ÁREA INFORMÁTICA

LICEO RUIZ TAGLE

PROTOCOLO DE CIBERSEGURIDAD Y PROTECCIÓN DE DATOS

LICEO RUIZ TAGLE

ESTACIÓN CENTRAL

ÍNDICE

1. INTRODUCCIÓN

Nos encontrados a comienzos del siglo XXI, vivimos en una era tecnológica llena de innovación, oportunidades, mejoras y peligros. Es cierto que la tecnología nos abre infinidad de caminos, caminos que tenemos que descubrir a base de ensayo y error. No hay mayor aprendizaje que aprender de los errores y los centros educativos desempeñan una gran labor en ese aspecto.

La tecnología forma parte de nuestras vidas. Desde el momento que nacemos y nuestros familiares mandan una foto de un bebé a través de un dispositivo ya estamos poniendo información personal a disposición del mundo. Tenemos la libertad de compartir imágenes, textos y audios con quien queramos, pero a su vez no somos conscientes de que esos datos quedan en Internet para siempre. Por eso, debemos poner medios y evitar que nuestra información pueda ser manejada por otras personas con facilidad.

El correcto uso de los dispositivos digitales por parte de los trabajadores del Liceo nos lleva al desarrollo del aspecto básico de este protocolo, la ciberseguridad.

2. CIBERSEGURIDAD

La **ciberseguridad** es la práctica de defender los ordenadores, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. La seguridad de la información protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito. Para evitar en la medida de lo posible la ciberdelincuencia sólo es necesario seguir una serie de pautas muy básicas y sencillas pero efectivas para ponérselo muy difícil a los ladrones de datos.

2.1 RECOMENDACIONES DE CIBERSEGURIDAD PARA LOS ESTUDIANTES

Muchos de nuestros estudiantes tienen dispositivos móviles, tabletas, quizás algunos hasta tengan portátiles propios y somos conscientes de que la gran mayoría manejan las videoconsolas a la perfección, pues bien, estos dispositivos están conectados a una red Wifi en algún momento. El primer consejo que queremos dar a nuestro alumnado es que tengan en cuenta que no todas las redes Wifi son seguras. Si se conectan a una red de un centro comercial, de un aeropuerto o de un restaurante puede que estén dejando entrar a sus dispositivos algo más que Internet. **No todas las Wifi públicas son seguras.**

Todo aparato tecnológico puede estropearse por dos motivos; porque se ha quedado obsoleto y ya no funciona como el primer día o porque le ha pasado algo ajeno al dispositivo, esto quiere decir que ha recibido un golpe de un agente externo o que le ha entrado un virus que hace nuestro dispositivo no responda a nuestros requerimientos. Por eso no debemos olvidar el **uso de antivirus.**

Cuando nos compramos un dispositivo nuevo lo primero que nos pide en configurarlo, es decir ponerlo a nuestro gusto. Cuando usamos Internet debemos acordarnos de **activar los bloqueos de contenido peligroso** o publicidad irrelevante.

Llega el momento de usar las aplicaciones para comunicarnos con nuestra gente, pero no nos podemos fiar porque en realidad estamos hablando delante de una pantalla ¿quién sabe si estamos hablando la persona que pensamos? **Cuidado con transmitir información personal** porque nunca estamos seguros de quién puede recibir esa información.

Es aconsejable **utilizar contraseñas robustas**, es decir, de difícil desencriptación. Lo ideal es que tenga al menos 8 dígitos, que contenga caracteres alfanuméricos, algún símbolo, mayúsculas y minúsculas, así evitarás que te roben la contraseña y entren en tus cuentas.

Muchas veces ponemos información en los dispositivos para jugar o para hacer tareas. Es recomendable usar siglas o **cifrar los datos** para evitar que sepan tu información personal, por ejemplo, no pongas tu nombre completo, escribe sólo las consonantes.

Cuando entramos a plataformas como Gmail, Classroom, Canvas, etc. Debemos **recordar cerrar sesión** siempre, ya que si usamos un dispositivo electrónico de uso público el siguiente usuario puede entrar en nuestras cuentas o ver nuestra información.

Pasamos una gran cantidad de tiempo con nuestros dispositivos, vamos a la playa, al parque, comemos con ellos al lado eso provoca que se ensucien por fuera. ¿Te has parado a pensar que también se ensucian por dentro? Cuando visitamos páginas web o descargamos archivos siempre se quedan datos, rutas o cookies almacenadas que hacen que nuestros dispositivos vayan lentos o peor aún que alguien se cuele en ellos. Es bueno **limpiar el caché y las cookies o actualizar el software con regularidad.**

Después de todos estos consejos sólo queda recordar que usamos la tecnología para comunicarnos y que no hay nada mejor que hacerlo con educación. **Usa un lenguaje correcto** sin malas palabras ni imágenes desagradables porque detrás de esa pantalla hay otra persona como tú.

