sphero

BOLT™

# LABORATORIOS DE CIBERSEGURIDAD

## GUÍA DEL EDUCADOR

# CONTENIDO

# INTRODUCCIÓN

Nuestra sociedad cada vez más digital pone el mundo a nuestro alcance, lo que nos permite aprender prácticamente cualquier cosa, comunicarnos y colaborar con personas en el otro lado del mundo e innovar soluciones para nuestros mayores desafíos. Desafortunadamente, el mundo digital nos abre a un conjunto de amenazas completamente nuevo y aterrador. La demanda nunca ha sido mayor de una fuerza laboral robusta de seguridad cibernética y ciudadanos con una sólida comprensión de la ética informática y cómo proteger sus vidas digitales.

Los laboratorios de ciberseguridad Sphero BOLT tienen como objetivo abordar este desafío dando vida a los conceptos de ciberseguridad a través de experiencias prácticas de aprendizaje. BOLT simula y modela conceptos que a menudo se ocultan en lo profundo de las computadoras, las redes y el código para que los estudiantes de secundaria puedan visualizarlos, discutirlos y comprenderlos por completo.

Los laboratorios fueron desarrollados en colaboración con **Dra. Paulina Mosley** , Profesor Titular y Presidente Asociado de Tecnología de la Información en Pace University. La experiencia en la materia del Dr. Mosley garantiza que el aprendizaje en los laboratorios sea preciso y actual. Al mismo tiempo, como director de **Criptobot del campamento** , su entusiasmo por involucrar a más estudiantes de secundaria y preparatoria en las carreras de seguridad cibernética garantiza que los laboratorios sean relevantes, de gran interés y, lo más importante, ¡divertidos!

## Objetivos

***Al final de la unidad, los estudiantes serán capaces de:***

- explicar cómo las computadoras usan redes privadas y públicas para transmitir información
- diferenciar entre usos éticos y no éticos de la tecnología
- evaluar los riesgos y beneficios de las diferentes prácticas informáticas
- identificar diferentes tipos de piratas informáticos y explicar sus motivos
- identifique y explique los ataques cibernéticos comunes, incluidos el phishing, el malware, los ataques distribuidos de denegación de servicio y más
- explicar las técnicas que utilizan los profesionales de ciberseguridad para proteger los dispositivos conectados a Internet y los usuarios de computadoras
- compartir estrategias para mantenerse a sí mismos y a sus dispositivos a salvo de ciberataques comunes
- describir posibles trayectorias profesionales en el campo de la ciberseguridad

# LA MISIÓN SPHERO

Sphero está transformando la educación de PK-12 con herramientas accesibles que fomentan la exploración, la imaginación y la perseverancia a través de STEAM y la informática. Con la ayuda de educadores de todo el mundo, estamos capacitando a los estudiantes de todos los orígenes y habilidades para que descubran sus intereses y pasiones mientras los equipamos con las habilidades que necesitan para ser los futuros Changemakers del mundo.

# QUERIDOS EDUCADORES,

## ¡BIENVENIDOS A LOS LABORATORIOS DE CIBERSEGURIDAD!

La ciberseguridad se está convirtiendo rápidamente en una prioridad a medida que las mentes jóvenes aprenden STEM y se preparan para unirse a la fuerza laboral en esta era de la información y la rápida globalización. Según los datos recopilados por la Oficina de Estadísticas Laborales de EE. UU. (BLS), la demanda de trabajos de ciberseguridad, como los analistas de seguridad de la información, crecerá hasta un 33 % en los próximos diez años. Sin embargo, según los datos del Centro Nacional para la Mujer y la Tecnología de la Información (NCWIT, 2010), solo alrededor del 3 % del grupo disponible de graduados de escuelas secundarias pertenecientes a minorías obtendrán títulos en informática de colegios y universidades estadounidenses, por lo que carecen de las calificaciones para ocupar estos puestos de trabajo.

