SEGURIDAD DIGITAL EN CONSERVATORIOS: MANUAL DE AYUDA PARA ALUMNOS/AS

1.- Privacidad y seguridad en internet

A lo largo de todos los días del año, desde que nos levantamos hasta que nos acostamos el uso y la dependencia de la información que nos proporciona Internet es una realidad, convertida en hábito, que nos condiciona casi de forma inconsciente. Lo primero que cogemos es el móvil.

El uso de las llamadas Nuevas Tecnologías rige nuestras vidas, condicionas nuestras relaciones, controla nuestros procesos de aprendizaje, de trabajo, de relaciones personales.

Todos somos conscientes, en mayor o en menor medida, del tiempo que pasamos diariamente en las redes sociales, se llamen como se llamen, pero ¿somos conscientes de lo que supone ese comportamiento?, ¿controlamos y somos conscientes de los beneficios o de los riesgos que ello conlleva?

Este es nuestro objetivo y nuestra responsabilidad, acercar los beneficios, pero también los riesgos que el uso de las Nuevas Tecnologías ofrece a los alumnos de nuestro centro. Estamos en un Conservatorio Profesional de Música y el buen uso que esos recursos nos ofrecen en vuestra formación, y en la nuestra, es el objetivo de esta publicación. Cómo podemos trabajar, estudiar mejor con los recursos que están en la red y cómo controlar que ese medio no nos controle a nosotros, a vosotros.

Es por ello, que este documento va dirigido, especialmente a vosotros, los alumnos. En un porcentaje muy elevado sois alumnos menores de edad y los recursos formativos que compartimos con vosotros, de forma online, obliga en muchos casos a lo padres a ser los destinatarios de estos. Nuestra responsabilidad, la de todos los implicados en el proceso educativo, es conocer las ventajas y los inconvenientes, la seguridad y los riesgos de su uso.

Y la primera premisa que debéis tener presente es cuidar vuestra privacidad. Vuestra información personal: nombre y apellidos, dirección, teléfonos (casa o privado), documento nacional de identidad, edad, centro de estudios, aficiones, etc. no se proporciona a nadie, salvo que lo padres o tutores lo autoricen, o sean datos requeridos por organismos oficiales de pleno conocimiento del interesado.

2.- Uso saludable de Internet

Entre los temores que los padres tienen en relación con el uso y acceso de sus hijos a Internet se encuentran saber las páginas que visitan, con quién se comunican, que contenidos son los que les interesan, y otros muchos. Y, además, estos padres se preguntarán ¿es seguro moverse por la red?, ¿qué riesgos acechan a los usuarios?

Hoy está muy en boga el concepto "ciberseguridad en la red", concepto que cada usuario cree saber definir, pero que muchos no podemos desarrollar en profundidad. Oímos hablar de estafas en la red, de suplantación de identidades, de *malware*, de contraseñas seguras, de encriptaciones, etc. Pero todo este lenguaje, a qué se debe.

Solo con un clic accedemos a información, abrimos correos, entramos en páginas aparentemente inofensivas, con presencia muy atractiva y con contenidos que nos atraen.

¿Todo ello es en apariencia muy honesto? No siempre. Debemos ser conscientes que nuestra actividad delante de un terminal esta controlado por organismos, personas, asociaciones, etc., y el uso que se hace de esa información que facilitamos excede a nuestra capacidad de control. No hay nada que hagamos en nuestro ordenador que no quede constancia de ello en algún servidor o en algún proveedor informático. Se hace pues necesario conocer o tener presente algunos conceptos.

2.1.- Ingeniería social

¿Qué es? Es la técnica usada por los ciberdelincuentes que consiste en engañar o manipular a las personas para conseguir información personal o para obtener acceso a sus equipos

¿Cómo preparan el engaño? Los términos más comunes, que definen los procedimientos que emplean para conseguir esos propósitos son: *phishing, sextorsión, smishing, baiting, dumpster diving,vishing, shoulder surfing, ransomware*, *quid pro quo* o redes sociales.

