ESCUELA DEL MAGISTERIO

PROCEDIMIENTO SUGERIDO PARA USO DE VIDEOLLAMADAS

Equipo Directivo y Asesoría Pedagógica

Ante la situación educativa actual durante el período de cuarentena se ha visto la necesidad de generar espacios de encuentros virtuales de los diferentes actores institucionales a través de videollamadas o videoconferencias (docentes con estudiantes, docentes con colegas, preceptores, equipos de gestión, administrativos, etc.).

En particular, el encuentro por videollamadas entre docentes y estudiantes ha sido un medio muy útil para lograr contactos de mayor cercanía y agilizar la vinculación con los jóvenes. Para ello, los docentes han utilizado diversas plataformas que posibilitan videollamadas con distintas características y prestaciones.

Se espera que en dichos entornos, tanto docentes como estudiantes se conduzcan como lo hacen en los salones de clases y tal como se indica en el Compromiso de Convivencia de la Escuela del Magisterio.

Sin embargo, en el Compromiso de Convivencia no se especifican aspectos vinculados con las videollamadas, por lo cual se mencionan a continuación algunas **sugerencias** para el manejo dentro de esos medios y evitar situaciones inapropiadas.

Antes del encuentro:

- Es importante que el docente ingrese al menos 5 (cinco) minutos antes de la hora fijada para que pueda recibir a los estudiantes.
- Es necesario que todos los participantes, incluido el docente, tengan el video encendido.
- Admitir solamente a aquellas personas que se identifiquen con nombre y apellido y cuya identidad corresponda a los estudiantes de su curso. En caso que no se identifique, advertir a esa persona que será expulsada de la sala.

Durante el encuentro:

- Si el docente desea compartir su escritorio, es conveniente que tenga abierto el documento digital a proyectar.
- Evitar mostrar el escritorio personal o hacer búsqueda en la computadora cuando se comparte el escritorio con los estudiantes.
- No ceder el control de la computadora a ningún estudiante.
- Reservar la posibilidad de compartir pantalla solamente para el docente, quien administra el encuentro.
- Usar el chat común sólo para preguntas generales dirigidas al docente.
- Revisar el chat durante el encuentro virtual cada cierto tiempo, para no perder la relación de las interacciones.
- Solicite a los estudiantes que tengan sus micrófonos mudos mientras no estén hablando, para evitar ruido ambiental e interferencias en el sonido.

- Establecer contacto visual y personal con los estudiantes, en la medida de lo posible. Solicitar que los estudiantes tengan la cámara encendida durante el encuentro. En caso de problemas de conexión, pida al estudiante que escriba en el chat para verificar su presencia.
- En caso de detectar algún ingreso no identificado, una vez comenzada la reunión solicitar su identificación. Si esa persona no lo hiciere, expulsarlo de la sala o en caso de emergencia cerrar todos la sesión.

Si ocurrieran situaciones inapropiadas durante la conexión, tanto de los estudiantes como de otras personas que ingresaran sin identificación ni autorización, se recomienda implementar los siguientes pasos:

- Antes de cerrar la sesión, de ser posible, realizar capturas de pantalla para registrar la intromisión de una persona no autorizada o las conductas observadas como inapropiadas, tanto en las imágenes como en el chat.
- Solicitar a los estudiantes que salgan de la sesión y/o sacar de la misma a los estudiantes.
- Buscar un medio de comunicación alternativo con los estudiantes, como whatsapp con el delegado.
- Contener a los estudiantes, dialogar con ellos sobre lo sucedido, compartiendo lo que sintieron y las medidas de protección que cada uno puede tomar en el uso de la tecnología.
- Reportar de manera inmediata vía whatsapp o telefónicamente al Director/a o Vicedirector/a indicando el nombre del docente, curso, horario del encuentro, cantidad de estudiantes conectados. También se podrá informar al Jefe de área.

Después de ocurrido el incidente:

- El docente afectado, luego de la información telefónica a las autoridades plasmará lo ocurrido en un informe escrito que elevará al Equipo directivo.
- El Equipo directivo elaborará un Acta en la que Informará lo sucedido a DIGES. Remitirá la misma al Jefe de área para su conocimiento.
- El Equipo directivo y Servicio de Orientación informarán a las familias lo acontecido y solicitará su colaboración pidiendo información sobre lo ocurrido en el hogar.

Al terminar el encuentro:

- Es muy importante que el docente cierre la reunión, asegurándose previamente que todos los estudiantes hayan salido del espacio virtual.
- La sesión finalizará haciendo click en el ícono del teléfono. Si en lugar de este procedimiento se cierra directamente la ventana de la videollamada, sin tocar el ícono del teléfono, la reunión quedará abierta y la seguridad de quien organizó el encuentro se verá vulnerada.

Como información de apoyo al procedimiento sugerido, incluimos en Anexo las recomendaciones realizadas por el equipo de TICs de la Escuela del Magisterio para mantener comunicaciones seguras mediante videollamadas.