Sphero BOLT Cybersecurity Labs es un conjunto de experiencias prácticas guiadas alineadas con los estándares que introducen a los estudiantes a los principios, la ética y las técnicas de ciberseguridad. Los laboratorios, que utilizan múltiples puntos de entrada y conexiones a temas relevantes en la vida cotidiana de los estudiantes, ayudarán a crear una base sólida de seguridad cibernética para los estudiantes que se puede usar para mejorar su higiene digital e iniciarlos en el camino hacia una carrera de seguridad cibernética. Una de las principales fortalezas de este plan de estudios es la diferenciación de actividades para diversos conjuntos de habilidades, mujeres jóvenes y minorías. Los laboratorios se pueden modificar fácilmente para estos estudiantes con diversos conjuntos de habilidades para que la entrega del contenido sea inclusiva y atractiva mientras se cultiva la autoeficacia, un factor crítico en el éxito de los estudiantes.

Es nuestro deseo que los estudiantes que interactúen con estos laboratorios se sientan empoderados con conocimientos, conjuntos de habilidades tecnológicas y una mentalidad de que no hay nada que no puedas hacer si te lo propones. Diviértete, haz preguntas, comete errores, haz amigos y, lo más importante, ¡te exigimos que te diviertas!

Atentamente,
Dra. Paulina Mosley
Universidad de ritmo
Profesor Titular y Cátedra Asociada de Tecnologías de la Información
Director del Campamento CryptoBot

# CARACTERÍSTICAS DEL LABORATORIO

## Diseñado para estudiantes de secundaria

Los laboratorios están diseñados específicamente para introducir a los estudiantes de secundaria en el campo de la seguridad cibernética con dos objetivos principales. En primer lugar, los laboratorios enseñan y refuerzan los principios de la higiene digital y el uso ético de la informática para que los estudiantes sepan cómo protegerse a sí mismos y a su comunidad. En segundo lugar, los laboratorios muestran cómo los piratas informáticos ilegales suelen atacar redes y dispositivos, así como los pasos que toman los profesionales de la seguridad cibernética para detener los ataques de modo que los estudiantes creen una base para profundizar en la educación y las carreras de seguridad cibernética.

## Enfocado en Ciberseguridad

El enfoque de los laboratorios está en la seguridad cibernética, no en la enseñanza de habilidades de programación informática. Los programas creados previamente proporcionados permiten a los estudiantes interactuar con los conceptos de seguridad cibernética listos para usar sin ninguna experiencia previa en programación. Sin embargo, los estudiantes sacarán más provecho de los laboratorios si tienen alguna experiencia previa con la codificación de bloques y con los robots BOLT. Recomendamos encarecidamente completar las actividades de Introducción a los bloques en la aplicación Sphero Edu antes de completar los laboratorios de ciberseguridad.

## Fácil de diferenciar y ampliar

Utilice las ideas y los recursos de las notas del educador para ayudar a adaptar los laboratorios a las experiencias y necesidades de sus alumnos. Encontrará enlaces a ideas didácticas, recursos y videos, así como ideas para llevar el aprendizaje de los estudiantes más allá.

## Vinculado a trayectorias profesionales

Los laboratorios destacan cómo trabajan los profesionales de la seguridad cibernética para mantenernos a nosotros y nuestros dispositivos informáticos a salvo de las amenazas cibernéticas y ampliar los horizontes de los estudiantes para considerar futuras carreras de seguridad cibernética. En el laboratorio final, los estudiantes exploran diferentes opciones profesionales e investigan y presentan sus hallazgos a sus compañeros.

## Alineado a los Estándares de Ciberseguridad

Los laboratorios están alineados con el Estándares de aprendizaje de seguridad cibernética K-12 —desarrollado en 2021 por Cyber.org y educadores en los Estados Unidos, para "aumentar la alfabetización en seguridad cibernética de los estudiantes y construir una fuente sólida de futuros talentos en seguridad cibernética". Los estándares están organizados en tres temas centrales: Sistemas informáticos (CS), Ciudadanía digital (DC) y Seguridad (SEC).

