

CIBERCONSEJOS

para comunidades educativas más seguras



Escuelas y universidades son atractivas para delincuentes

1. Acceso no autorizado a plataformas escolares: Delincuentes pueden robar identidades, realizar declaraciones de impuestos falsas, generar pagos a terceros, alterar el registro de los alumnos y secuestrar sitios web o cuentas de redes sociales, entre otros riesgos.

2. Phishing y ransomware: Con listas de correos de alumnos o funcionarios pueden enviar emails, SMS o WhatsApp haciéndose pasar por el colegio y robar datos personales o convencer a sus víctimas de descargar programas maliciosos, como los que posibilitan el ransomware (cifrado de su PC para exigir un rescate).

Ciberconsejos para profesores e instituciones

1. No exponer información de los alumnos y apoderados en el sitio web, como fotos, horarios y matrículas. Si necesita subir estos datos, resguárdelos con usuario y contraseña, dando acceso solo a quienes lo necesitan.

2. Fomentar la creación de contraseñas fuertes por profesores y alumnos, y la activación de doble factor de autenticación en dispositivos y apps.

csirt.gob.cl/recomendaciones/ciberconsejos-para-crear-contrasenas-seguras/



Ciberconsejos para instituciones educacionales



- **Elaborar** una estrategia de ciberseguridad y planes de defensa y prevención.
- **Crear** un protocolo de respuesta ante incidentes, para que los usuarios sepan qué hacer frente a un ciberataque.
- **Monitorear** regularmente redes y datos para identificar actividades maliciosas
- **Implementar** controles de protección como firewall, sistemas de prevención de intrusos, filtrado de URL, seguridad en emails y filtros de privacidad.

Ciberconsejos para profesores e instituciones

- **Usar** sistemas de protección en capas para el bloqueo de amenazas y niveles de privilegio para los usuarios.
- **Considerar** la ciberseguridad de sistemas como escritorios remotos (RDP) y redes privadas virtuales (VPN).
- **Procurar** plataformas de educación a distancia seguras en cuanto a confidencialidad, integridad y disponibilidad de los datos procesados, almacenados y transmitidos.



Ciberconsejos para instituciones educacionales



- **Los profesores** deben usar computadores de la institución y de usar un equipo personal, se debe verificar que cumpla requisitos de seguridad.
- **Crear** copias de seguridad periódicas, con mínima conectividad con otros sistemas e internet. Realizar regularmente pruebas de recuperación.
- **Capacitar** a toda la comunidad sobre ciberseguridad y reforzar las medidas de precaución.

Ciberconsejos para toda la comunidad



- 1. Ingresar** a las plataformas educacionales desde sitios seguros y evitar wifi públicas.
- 2. Cerrar** la sesión de la plataforma cada vez que se deje de utilizar.
- 3. Usar** software original. Actualizar software regularmente y especialmente cuando se descubren nuevas vulnerabilidades
- 4. Contar** con antivirus y antispam actualizados y de proveedores con buena reputación.