



## REGLAMENTO INTERNO DE CIBERSEGURIDAD

Los servicios informáticos que se implementan en el ámbito educativo llevan a una alta exposición de los estudiantes a los medios digitales; por lo que se requieren medidas para garantizar la seguridad de las personas, así como el acceso a la información.

Se han establecido normas para resguardar la seguridad y la salud de estudiantes y docentes, siendo las principales:

- El uso de las plataformas FACTS, CLASSROOM y GOOGLE MEET para el desarrollo de las sesiones de aprendizaje. En algunos casos, los docentes pueden utilizar plataformas autorizadas según los programas académicos de cada nivel.
- No habrá reposición de exámenes frente a ausencias injustificadas.
- Evitar sitios web desconocidos que pidan información personal que pueda comprometer su privacidad.
- Mantenerse alerta ante sitios web falsos, páginas engañosas y fraudes electrónicos. Antes de introducir datos en formularios web contraste la información desde páginas oficiales.
- Utilizar software de seguridad antimalware/antivirus
- Respalidar periódicamente su información en lugar seguro. Extremar la precaución al usar memorias USB o descargar archivos.
- Cuando organice o asista a videoconferencias:
  - Deshabilite los micrófonos de los asistentes y la opción de compartir escritorio por defecto.
  - Una vez que la reunión ha comenzado y todos están presentes se recomienda bloquear la reunión.
  - Comparta los enlaces por un medio seguro, no los comparta en redes sociales u otros foros públicos.
  - Desactive la transferencia de archivos para evitar que el chat se sature con contenido no solicitado.
  - Ponga a los asistentes en sala de espera, previa verificación se va aceptando su ingreso.
  - No use los chats de la plataforma para mensajes privados ni comparta información personal.
  - Apague su micrófono.

Para el estudiante:

- ❖ Disponer de un lugar adecuado -sin distracciones, con buena iluminación y buena recepción de señal de internet- para recibir las clases.
- ❖ Conectarse puntualmente usando el correo institucional con la cámara encendida y el micrófono apagado.
- ❖ Mostrar un adecuado arreglo personal y permanecer conectado durante la clase.

- ❖ No es permitido tomar fotografías de las sesiones de clases, grabar video y utilizar fondos virtuales.
- ❖ No es permitido comer durante las clases.
- ❖ Preparar sus materiales antes de la clase.
- ❖ Participar de manera activa, respetuosa y autónoma.
- ❖ Al momento de realizar exámenes es obligatorio mostrar su área de trabajo y permanecer con la cámara abierta.

Para los padres:

- ❖ Evitar ausencias de las clases a menos que sea imprescindible, se debe presentar excusa por correo electrónico a Dirección de Nivel antes de la clase. En algunos casos se puede solicitar nota médica.

#### A. Correo electrónico

A los estudiantes y docentes del Colegio Viena Guatemalteco se les provee de una cuenta de correo institucional, en el caso de Primaria baja y Preprimaria ésta queda a cargo de los padres. Las recomendaciones para el uso de estos son:

- Cuando reciba correos electrónicos no solicitados (Correo Spam), o con contenidos sospechosos o que pidan ingresar a un enlace o archivo misterioso, no lo abra, es muy probable que se trate de una infección de malware/virus cibernético hacia el equipo/dispositivo.
- Si recibe solicitudes en donde le piden información privada, desconfíe y verifique por otros medios sobre la veracidad de la información. Los sistemas antimalware/antivirus pueden ayudar a detectar cualquier anomalía en caso de ser infectado.

#### B. Formas de riesgo y síntomas de un riesgo virtual

Existen amenazas como el malware o software malicioso que pueden infectar su computadora o dispositivo. Los equipos se “infectan” a partir de accesos a sitios web maliciosos, correos electrónicos no solicitados con links de acceso o archivos infectados, o por intercambio de archivos infectados por dispositivos USB, entre otros mecanismos. Es fundamental contar con un sistema actualizado de antimalware/antivirus informático.