## Tema: Sistemas de Computación (CS)

- **6-8.CS.AP** Discuta el papel que juega el software en la protección de un sistema seguro.
- **6-8.CS.CC** Identificar las ventajas y desventajas de varios modelos de computación en la nube.
- **6-8.CS.COMM.1** Comparar y contrastar topologías de red.
- **6-8.CS.COMM.2** Diferenciar entre las direcciones MAC e IP de un dispositivo de red.
- **6-8.CS.COMP** Identificar el papel de los componentes de red conectados.
- **6-8.CS.DURO** Desarrollar estrategias para crear conciencia sobre las vulnerabilidades del hardware.
- **6-8.CS.IOT** Evalúe los riesgos y beneficios de los dispositivos de Internet de las cosas.
- **6-8.CS.PÉRDIDA** Explicar la función y la importancia de las copias de seguridad.
- **6-8.CS.OS** Discuta los riesgos de los sistemas operativos obsoletos.
- **6-8.CS.PROG** Explicar el papel de las secuencias de comandos en los ataques cibernéticos.
- **6-8.CS.PROT** Identificar los tipos de conexión de protocolo utilizados para diferentes servicios disponibles en línea.
- **6-8.CS.SUAVE** Identificar ejemplos de vulnerabilidades que existen en el software.

## Tema: Ciudadanía Digital (DC)

- **6-8.DC.AUP** Comprender los diversos acuerdos y cómo protegen a los usuarios y propietarios de la tecnología.
- **6-8.DC.CYBL** Desarrollar estrategias para crear conciencia sobre los efectos y los métodos para identificar y prevenir el ciberacoso.
- **6-8.DC.ETH** Distinguir entre hacking ético y malicioso.
- **6-8.DC.PIE1** Reconocer las muchas fuentes de datos que componen una huella digital.
- **6-8.DC.PIE2** Reconocer la permanencia de una huella digital.
- **6-8.DC.IP** Explique cómo la propiedad intelectual y los derechos de autor se relacionan con el uso justo.
- **6-8.DC.LEY** Analice las leyes federales, estatales y locales específicas en relación con la ciberseguridad y la privacidad.
- **6-8.DC.PP.1** Discuta los riesgos y beneficios de compartir PII.
- **6-8.DC.PP.2** Examinar técnicas para detectar, corregir y prevenir la divulgación de PII.
- **6-8.DC.THRT** Describir varios tipos de actores de amenazas.

## Tema: Seguridad (SEC)

- **6-8.SEG.ACC** Explicar el concepto de control de acceso y cómo limitar el acceso a usuarios autorizados.
- **6-8.SEG.AUT.** Explique cómo los métodos de autenticación y autorización pueden proteger a los usuarios autorizados.
- **6-8.SEC.CIA** Explicar los efectos de una falla de la Tríada de la CIA.
- **6-8.SEC.COMP** Describir estrategias de defensa en profundidad para proteger redes simples.
- **6-8.SEG.LLORAR** Analice los métodos y la necesidad de cifrar la información cuando se intercambia, por ejemplo, http frente a https.
- **6-8.SEC.CTRL** Describir Defensa en profundidad y cómo funcionan juntos los controles de acceso físico.
- **6-8.SEG.DATOS** Describa los datos en sus tres estados y las amenazas potenciales para cada estado.
- **6-8.SEG.INFO** Analizar amenazas y vulnerabilidades a la seguridad de la información para individuos y organizaciones.
- **6-8.SEC.NET** Explicar cómo las acciones maliciosas amenazan la seguridad de la red.
- **6-8.SEC.PHYS** Explicar cómo las acciones maliciosas amenazan la seguridad física.

# ESTRUCTURA DE LABORATORIO

**Cada laboratorio utiliza la siguiente estructura para involucrar a los estudiantes y desarrollar una comprensión más profunda de los conceptos de ciberseguridad:**

## Activar

En **Activar pasos** , los laboratorios hacen conexiones con el conocimiento previo que los estudiantes ya pueden tener sobre el tema y atraen el interés de los estudiantes.

## Aprender

En **Aprender pasos** , los laboratorios proporcionan vocabulario y conceptos básicos de aprendizaje para permitir a los estudiantes aumentar su comprensión de la seguridad cibernética. Utilice las ideas y la información de las notas del educador para llevar más lejos este aprendizaje.