- Un primer paso es la investigación sobre la víctima, recogiendo información sobre ella.
- En segundo lugar, se configura un "gancho", se elabora un engaño para ganarse la confianza de la víctima: un premio, una devolución, una suscripción. Todo en una apariencia oficial de una página institucional oficial, seria y de garantías.
- En tercer lugar, la ejecución. Manipulación de la víctima para que facilite la información necesaria o lleve a cabo una serie de pasos. Información

de índole personal y económica: dirección, DNI, cuenta personal, tarjeta de crédito (incluso código de acceso).

- En cuarto lugar, el ciberdelincuente, obtenida esta información sale de este contexto y borra las huellas para no poder ser descubierto

2.2.- Peligros y repercusiones del uso inadecuado de las nuevas tecnologías.

En el momento que se suben datos, fotos a Internet esa información queda ahí para toda la vida. Cada vez que se publica una foto en una plataforma social, esa foto pasa a ser propiedad de todos los usuarios y deja de ser controlada por los padres o por los usuarios de esa red. No controlamos el alcance de nuestras publicaciones y el buen o mal uso de estas.

Qué tiene que saber los “nativos digitales”.

- En primer lugar, que nada es gratis en la Red
- Deben saber los límites entre lo publico y lo privado
- En la vida hay límites y alcanzar cualquier objetivo implica esfuerzo. Nada se consigue de forma inmediata
- Es imprescindible contrastar y saber buscar información. Tenéis que aprender que, cuando queréis buscar temas que os interesan, deis acudir a páginas oficiales, a páginas que ofrezcan calidad y seriedad en la información, y que os permitan contrastar esas informaciones con otras páginas menos oficiales.
- Pero, además, qué dedicación diaria será saludable y cuánta es perniciosa para nuestra salud, para nuestras tareas formativas, para nuestras relaciones sociales, ¿o familiares?
- ¿Qué consecuencias, de todo tipo, tiene el uso excesivo de nuestras conexiones a la red?

Problemas de obesidad, trastornos del sueño, trastornos de comportamiento, como la ira o la agresividad son consecuencia de un mal uso de esas tecnologías.

La emisión de la radiación que los aparatos producen es una alarma que la OMS califica como riesgo de clase 2B (posible cancerígeno).

2.3.- Fomento del uso responsable

No debemos impedir su acceso, pero si limitar y enseñar un uso saludable de las TIC. Son muchas y muy diversas las formulas utilizadas por los ciberacosadores. El acosador se aprovecha del anonimato para hacer daño y utiliza la red para que el hecho delictivo sea extensivo y mucha gente pueda acceder a ese mal uso, generando mucho daño a la víctima, lo que provoca al acosador un gran disfrute. Los padres deben tener presente que las acciones de

un menor son responsabilidad directa de ellos, que son los que deben responder ante la ley de esas presuntas malas acciones de sus hijos.

¿Qué hacemos? La víctima, cuando no conoce al acosador, debe recopilar datos, bloquear y denunciar en plataforma y denunciar ante FFCCSE. Si conoce al acosador: recopilar pruebas, ponerse en contacto con el o ella y sus responsables; ponerse en contacto con el centro educativo y si no cesa el acoso, denunciar. Pero además debe haber un plan en su propia casa, en su familia: debe haber diálogo y comunicación; no culpabilizar; disposición total a solucionar el problema; preguntas abiertas y no dirigidas; acordar y explicarle lo que se va a hacer; y por último acudir a un psicólogo.

No vamos a enumerar todas, pero si aquellas que afectan, según los estudios, a uno de cada dos menores. *Ciberbullyng, grooming* o *sexting* son términos que definen esas malas prácticas

- El *ciberbullyng:* acoso o maltrato a menores por la red. Cuando se repite esta acción es cuando se entra en este tipo de acoso. El menosprecio, hacer circular información despreciativa sobre un menor, enterarse de un secreto y difundirlo en la red, inventarse un bulo y hacerlo circular, excluirle de las relaciones entre compañeros, etc.
- El *sexting*: envío de fotos o videos de carácter sexual a través de la red. Se empieza a practicar en la pre-adolescencia, 12 -13 años. Se puede realizar de forma activa o de forma pasiva. En muchos casos son las chicas las que lo hacen de forma activa y los chivos lo practican de forma pasiva, difundiendo esos contenidos.

  Cuando una foto se manda a alguien conocido nuestro, debemos saber que no estamos mandando la foto en cuestión o el video a esa persona, se lo estamos mandando a una empresa: WhatsApp, Gmail, etc. Estas empresas ya difunden el contenido y se convierten en los dueños de ese material.

