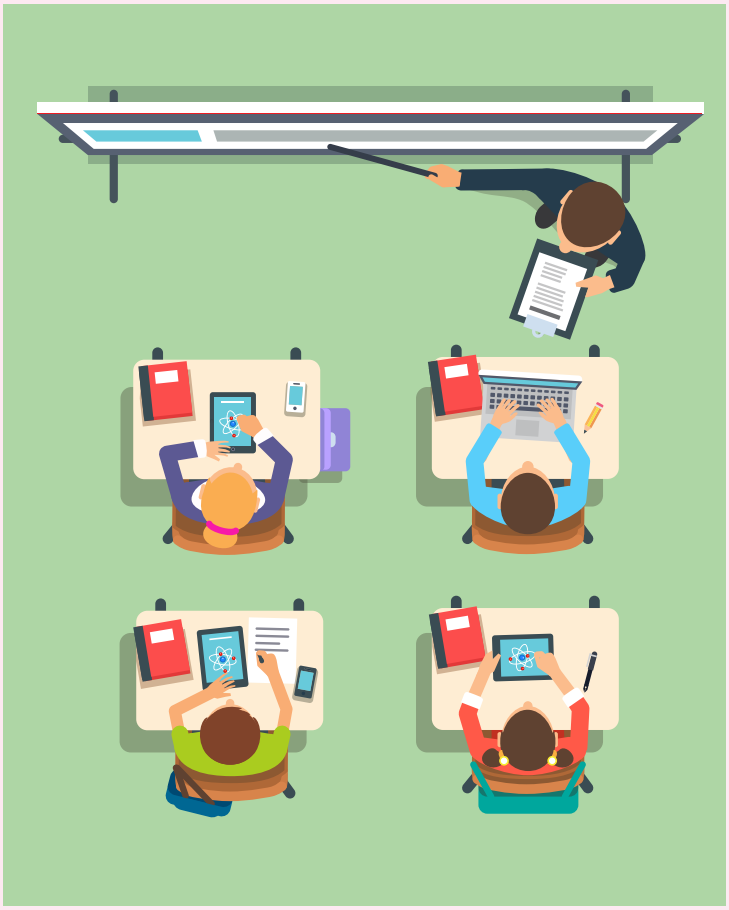
Guía digital de recomendaciones de ciberseguridad para maestros

escuelas ciberseguras®



Cuanto más usamos la tecnología, más necesitamos protegerla. Las escuelas deberían liderar el camino en **ciberseguridad y privacidad**, sin embargo, el sector de la educación es uno de los más atacados por el cibercrimen. En los últimos años, ha habido un incremento en los ataques de ransomware en escuelas y universidades, que han causado daños con un valor de millones de dólares.

Además, los docentes son cada vez más el blanco de ciberdelincuentes y estafas de phishing. Con su acceso a los datos de los estudiantes y las redes escolares son un objetivo fácil para los cibercriminales, siendo el grupo más vulnerable, por ello necesitan ser conscientes de su huella digital y protegerse de las ciberamenazas.

Esta guía analiza la importancia de la ciberseguridad para los docentes en su vida cotidiana y cómo pueden protegerse a sí mismos y a sus alumnos. Recordemos que hoy y siempre es importante cuidar nuestra identidad digital, privacidad y seguridad.

Principales riesgos para los docentes y sus alumnos

INGENIERÍA SOCIAL

PHISHING:
Habitualmente a través de correo electrónico se busca suplantar la identidad de un conocido o de alguna organización, p.e. la SEP, el colegio o un directivo, con el fin de engañar al docente para que proporcione contraseñas, datos sensibles o que haga clic en un enlace malicioso y que de esta forma se infecte su dispositivo con malware.

SMISHING: ataque similar al phishing pero realizado a través de mensajes SMS o de aplicaciones de mensajería y que puede incluir enlaces cortos para engañar a los profesores.

VISHING: Método que busca engañar a la víctima a través de una llamada telefónica, buscando que se introduza un pin por medio del teclado del dispositivo telefónico o persuadir al usuario para compartir información sensible.

