VAUGHN
NEXT CENTURY LEARNING CENTER

Guía de Concienciación sobre Ciberseguridad

Audiencia	Todos los empleados, el profesorado, el personal y los contratistas
Versión	1.0
Fecha de entrada en vigor	25/08/2026
¿Preguntas?	Contacte con el servicio de asistencia técnica (Help Desk) mediante un ticket de Freshservice.

Bienvenida

Cada día, usted ayuda a proteger a los estudiantes y a las familias a quienes servimos, no solo en el aula, sino también cada vez que inicia sesión, abre un correo electrónico o gestiona el expediente de un estudiante. La ciberseguridad en Vaughn NCLC no es tarea exclusiva del departamento de IT; es responsabilidad de todos.

Esta guía abarca lo que necesita saber y hacer. Es breve a propósito, con el objetivo de que realmente la lea y la recuerde. Si desea conocer los detalles técnicos completos de la política, el departamento de TI dispone del Manual del Programa de Ciberseguridad y puede responder a cualquier pregunta que tenga.

VAUGHN
NEXT CENTURY LEARNING CENTER

Tabla de contenido

Bienvenida..... 2
Tabla de contenido.....3
1. Sus 5 responsabilidades principales..... 4
2. Contraseñas y MFA: simplificados..... 5
3. Identificación de phishing y estafas.....6
4. Protección de la información de estudiantes y empleados.....7
5. Uso seguro de dispositivos y cuentas de Vaughn NCLC..... 8
6. Uso seguro de la tecnología.....9
7. Si algo sale mal: cómo informarlo..... 10
8. Hoja de referencia rápida..... 11
9. Su capacitación anual.....12

1. Sus 5 responsabilidades principales

1. **Proteja su contraseña.** Nunca la comparta, no la anote donde otros puedan verla y utilice la autenticación multifactor (MFA) siempre que esté habilitada en los sistemas que utiliza.
2. **Deténgase y piense antes de hacer clic.** La mayoría de los ciberataques comienzan con un correo electrónico o un mensaje de texto.
3. **Maneje con cuidado la información de los estudiantes y del personal.** Acceda únicamente a la información necesaria para su trabajo y compártala solo con personas autorizadas para verla.
4. **Utilice únicamente tecnología aprobada.** Si desea utilizar una nueva aplicación o herramienta en línea para actividades de Vaughn NCLC, consulte primero al departamento de IT.
5. **Informe de inmediato cualquier situación que le parezca inusual.** Nunca tendrá problemas por reportar un error o un mensaje sospechoso; podría estar evitando un problema mucho mayor.

2. Contraseñas y MFA: simplificados

Construyendo una contraseña segura

- Al menos 12 caracteres, cuanto más tiempo, más fuerte. Piense en una frase corta en lugar de una sola palabra.
- Mézclalo: incluye letras mayúsculas y minúsculas, números y un símbolo.
- No utilices tu nombre, tu nombre de usuario, Vaughn NCLC o la mascota de la escuela, ni un patrón sencillo como "12345" o "aaaa".
- Nunca reutilice su contraseña de Vaughn NCLC para una cuenta personal o una contraseña personal para los sistemas de Vaughn NCLC.

¿Qué es la autenticación multifactor (MFA) y por qué la necesito?

La autenticación multifactor (MFA) consiste en demostrar que realmente eres tú mediante algo más que una simple contraseña; por lo general, se trata de confirmar el acceso rápidamente pulsando un botón en una aplicación de tu teléfono. Es una de las formas más eficaces de detener a un atacante que haya robado o adivinado tu contraseña. Si un sistema te pide que configures la MFA, por favor hazlo cuanto antes.

¿Recibes una solicitud de aprobación de MFA que no has pedido? No pulses «Aprobar». Deniégala e infórmalo al departamento de IT de inmediato. Es probable que alguien tenga tu contraseña.

Cómo mantener segura su contraseña

- Nunca comparta su contraseña con un compañero de trabajo, supervisor, miembro del personal de IT ni con nadie más; el personal de IT legítimo nunca se la solicitará.
- Considere utilizar un gestor de contraseñas aprobado para generar y almacenar contraseñas seguras y únicas.
- Si cree que su contraseña puede haber quedado expuesta, cámbiela de inmediato e informe al departamento de IT.

