales que puedan afectar personalmente al alumno.

- **¿Se pueden publicar en la web del centro los datos de los profesores, tutores y otros responsables del centro? ¿Y de los alumnos?**

Cuando se trata de una web en abierto, es decir, cuando puede acceder cualquier persona de manera indiscriminada y no resulta necesario para la función educativa es necesario contar con el consentimiento previo. En cambio, si la información que se publica está restringida a los alumnos, padres o tutores se puede publicar, informando a los docentes de ello.

En el caso de que se publiquen **fotografías o videos de alumnos** es necesario obtener el consentimiento. Podría llevarse a cabo de manera que no se pudiera identificar a la persona, por ejemplo, pixelando las imágenes.

Asimismo, es posible la publicación de imágenes o videos de eventos desarrollados en el entorno escolar con la única finalidad de que los padres tengan acceso, siempre que sea en un entorno seguro con previa identificación y autentificación.

Para más información:

http://www.tudecideseninternet.es/agpd1/images/guias/GuiaCentros/GuiaCentrosEducativos.pdf