PRÁCTICAS RECOMENDADAS PARA PROTEGER SU AULA VIRTUAL

1
SELECCIONA UNA APLICACIÓN, LA MÁS SEGURA POSIBLE

Antes de utilizar una aplicación para comunicarnos con nuestros estudiantes e impartir nuestras clases debemos valorar la seguridad que tienen las mismas. Plataformas como Zoom, Microsoft Teams*, Skype, GoToMeeting, Meet, WhatsApp, etc., cada una de ellas tienen ventajas y desventajas que valorar.

2
BLOQUEE SU AULA VIRTUAL

Espere a que todos sus estudiantes ingresen al aula virtual y, a continuación, escoja la opción bloquear reunión o sesión.

3
CONTROLAR EL USO COMPARTIDO DE LA PANTALLA

La actualización de muchas de las aplicaciones ahora nos permiten que el anfitrión sea el único que pueda compartir contenidos en clase de forma predeterminada.

4
NO PUBLICAR IMÁGENES DE LAS SESIONES EN REDES SOCIALES

Se recomienda NO publicar imágenes de sus clases virtuales en redes sociales.

5
BLOQUEAR EL CHAT

Los docentes pueden restringir el uso del chat de la clase para que los estudiantes no puedan enviar mensajes privados o públicos.

6
HABILITAR LA SALA DE ESPERA

Se puede habilitar la opción para que todos los participantes entren primero a la sala de espera y el docente vaya autorizando la entrada a cada uno de sus estudiantes.

7
ELIMINAR PARTICIPANTES

En las actualizaciones de las aplicaciones el anfitrión tiene la opción de eliminar a cualquier participante que considere que no debe estar presente en la reunión.

* Aplicación oficial para el uso de docentes y estudiantes del Ministerio de Educación del Ecuador. La misma está enlazada con los correos y usuarios institucionales.

Todas las opciones descritas estarán en función de la aplicación que utilice. Verificar es indispensable.

El mundo virtual de Eugenia