## Investigar

En **Investigar pasos** , los estudiantes abren y ejecutan un programa BOLT para comenzar a explorar los temas de manera práctica.

## Cortar a tajos

En **Hackear pasos** , los estudiantes modifican el programa para extender el modelo a través de escenarios y juegos adicionales.

## Asegure su comprensión

En **Asegure sus pasos de comprensión** , los estudiantes conectan el modelo BOLT con la informática en su vida cotidiana y discuten sus aprendizajes sobre ciberseguridad con sus compañeros de clase.

# CONSEJOS DE FACILITACIÓN

## Antes de enseñar:

- Lea las instrucciones de los estudiantes para la actividad, pruebe la programación y anticipe los obstáculos que pueden encontrar sus estudiantes.
- Lea las notas del educador en los Pasos de laboratorio y considere los puntos en los que pausará a los estudiantes para la instrucción y el debate de toda la clase.
- Prepare el espacio de su salón de clases para las necesidades del laboratorio de acuerdo con las instrucciones de los estudiantes y las notas del educador.
- Determine si el laboratorio usa comunicaciones IR entre dos o más grupos y, si es necesario, planee grupos de estudiantes más grandes con dos o más BOLTS y dispositivos de programación.
- Asegúrese de que todos los robots y dispositivos de programación estén completamente cargados.
- Plan para dos estudiantes por robot BOLT.

## Durante la Enseñanza:

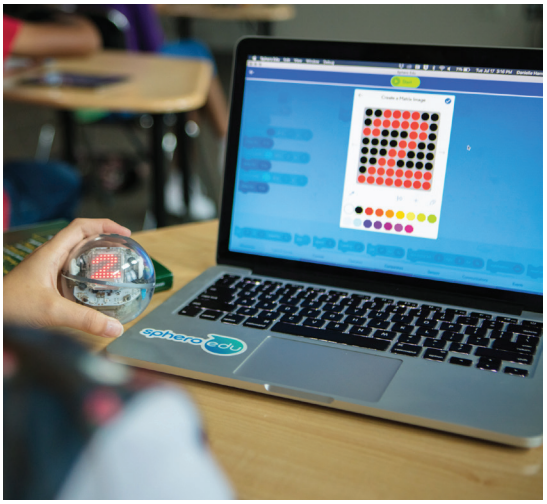
- Haga circular el espacio de su salón de clases para solucionar problemas con los estudiantes. Si varios grupos están luchando con el mismo problema, resuélvalo con toda la clase.
- Use las notas del educador para posibles soluciones de los estudiantes, así como ideas sobre cómo ampliar los desafíos y el aprendizaje.
- Considere el tiempo. Si es posible, reserve de 5 a 10 minutos al final de su período de instrucción para el paso Asegure su comprensión.

## Después de enseñar:

- Reflexionar sobre el aprendizaje de los alumnos. ¿Qué fue fácil para los estudiantes? ¿Qué fue difícil? ¿Hubo algún artefacto del aprendizaje de los estudiantes que pueda compartir con toda la clase para abordar un desafío común o mostrar un concepto de programación o una estrategia de resolución de problemas?
- Explore cómo puede usar ideas y recursos en el laboratorio y/o las notas del educador para profundizar el aprendizaje de los estudiantes.
- Considere cómo podría convertir el tema en un proyecto independiente o grupal. Por ejemplo, los estudiantes podrían investigar otro ejemplo de un esquema de phishing y presentar su aprendizaje a sus compañeros.

# AGRUPACIONES DE LABORATORIO

Los laboratorios de ciberseguridad se dividen en **cuatro niveles** —rojo, amarillo, azul y verde—cada uno con **cinco laboratorios** . Los laboratorios se presentan en forma suelta. **orden secuencial** , comenzando con los conceptos de ciberseguridad más introductorios y terminando con algunos de los más avanzados. Puede comenzar en Rojo 1 y enseñar todo el camino hasta Verde 5. Sin embargo, cada laboratorio también está destinado a **ser único** . Puede **escoge y elige** temas que son más relevantes para las necesidades de sus estudiantes y su plan de estudios. Preste mucha atención a la **requisitos previos de codificación** , si los hubiere, enumerados en la descripción del laboratorio al momento de la planificación.