MALWARE

Código malicioso diseñado para efectuar acciones dañinas en el dispositivo del usuario sin su autorización, las cuales pueden ir desde el espionaje, el robo de datos y el secuestro de información hasta la manipulación de componentes y funciones del sistema sin que la víctima se percate.

ROBO DE IDENTIDAD

Acción de utilizar de manera indebida los datos personales del docente para cometer un fraude u otro tipo de delito. Habitualmente, el cibercriminal se apropia de la identidad de la víctima y se hace pasar por ella para obtener un beneficio.

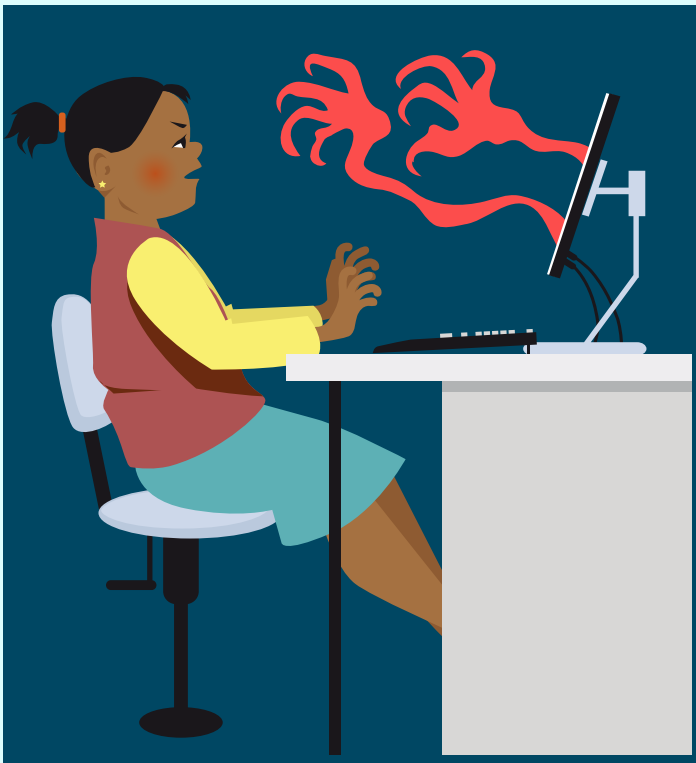
INVASIÓN A LA PRIVACIDAD

Al exponerse una gran cantidad de datos en el ciberespacio sin mantener control sobre lo que se comparte y con quién se comparte, se corre el riesgo de una invasión a la privacidad del docente o de sus alumnos. Esta circunstancia puede generar otro tipo de riesgos.

PÉRDIDA DE CONFIDENCIALIDAD DE LA INFORMACIÓN

Desde un estudiante molesto hasta un cibercriminal puede buscar acceder a información confidencial o privada, lo cual puede concretarse a través del abuso de contraseñas u otros métodos.

Riesgos en menores



Como docente es muy importante platicar con tus alumnos acerca de estos riesgos para prevenir.

¡TODOS ESTAMOS EXPUESTOS!

- **ACCESO A CONTENIDO NO ADECUADO** que atente contra la integridad de los alumnos.

- **CONTACTO CON DEPREDADORES EN LÍNEA Y GROOMING,** el cual se presenta cuando un adulto busca contactar a menores haciéndose pasar uno de ellos para buscar ganar su confianza y después llegar a abusar sexualmente.

- **CIBERACOSO**, al compartir o enviar contenido dañino en cualquier red social que puede afectar la integridad de los niños y adolescentes.

- **CIBERBULLYING** es un tipo de acoso cibernético que se da entre menores, en donde uno o varios, buscan conscientemente lastimar al otro.

- **CIBERVIOLENCIA DE GÉNERO**, se presenta por una persona o grupo de personas hacia otra u otros del sexo opuesto, en el que se ejerce violencia a través de insultos, acoso, control, ataques o chantaje en los medios digitales.

- **SEXTING,** que es la práctica concensuada entre pares de envío de imágenes o video con contenido sexual a través de medios digitales.

- **SEXTORSION,** que es el chantaje a un menor de exponer video o imágenes íntimas en medios sociales si no se recibe un beneficio económico o de otra índole.

Recomendaciones

Es un buen momento para contemplar algunas recomendaciones que nos auxilien cuando abordamos la tecnología en el ciberespacio.