  Ni las personas somos seguras ni somos fiables y podemos por un error mandar información a la persona equivocada o a un grupo equivocado, lo cual puede generar problemas de por vida. Con esta mala practica lo primero que hay que hacer es no generar ese material; en caso de que me llegue no lo difundo y lo denuncio a las autoridades.

- *Grooming*: se refiere al acoso sexual de un adulto a un menor a través de las pantallas.
- *Vamping/Descanso*: quitarse tiempo de descanso por estar con las tecnologías, sean las que sean, entre las manos, viendo videos de youtube, chat, WhatsApp, facebook, instagram, etc. El respeto al tiempo de descanso debe ser irrenunciable y en ningún caso un menor debe quitarse tiempo de descanso para estar con el móvil o la Tablet.

- Contenido inapropiado, tanto de carácter sexual, como de temática violenta, delincuencia, conducción temeraria, retos macabros,
- Comunidades online de riesgo: promueven o promocionan conductas peligrosas.
- Modas, retos y juegos que ponen en serio peligro la integridad de lo jóvenes
- Código PEGI: edad y contenidos de los videojuegos.
- Consecuencias del uso o del abuso de las nuevas tecnologías: físicas, irritación y fatiga ocular, tendinitis en pulgares o problemas de túnel carpiano, obesidad, dolores de espalda, sordera, codo de tenista, etc. A nivel lega, el uso irresponsable conlleva consecuencias para la familia, en la institución educativa, y lógicamente para el menor.

2.4.- Educación digital menores: educación conductual y educación tecnológica.

La prevención siempre comienza fomentando una comunicación sana con los menores y haciéndoles participes de los riesgos a los que se enfrentan al compartir su información personal en Internet. Deben saber qué tipo de contenidos pueden ser públicos y cuáles deberían mantener en privado.

“Pensar antes de publicar” siempre es una buena pauta. Antes de compartir contenido deben reflexionar sobre qué pensará quien lo vea, cómo lo podrá utilizar y qué posibles consecuencias podría tener, tanto en el presente como en el futuro.

Fomentar este pensamiento crítico no sólo incluye pensar en la propia privacidad, sino también en la de los demás. A la hora de compartir información sobre otras personas, es necesario pedir permiso y guardar su intimidad

Existen multitud de medidas tecnológicas que os ayudarán a proteger la información que publicáis:

- Opciones de privacidad. Configurarlas adecuadamente es imprescindible en cada aplicación o servicio que utilicéis. A menudo os puede resultar complejo, por lo que podemos recurrir a recursos que están a nuestra disposición, como la Guía de Privacidad y Seguridad en Internet de la OSI y la AGPD.

- Opciones de seguridad. Hoy en día cualquier servicio (redes sociales, servicios online, etc.) o dispositivo (ordenadores, tablets y teléfonos móviles), contiene mucha información privada que debe protegerse. El uso correcto de contraseñas robustas, bloqueo de pantalla, preguntas de seguridad y otras opciones de acceso es esencial para limitar el acceso.

- Control de contactos y amistades. Es habitual que los menores añadan en sus redes sociales a personas que realmente no conocen, con lo que su información acaba en manos de personas totalmente extrañas. Es importante promover una lista de contactos segura, para que puedan controlar con quién comparten la información.

- Sincronización. Muchas aplicaciones conectan nuestra cuenta de usuario con otras aplicaciones (como, por ejemplo, para tuitear automáticamente las fotos de Instagram). Debemos revisar los permisos de privacidad de cada aplicación, para evitar publicar información no deseada.

- Uso de equipos públicos. Es recomendable evitar su uso si se va a gestionar información sensible o privada. No obstante, de hacerlo, se recomienda utilizar la opción de navegación privada del navegador, no guardar las contraseñas y cerrar sesión de los servicios al finalizar para evitar que cualquiera que utilice el equipo a continuación pueda acceder a nuestro correo electrónico, redes sociales, banca online, etc.

- Selección de aplicaciones y redes sociales. Es importante leer las condiciones y permisos de cada servicio para saber si son adecuadas o suponen una amenaza para la privacidad. Esta situación también aparece al utilizar aplicaciones de terceros dentro de otros servicios, como juegos en redes sociales.