3. Identificación de phishing y estafas

El *phishing* consiste en un correo electrónico, mensaje de texto o llamada telefónica fraudulentos diseñados para engañarle y lograr que haga clic en un enlace malicioso, abra un archivo adjunto infectado o facilite información, como su contraseña o la autorización para una transferencia bancaria. Es la principal vía por la que se hackean los sistemas de las escuelas.

Señales de alerta comunes

- Lenguaje urgente o amenazante ("su cuenta se cerrará hoy").
- Una solicitud para comprar tarjetas de regalo, transferir dinero o cambiar los datos de depósito directo de la nómina, especialmente si dice provenir de un ejecutivo.
- Un archivo adjunto o enlace inesperado, incluso si parece provenir de alguien conocido.
- Una dirección de remitente casi correcta, pero no del todo (una letra de más, dominio incorrecto).
- Un mensaje que lo presiona para que omita los procedimientos habituales "solo por esta vez".
- Un código QR en un correo electrónico o folleto inesperado que le pide que lo escanee e inicie sesión.

Qué hacer

- Haz una pausa. Las solicitudes legítimas pueden esperar unos minutos para que las verifiques.
- Verifica las solicitudes inusuales, especialmente las relacionadas con dinero o cambios en la nómina, a través de un canal de comunicación independiente y conocido (llama a la persona, no respondas al correo electrónico).
- Pasa el cursor sobre los enlaces antes de hacer clic para ver a dónde te llevan.
- Si tienes dudas, reenvíalo al departamento de IT o usa el botón "Reportar phishing" de tu organización antes de hacer clic en cualquier cosa.

*De vez en cuando, el departamento de IT realiza pruebas simuladas de *phishing* para ayudar a todos a practicar la identificación de estos mensajes. Se trata de ejercicios de aprendizaje, no de trampas para poner a prueba a nadie; el objetivo es crear un hábito que los proteja tanto a ustedes como a sus estudiantes.*

4. Protección de la información de estudiantes y empleados

Vaughn NCLC maneja diariamente información confidencial, como expedientes académicos de los estudiantes, información sobre salud y servicios de apoyo, así como datos del personal y de nómina. Proteger estos datos constituye tanto una responsabilidad profesional como, en el caso de los expedientes estudiantiles, una obligación legal conforme a la normativa FERPA.

Qué hacer y qué no hacer en el día a día

- Sí: acceda únicamente a los registros de estudiantes o empleados que necesite para sus funciones laborales actuales.
- Sí: envíe archivos confidenciales solo a través de los sistemas seguros y aprobados de Vaughn NCLC.
- Sí: bloquee la pantalla (tecla Windows + L) siempre que se aleje de su dispositivo.
- No: envíe datos confidenciales de estudiantes o personal a una cuenta de correo electrónico personal.
- No: deje registros impresos que contengan información de estudiantes o personal a la vista o sin supervisión.
- No: hable sobre información confidencial de estudiantes o personal en áreas públicas o con personas que no necesiten conocerla.
- No: cargue datos de Vaughn NCLC en una cuenta de almacenamiento en la nube personal o en una aplicación no aprobada por el departamento de IT.

5. Uso seguro de dispositivos y cuentas de Vaughn NCLC

- Los dispositivos proporcionados por Vaughn NCLC siguen siendo propiedad de Vaughn NCLC. Utilícelos únicamente para fines escolares autorizados.
- No instale software ni extensiones del navegador que no hayan sido aprobados por el departamento de IT.
- No deshabilite el antivirus, el cortafuegos ni otras herramientas de seguridad instaladas en su dispositivo.
- Mantenga el dispositivo consigo o en un lugar seguro. Informe de inmediato si el dispositivo se pierde o es robado, incluso si no está seguro de que realmente se haya perdido.
- Devuelva el equipo de Vaughn NCLC sin demora cuando se le solicite o cuando deje de formar parte de Vaughn NCLC.
- Utilice únicamente tecnología y herramientas en la nube aprobadas por el departamento de IT para actividades escolares. Las nuevas aplicaciones y herramientas "gratuitas" pueden conllevar riesgos reales de seguridad y privacidad, aunque parezcan inofensivas.