Familiarízate con tus herramientas

•¡Aprende a usarlas!
•Comprende funciones y beneficios
•Configúrala de manera adecuada.
•Configura tu privacidad. Accede a instructivos y materiales oficiales o pide a tu institución que te apoye con ello.

Tus alumnos y los padres de familia también deben de saber usarlas.

Establece reglas

De la misma manera que tienes reglas en el salón de clase debes establecerlas en el aula virtual, buscando que en todo momento se cuide tu privacidad y la de los estudiantes.

Crear contraseñas

Es muy importante que cuando accedas a las aplicaciones tanto personales como educativas utilices contraseñas seguras, robustas y que no las compartas con nadie.

Los educadores siempre deben usar contraseñas seguras con una combinación de números, letras y símbolos. ¡Nunca expongas tus contraseñas frente a tus alumnos!

Utiliza contraseñas diferentes para cada una de tus cuentas y usa un llavero de contraseñas para administrarlas.

Es recomendable además, que utilices la opción de doble factor de autenticación cuando las aplicaciones cuentan con esta funcionalidad. Este control permite agregar una capa adicional de seguridad a tu acceso, ya que además de la contraseña se requerirá de otro dato para acceder a tus plataformas.

Salas virtuales

•Activa la sala de espera hasta que apruebes el ingreso de cada uno de los participantes.
•Pasa lista e identifica a cada uno de los alumnos.
•Expulsa a usuarios ajenos o no deseados a tu clase.
•Cierra el acceso a la reunión cuando ya todos estén dentro de la sala.

Compartir pantalla y archivos

•Deshabilita la función a tus alumnos, solo actívala cuando lo requieras.
•Solo el anfitrión debe poder compartir pantalla o extenderla.
•Desactiva las funciones de compartir archivos y mensajería privada para evitar conversaciones paralelas inapropiadas.
•Asegúrate que la información que se comparta en pantalla no incluya datos personales tuyos o de tus alumnos.

Cuidado con el phishing

•Los educadores nunca deben abrir archivos adjuntos sospechosos ni hacer clic en enlaces de fuentes desconocidas.
•También deben ser conscientes de los riesgos que implica el uso de cuentas de redes sociales con fines profesionales.

Protege tus dispositivos

•Ya sea tu computadora, tableta o dispositivo móvil debes protegerlos con una herramienta ante diferentes tipos de malware.
•Mantén actualizados tus dispositivos.
•También debes cifrar la información de tus dispositivos.
•Bloquea tu sesión cuando no estés frente a tu computadora, ya sea en el aula o en casa si es que continuas en línea.
•Cubre tu cámara web cuando no la requieras.
•Respalda tu información periódicamente.
•Evita el uso de redes Wi-Fi públicas

Uso de sitios públicos educativos

Internet nos proporciona una cantidad de recursos ilimitada para un sinfín de actividades, esto por supuesto también aplica para las instituciones educativas que pueden apoyarse de recursos educativos en línea, sin embargo a continuación proporcionamos algunas recomendaciones para su uso:

1.Siempre notifica a tu institución educativa sobre el o los sitios web que te gustaría utilizar como tu soporte de enseñanza.
2.Revisa las condiciones de uso y el aviso de privacidad, si no protegen los datos personales tuyos o de tus alumnos evita su uso.
3.Notifiquen a los padres de familia de las razones en la selección de las páginas o plataformas a utilizar y las condiciones de seguridad y privacidad que ofrece la misma.
4.Desde el colegio den de alta a los alumnos y capacitenlos en el uso del sitio o plataforma.