3.- Plan estratégico educativo de seguridad y privacidad en la red.

Riesgos y propuestas antes incidentes

- Apoyo al menor: Es fundamental reaccionar con calma y no culparle de la situación, manteniendo la comunicación y la confianza: cuenta con nuestra ayuda y comprensión.

- Establecer nuevas medidas de seguridad: Si observamos que existe información privada publicada sin consentimiento, es necesario cambiar las contraseñas de los servicios online utilizados, ya que alguien puede haber accedido a ellos sin permiso.

- Comunicación: Si otra persona ha difundido información personal del menor, la primera opción es contactar y hacerle ver que esa información es privada y debería borrarla.

- Reporte al proveedor de servicios: Si el paso anterior no es suficiente, se debe contactar con los responsables del servicio donde se ha publicado para que tomen medidas.

- Denuncia: Ante una situación de ciberacoso, *grooming*, o suplantación de identidad, así como problemas derivados de la práctica del *sexting*, es importante contactar con las Fuerzas y Cuerpos de seguridad. El centro

de salud y su centro educativo pueden ofrecer al menor apoyo psicológico y emocional si es necesario.

La Agencia Española de Protección de Datos (AEPD) y el INCIBE han elaborado la "Guía de privacidad y seguridad en la red", documento imprescindible que recoge toda la información relacionada con el buen uso de las tecnologías, y que de forma muy resumida se ha trasladado a la presente guía. Acudir a esta fuente es imprescindible para ese correcto uso que todos deberíamos conocer.

https://www.osi.es/sites/default/files/docs/guiaprivacidadseguridadinternet.pdf

Esta guía se compone de dieciocho fichas:

- **FICHA 1:** Tus dispositivos almacenan mucha información privada ¿Te habías parado a pensarlo?
- **FICHA 2:** ¿Por qué son tan importantes las contraseñas?
- **FICHA 3:** ¿Son suficientes las contraseñas?
- **FICHA 4:** No esperes a tener un problema para realizar copias de seguridad
- **FICHA 5:** ¿Será fiable esta página?
- **FICHA 6:** ¿Tengo obligación de dar mis datos cuando me los piden?
- **FICHA 7:** ¿Cómo puedo eliminar datos personales que aparecen en los resultados de un buscador?
- **FICHA 8:** ¿Cómo puedo usar el navegador para que no almacene todos los pasos que doy por Internet?
- **FICHA 9:** ¿Quién puede ver lo que publico en una red social?
- **FICHA 10:** Identificando timos y otros riesgos en servicios de mensajería instantánea
- **FICHA 11:** Toda la información que se publica en Internet ¿es cierta?
- **FICHA 12:** Phishing: el fraude que intenta robar nuestros datos personales y bancarios
- **FICHA 13:** ¡Qué le pasa a mi conexión de Internet!
- **FICHA 14:** Quiero proteger mi correo electrónico
- **FICHA 15:** ¿Qué tengo que tener en cuenta si guardo mi información personal en la nube?
- **FICHA 16:** ¿Puedo compartir ficheros por Internet de forma segura?
- **FICHA 17:** No tengo claro para qué está utilizando mi hijo Internet, ¿qué puedo hacer?
- **FICHA 18:** ¿Las pulseras y relojes que miden la actividad física son seguros?

Internet segura: Is4K for side (Incibe); OSI, oficina de seguridad del internauta; Pantallas amigas. Son algunas de las referencias de direcciones a las que podemos acudir para informarnos y formarnos. El presente documento está inspirado en la formación e información facilitada por profesionales que

trabajan en un campo tan amplio como es la ciberseguridad y que debería ser una prioridad para todas las personas, jóvenes y adultos, formadores y alumnos, padres y madres, pues de su buen uso o del mal uso de las nuevas tecnologías va a depender su buen desarrollo educativo, personal, social, afectivo o incluso económico. Nuestro agradecimiento al INCIBE por la documentación que nos facilitan y que sin ella todo sería mucho más fácil para esos ciberdelicuentes que nos acosan y que cada día generan tantos y tantos males. Para mayor información siempre es recomendable acudir a las fuentes que se indican a continuación.

GUÍA DE SEGURIDAD EN REDES SOCIALES (RRSS)

https://www.incibe.es

https://www.is4k.es.