# NIVEL ROJO
## ÉTICA Y REDES

Los estudiantes comienzan su viaje de seguridad cibernética aprendiendo sobre prácticas informáticas éticas versus no éticas y consideran un código de ética informática. Luego, los estudiantes aprenden los conceptos básicos de cómo las computadoras se comunican a través de Internet y en redes privadas. Los laboratorios de huella digital rastrean los caminos de los estudiantes a través de Internet e introducen formas en que otros rastrean (y utilizan) sus acciones digitales.

***Haga clic en cada título o nombre de actividad para ver la actividad en la aplicación Sphero Edu***

## ROJO 1 *La ética de la computación: correcto versus incorrecto*


Un sólido código de ética forma el corazón de la ciberseguridad, que influye en las decisiones que tomamos cuando usamos nuestros dispositivos informáticos, así como en la forma en que nos protegemos a nosotros mismos y a los demás de las ciberamenazas.

***Al final de este laboratorio, los estudiantes podrán:***

- explicar un Código Ético para profesionales informáticos.
- diferenciar entre una decisión ética y una no ética.

## ROJO 2 *Cómo funciona Internet: el panorama general*


La mayoría de nosotros usamos Internet a diario para el trabajo, la escuela y la vida. Pero, ¿qué es exactamente Internet y cómo funciona?

***Al final de este laboratorio, los estudiantes podrán:***

- describir los protocolos IP y TCP.
- use robots BOLT para explicar cómo funciona Internet.
- comparar y contrastar sitios web que usan HTTP y HTTPs.

## ROJO 3 *Redes privadas: mantenerlo privado*


Internet es un gran espacio público, pero lo más probable es que pase la mayor parte de su tiempo accediendo a Internet desde una red privada llamada red de área local (LAN), ya sea que esté en casa, en la biblioteca o en la escuela.

***Al final de este laboratorio, los estudiantes podrán:***

- definir y diagramar una red de área local (LAN).
- describir la función de un módem y un enrutador.
- explicar cómo los cortafuegos protegen los dispositivos en una LAN de la Internet pública.

## ROJO 4 *Huellas digitales: nuestras huellas en Internet*


Al igual que una huella en el suelo, las huellas digitales se pueden usar para rastrear sus decisiones y movimientos en línea. Es importante que empieces a pensar en esto tan pronto como empieces a usar Internet.

***Al final de este laboratorio, los estudiantes podrán:***

- Identifica qué es una huella digital.
- Cree un modelo de una huella digital como clase.
- Mire qué hay actualmente en su huella digital.

## ROJO 5 *Gestión de su huella digital*


Comprender cómo se crea su huella digital y para qué se utiliza es fundamental para protegerse a sí mismo y a su información. Si bien muchas partes de su huella digital pueden ser inofensivas, e incluso útiles, sin la atención adecuada, pueden convertirse rápidamente en una gran cantidad de información a la que no desea que nadie tenga acceso.

***Al final de este laboratorio, los estudiantes podrán:***

- Identificar qué tipos de información podrían incluirse en una huella digital.
- Decida qué piezas de información querrían y no querrían en su huella digital.
- aprender técnicas sobre cómo controlar su huella digital.

# NIVEL AMARILLO
## CIBERACOSADORES Y HACKERS

Los estudiantes revisan el concepto de computación ética con un enfoque en el ciberacoso. Luego aprenden sobre los diferentes tipos de piratas informáticos; Además de los piratas informáticos no éticos/ilegales, también hay piratas informáticos éticos/legales que pasan sus días contrarrestando a los malos actores. Los estudiantes exploran algunas formas en que los malos actores utilizan el phishing y la ingeniería social para plantar virus y gusanos, dos tipos de malware que pueden causar daño.

***Haga clic en cada título o nombre de actividad para ver la actividad en la aplicación Sphero Edu***

## AMARILLO 1 *Ciberacoso: no seas un acosador*


El ciberacoso puede tener efectos increíblemente negativos no solo en la víctima, sino también en la persona que participa en el ciberacoso y en comunidades enteras en línea.