Otras referencias de apoyo

Norma de Escuelas Responsables en el Uso de Internet (NMX I 319 NYCE 2018)

Avalada por NYCE y publicada en el Diario Oficial de la Federación promueve que las instituciónes educativas establezcan y conozcan las condiciones de seguridad que deben tener para proveer el acceso y uso del internet

https://escuelasciberseguras.com/adquirir-norma.html

Micrositios del INAI

Brindan información para que las y los profesores de educación básica, principalmente sexto de primaria y secundaria, conozcan con cierta profundidad los conceptos básicos y la normativa mexicana relacionados con el derecho fundamental de protección de datos personales
https://micrositios.inai.org.mx/marcocompetencias/

•Aprendizaje en línea seguro: guía escolar para la protección de datos de los estudiantes en América Latina, donde Capa8 colaboró con el Banco Interamericano de Desarrollo

https://publications.iadb.org/es/aprendizaje-en-linea-seguro-guia-escolar-para-la-proteccion-de-datos-de-los-estudiantes-en-america

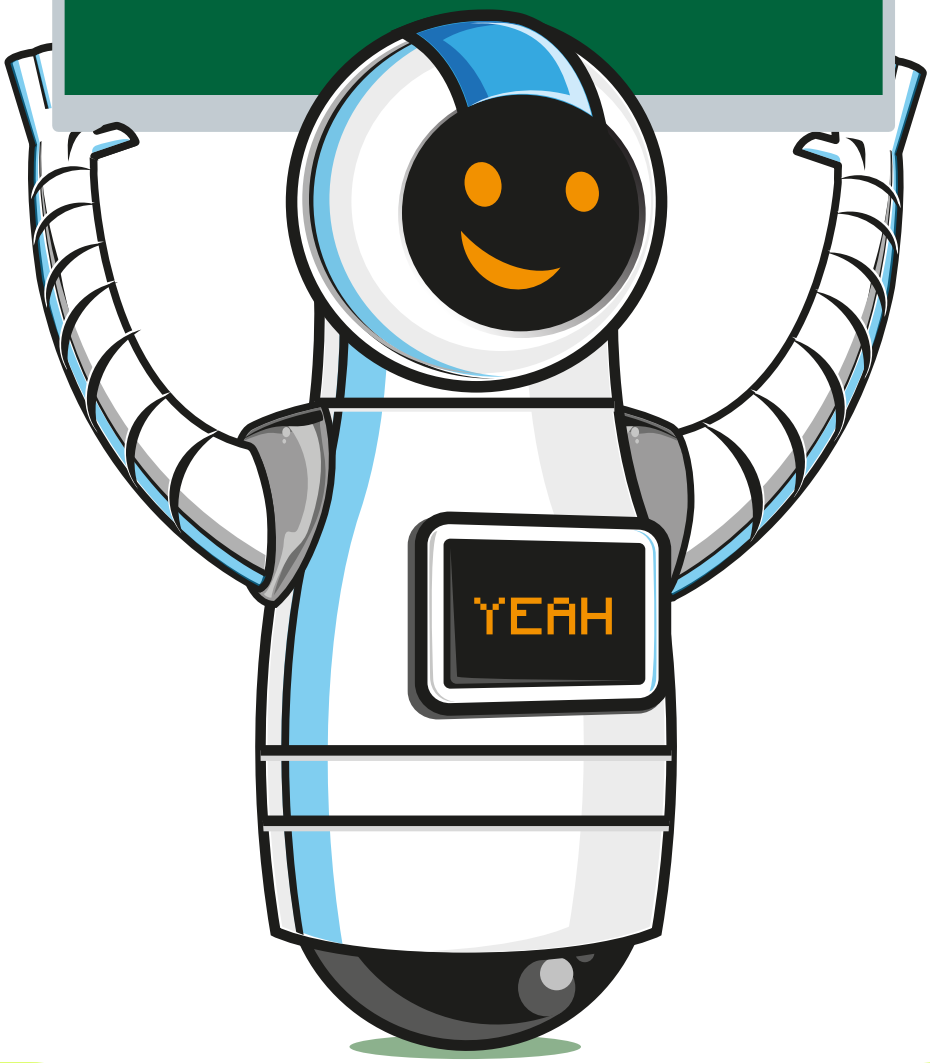
No tengas miedo de aprender algo nuevo ni de utilizar las herramientas digitales, recordemos que NADIE NACE SIENDO UN EXPERTO…. así que PERMÍTANSE SER PRINCIPIANTES.

Nuestro reconocimiento a todos los maestros del mundo por seguir poniendo el corazón, cuidando la educación de sus alumnos, aun a la distancia.

Contáctanos

https://escuelasciberseguras.com/

ciberseguras@capa8.com



capa8®

escuelas ciberseguras®