2.2 CONSEJOS DE CIBERSEGURIDAD PARA LAS FAMILIAS.

Hoy en día la gran mayoría de las familias tienen Internet en casa, por eso nuestro Liceo, les recuerda algunos aspectos a tener en cuenta para continuar con la protección de datos del colegio a sus hogares. Estas recomendaciones son:

- Cambiar la contraseña Wifi que vienen en el **Router** por defecto. Es aconsejable poner una contraseña diferente que sólo sea conocida dentro de ámbito familiar.
- Instalar antivirus en todos los dispositivos conectados a Internet. Normalmente los dispositivos tienen antivirus instalado, pero sólo por unos meses ya que es de prueba. Es recomendable asegurarse de que el antivirus va a estar activo a largo plazo.
- Revisar los permisos de las aplicaciones. Cuando instalamos una **App** estamos aceptando todas sus condiciones, debemos cerciorarnos de no permitir el acceso a la cámara o al micro siempre que no sea necesario.
- Eliminar aplicaciones que no se utilicen. Tener aplicaciones que no hacen falta es innecesario ya que estás dejando acceso a tus datos sin recibir nada a cambio.
- Elegir contraseñas seguras siguiendo los consejos de encriptación. Una contraseña robusta es la mejor barrera para evitar posibles peligros.
- Realizar copia de seguridad de los datos.

- Actualizar regularmente el software del dispositivo. Si renovamos el sistema interno de nuestros dispositivos siempre estaremos mejorando las prestaciones, seguridad y capacidad del mismo.
- Asegurar los dispositivos con contraseñas, PIN o información biométrica. Hoy en día llevamos tecnología por todas partes y con ella parte de nuestra vida, es imprescindible poner barreras para que en caso de pérdida del dispositivo no sea fácil entrar en él.
- Revisar la configuración de privacidad de las cuentas y redes sociales. Debemos revisar las opciones que nos proporcionan las cuentas y redes sociales en las que nos registramos ya que nos pueden llenar de correos o notificaciones irrelevantes o incluso compartir nuestra información sin darnos cuenta.

2.3 SUGERENCIAS DE CIBERSEGURIDAD PARA LOS TRABAJADORES/AS DEL LICEO RUIZ TAGLE

El Liceo dispone de varias redes Wifi que están distribuidas por todo el colegio, cuyas contraseñas son entregas a los funcionarios. Una de las primeras recomendaciones es **NO** entregar estas claves a los alumnos y evitar colocar estas contraseñas a la vista de los estudiantes.

Deben proteger sus credenciales de acceso (usuario y contraseña) de todas las plataformas que ocupan en el establecimiento. (**Syscolnet**, **Gmail**, **Classroom** y otras páginas educativas)

. Las recomendaciones a seguir son las siguientes:

- Usar contraseñas largas y alfanuméricas.
- Encriptar y asegurar la información sensible.
- Trabajar siempre en entornos seguros.
- No instalar programas no autorizados.
- Confiar sólo en remitentes conocidos.
- Cerrar sesión al salir de cuentas de correo o plataformas educativas.
- Apagar el computador, el último docente que ocupe la sala (proyector, parlante, ordenador).
- Sacar el pendrive de forma segura.
- No utilizar los equipos para ingresar a páginas como **Instagram**, **Tik Tok**, y otras **Redes Sociales**. Además de páginas bancarias u otras importantes de uso privado como: **Servicio Impuesto Interno**, clave única, etc.

2.4 CUIDADO DE DISPOSITIVOS Y SANCIONES

Estamos en un momento de cambio, una situación de transformación digital en la que nuestro Establecimiento Educativo tiene que asegurarse de dar pasos cortos pero seguros. Es un proceso laborioso en el que toda la comunidad educativa está implicada y debido a ello tiene que cumplir unas normas de cuidado y seguridad. Estas normas son sencillas pero inamovibles ya que como se ha citado en anteriores apartados es muy fácil que se filtren los datos.

Se realizarán trabajos de mantención de todos los ordenadores, con relación a sus cookies, caché, aplicaciones no autorizadas, etc.

La mantención se hará a lo menos **3 veces por semestre**, debido a la gran cantidad de equipos, ya que se debe analizar, gestionar y borrar toda la información que pudiera quedar almacenada en los computadores.

Con respecto a las sanciones, el mal uso de cualquier plataforma por parte de los alumnos o trabajadores tendrán las sanciones pertinentes de acorde al REGLAMENTO INTERNO DE CONVIVENCIA ESCOLAR (**RICE**)

3 CONCLUSIONES

Con la elaboración de este documento se pretende actualizar la protección de nuestros usuarios y comunidad educativa. Dadas las circunstancias que la pandemia nos ha dejado hemos sabido apreciar que podemos seguir conectados a través de la tecnología y que ello nos lleva a aumentar las precauciones, ya que es un medio de fácil acceso que nos provoca tanta confianza que le cedemos nuestros datos más personales sin darnos cuenta. Debido a esta circunstancia nace la necesidad de crear este documento que nos ayuda a aprender más sobre toda la información que usamos y transmitimos con las nuevas tecnologías.

Nuestro Liceo Ruiz Tagle tiene la intención de proteger todos los datos con la mayor rigurosidad posible y a su vez aumentar el correcto uso de las nuevas tecnologías en la comunidad educativa.