6. Uso seguro de la tecnología

- Conéctese a los sistemas de Vaughn NCLC únicamente a través del método seguro aprobado (VPN u otro acceso autorizado por el departamento de IT), y no mediante redes Wi-Fi abiertas, desconocidas o sin protección.
- Mantenga protegida su red Wi-Fi doméstica con contraseña y asegúrese de que el software de su enrutador esté actualizado.
- Evite trabajar con información confidencial a través de redes Wi-Fi públicas (como las de cafeterías o aeropuertos) si no cuenta con protección VPN.
- Asegúrese de que nadie más pueda ver su pantalla cuando trabaje en espacios públicos o compartidos.
- Utilice únicamente dispositivos que cumplan con los requisitos de seguridad de Vaughn NCLC para acceder de forma remota a sistemas que manejan información confidencial.

7. Si algo sale mal: cómo informarlo

Si ves algo sospechoso, haces clic donde no debías, pierdes un dispositivo o crees que tu cuenta podría estar comprometida, avisa al departamento de IT de inmediato. Informar rápidamente es el factor más importante para limitar los daños.

Informe inmediatamente si nota:

- Un correo electrónico, mensaje de texto o llamada telefónica sospechosos
- Un dispositivo perdido, robado o posiblemente comprometido
- Una solicitud de autenticación multifactor (MFA) que no has solicitado
- Comportamiento inusual del equipo (ventanas emergentes, lentitud, archivos que no se pueden abrir, mensajes de rescate)
- Envío accidental de información confidencial a la persona equivocada
- Cualquier otra cosa que simplemente parezca sospechosa o incorrecta

Cómo informar

Contacta con el servicio de asistencia técnica (Help Desk) tan pronto como notes el problema. Incluye qué sucedió, cuándo ocurrió y qué acciones has realizado ya (por ejemplo, si hiciste clic en un enlace).

No será disciplinado por informar un error de buena fe. No informar y dejar que un pequeño problema se convierta en uno más grande es el resultado que estamos tratando de evitar. En caso de duda, repórtelo.

8. Hoja de referencia rápida

Situación	Qué hacer
Recibiste un correo electrónico sospechoso.	No hagas clic. Notifícalo a IT.
Hiciste clic en un enlace no válido o abriste un archivo adjunto no válido.	Desconéctate de la red Wi-Fi si es posible e informa a TI de inmediato. No esperes.
Has recibido una solicitud de MFA que no pediste.	Niégalo. Cambia tu contraseña. Informa a IT.
Perdió un dispositivo Vaughn NCLC.	Notifícalo a IT de inmediato, aunque creas que lo vas a encontrar.
Necesita compartir datos de estudiantes o del personal.	Utilice únicamente los sistemas aprobados de Vaughn NCLC; nunca utilice correo electrónico personal ni almacenamiento en la nube personal.
Quieres usar una nueva aplicación o un nuevo sitio web para el trabajo.	Consulta al departamento de IT antes de empezar a usarlo.
Estás trabajando desde casa o desde un lugar público.	Utilice el método de conexión segura aprobado; mantenga su pantalla privada.
Has olvidado tu contraseña.	Utilice el procedimiento oficial de restablecimiento. Nunca le pida el suyo a un compañero de trabajo.

9. Su capacitación anual

Todos los empleados completan una capacitación de concienciación sobre ciberseguridad al incorporarse a Vaughn NCLC y, posteriormente, al menos una vez al año. Algunos puestos (IT, Recursos Humanos./Finanzas, líderes escolares y personal con acceso a datos confidenciales de los estudiantes) reciben capacitación adicional específica para su función. Asimismo, es posible que reciba ocasionalmente recordatorios breves, ejercicios de simulación de *phishing* o repasos rápidos a lo largo del año; estas actividades forman parte de los esfuerzos para mantener a toda la comunidad de Vaughn NCLC alerta y preparada.

Gracias por dedicar tiempo a leer esta guía y por ayudar a proteger a los estudiantes, las familias y los compañeros de Vaughn NCLC. Si alguna vez tiene alguna pregunta, ya sea sobre un correo electrónico sospechoso, una nueva herramienta que desee utilizar o cualquier otro asunto, el servicio de asistencia técnica (IT Help Desk) es siempre el lugar adecuado al que dirigirse.