***Al final de este laboratorio, los estudiantes podrán:***

- Explique la definición de ciberacoso.
- discutir los efectos que tiene el ciberacoso en la salud mental.
- Explore diferentes formas en que puede prevenir el ciberacoso.

## AMARILLO 2 *Tipos de Hackers: Hackear o No Hackear*


Lo bueno, lo malo y todo lo demás. El mundo de la ciberseguridad está lleno de todo tipo de piratas informáticos con una amplia variedad de motivaciones.

***Al final de este laboratorio, los estudiantes podrán:***

- Explique la definición de piratería.
- discutir las consecuencias legales y éticas de la piratería.

## AMARILLO 3 *Phishing: cómo lo encuentran los piratas informáticos ilegales*


El phishing y la ingeniería social son técnicas comunes que los piratas informáticos sin ética utilizan para convencer a las personas desprevenidas de que brinden su información libremente y luego la usan para obtener acceso a sus contraseñas, cuentas bancarias, información de tarjetas de crédito y más.

***Al final de este laboratorio, los estudiantes podrán:***

- Explique la definición de phishing.
- analice los peligros del phishing, los engaños y la ingeniería social.
- discuta las diferentes formas en que puede protegerse de ser víctima del phishing.

## AMARILLO 4 *Virus: modelado de la propagación de una infección informática*


El malware o software malicioso diseñado para dañar e interrumpir nuestra tecnología es, lamentablemente, un hecho de la vida moderna. Sin embargo, aprender qué es y cómo funciona puede ayudarnos a todos a mantener nuestras computadoras y a nosotros mismos más seguros.

***Al final de este laboratorio, los estudiantes podrán:***

- describir los tres tipos principales de malware.
- modele cómo se propaga el malware como un virus con BOLT.
- describir los pasos que toman las personas y los profesionales de la ciberseguridad para combatir el malware.

## AMARILLO 5 *El gusano Morris: malware histórico*


Al igual que un gusano físico, los gusanos informáticos pueden retorcerse, propagarse y crecer a través de una red, infectando las computadoras a medida que avanzan. Si bien a veces son inofensivos, muchos gusanos son malware malicioso que puede dañar las computadoras y crear posibilidades de ataques.

***Al final de este laboratorio, los estudiantes podrán:***

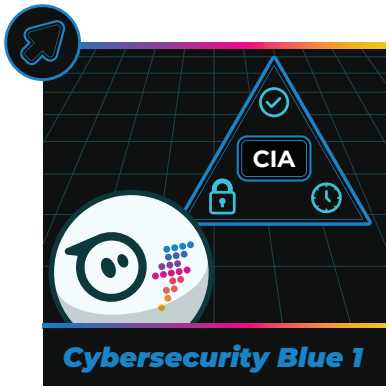
- comparar y contrastar gusanos y virus.
- modele el gusano Morris con un programa BOLT.
- describir los tipos de daños que pueden causar los gusanos.

# NIVEL AZUL
## TRÍADA DE LA CIA Y ATAQUES

Los estudiantes aprenden sobre el modelo CIA Triad, utilizado por los profesionales de ciberseguridad para planificar la seguridad de la información. Luego aprenden sobre otras amenazas de malos actores, incluidos los ataques DDoS, la detección y el escaneo, y los ataques de persona en el medio. Entrelazados en cada uno están las estrategias utilizadas por los piratas informáticos legales para contrarrestar la amenaza y garantizar la disponibilidad, integridad y confidencialidad de la información.

***Haga clic en cada título o nombre de actividad para ver la actividad en la aplicación Sphero Edu***

## AZUL 1 *Tríada de la CIA: planificación de la seguridad*

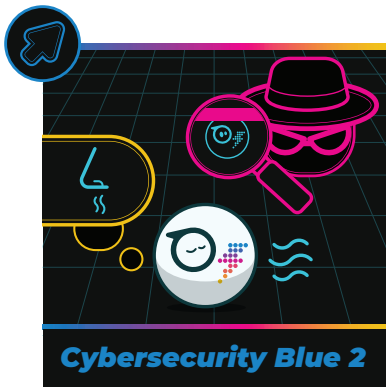



Al planificar la seguridad de la información y la red, los profesionales de ciberseguridad mantienen la tríada de la CIA (confidencialidad, integridad y disponibilidad) en el centro de su toma de decisiones.