ANEXO

GENERALIDADES DE SEGURIDAD PARA TENER EN CUENTA A LA HORA DE FORMAR PARTE EN SESIONES DE VIDEOCONFERENCIAS

Al momento de tratar el tema de seguridad en el tráfico de datos a través de una red, ya sea computacional o telemática, nos encontramos con diversos inconvenientes, en todos los casos, los proveedores de servicios de conexiones a salas de video conferencias, nos proporcionan seguridad, como también paquetes de actualizaciones que nos proporcionan tranquilidad a la hora de proteger nuestra intimidad académica y privada.

Esta seguridad se ve vulnerada en algunos casos a la hora de conectarnos hacia entornos donde el tráfico de datos se torna de intercambios constantes, donde nuestra PC o Notebook, juega un papel importante.

Los ingresos lógicos indebidos desde el exterior, o ataques informáticos, generalmente se producen para robar información, son cada vez más frecuentes, pero siempre existió.

En estos tiempos de confinamiento social, el uso de estas propuestas alcanza casi el 80%, siendo sumamente necesaria en la enseñanza aprendizaje de la educación a distancia.

Bien, tal vez todos tenemos una computadora con sistema operativo de curso legal, o sea Windows original, pero quien tiene hoy un paquete de office original, pensemos que la mayoría tenemos programas craqueados en nuestras computadoras "piratas", también podemos hablar de antivirus piratas y demás herramientas que utilizamos con frecuencia. Estos programas funcionan en nuestros equipos con seriales, fix, kmspico, etc., todos códigos troyanos, y un virus troyano es invisible a los antivirus, se replica y produce inestabilidad en nuestro sistema.

Esto concretamente es el inicio de la falta de seguridad de nuestros equipos, al no contar con actualizaciones críticas de seguridad por parte de los proveedores de software, somos víctimas de la inseguridad de nuestros equipos, sumado a los ataques externos, estamos seguramente en problemas serios.

En este tutorial vamos a tratar de asegurarnos de que nuestros equipos no revelen identidad propia, y también dificulte el ingreso y la búsqueda de información de atacantes molestos, para de esta forma no generen inestabilidad en nuestro sistema.

Paso 1: Utilizar como navegadores predeterminados Edge ó Google Chrome.

Paso 2: Antes de cada conexión, borrar todos los historiales de conexión, ir a configuración, historial, nuevamente historial, borrar datos de navegación, configuración avanzada, ir a desde siempre, tildar todas las opciones. Borrar.

Paso 3: No tener ningún programa redundando en el ciclo de conexión, por ejemplo, reproductores de audio, procesadores de texto (Word), o cualquier otro.

Paso 4: No tener contraseñas guardadas en el navegador, son fácilmente visibles para cualquiera que acceda al equipo, de forma presencial o externa. Para borrar, ir a configuración, contraseñas, y en ese espacio borrar todas las contraseñas, obviamente hacer un relevamiento para no perder ninguna.

Paso 5: No tener sincronizado el correo electrónico con el navegador, desactivarlo, o directamente no configurar la sincronización del mismo.

Paso 6: No tener ninguna cuenta de correo abierta en el ciclo de conexión, ya que la dirección IP es fácil de obtener.

Paso 7: En el caso de la cuenta de correo sea compartida entre la PC y la cuenta de correo del teléfono celular, dos consideraciones, apagar el teléfono o cerrar sesión momentánea de la cuenta de correo en el teléfono.

Paso 8: **Muy importante:** Desde la barra de tareas buscar "Permitir el acceso remoto al equipo", como lo indica la imagen 1, seleccionar e ingresar.

Luego, ver imagen 2**, <u>des tildar</u>** la opción "Permitir conexiones de asistencia remota a este equipo", y dejar tildad la opción "No permitir las conexiones a este equipo.

Imagen 1

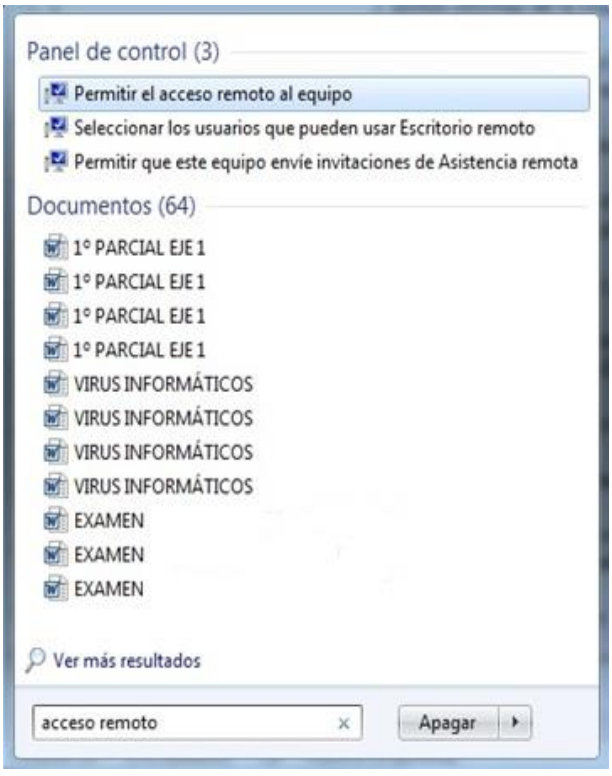

Imagen 2