***Al final de este laboratorio, los estudiantes podrán:***

- explicar el significado de Confidencialidad, Integridad y Disponibilidad en la Tríada de la CIA.
- describir el papel de cada principio en la tríada de la CIA en la protección de la información y los datos.

## AZUL 2 *Hacker Snooping: olfatear y escanear*




Antes de que un hacker pueda atacarte, debe conocer tus vulnerabilidades. Los delincuentes de ciberseguridad utilizan dos técnicas de reconocimiento para conocer sus vulnerabilidades: olfatear y escanear.

***Al final de este laboratorio, los estudiantes podrán:***

- Describe la diferencia entre olfatear y escanear.
- explicar cómo los atacantes arman la información que recopilan sobre los sistemas informáticos.
- use mensajes IR para hacerse cargo del BOLT de un equipo contrario.

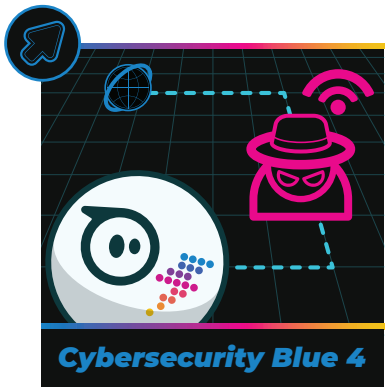
## AZUL 3 *Denegado: ataques de denegación de servicio*


Los ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS) son algunos de los ataques cibernéticos más comunes y perjudiciales. Los ciberdelincuentes relativamente inexpertos pueden acabar con grandes sitios web, haciendo que la información y los servicios no estén disponibles.

***Al final de este laboratorio, los estudiantes podrán:***

- describir los ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS).
- programe dos BOLT para representar al atacante y la víctima en un ataque DoS.
- modifique el programa para reducir la susceptibilidad de su BOLT a un ataque DDoS.

## AZUL 4 *Ataques de persona en el medio: ¿Quién está ahí?*




Un ataque de persona en el medio suena exactamente como lo que es: un pirata informático ilegal que intercepta las comunicaciones entre usted y los servicios de Internet que usa mientras está en una computadora.

***Al final de este laboratorio, los estudiantes podrán:***

- describir un ataque de persona en el medio.
- modele un ataque de persona en el medio con los robots BOLT.
- explicar cómo mantenerse seguros mientras usan computadoras conectadas a Internet.

## AZUL 5 *Círculos de influencia: Autenticar y autorizar*


Para distinguir entre diferentes tipos de usuarios, se pueden utilizar diferentes tipos de autorización de usuario. Cuando esta autorización se ve comprometida, puede tener consecuencias caóticas.

***Al final de este laboratorio, los estudiantes podrán:***

- definir la autenticación y su importancia en la ciberseguridad.
- analice los cuatro medios generales para autenticar la identidad de un usuario (contraseña, biométrico, electrónico, tarjetas inteligentes).
- modele los niveles de autorización con BOLT.
- describir algunos de los problemas de seguridad clave para la autenticación de usuarios.

# NIVEL VERDE
## LA CRIPTOGRAFÍA Y TU FUTURO

En el último nivel, los estudiantes profundizan en el mundo de los profesionales de la ciberseguridad y examinan cómo las contraseñas y el cifrado de la información pueden mantener segura nuestra información digital y nuestras vidas. En el laboratorio final, después de desarrollar una comprensión inicial de muchos temas de seguridad cibernética, los estudiantes obtienen una vista previa de las oportunidades laborales en el mundo de la seguridad cibernética.

***Haga clic en cada título o nombre de actividad para ver la actividad en la aplicación Sphero Edu***

## VERDE 1 *p@$$W0RD$!: ¿Qué hay detrás de una contraseña segura?*


¿Qué es más poderoso: un humano o una máquina? Bueno, cuando se trata de descifrar contraseñas, las computadoras son mucho más rápidas que nosotros.

***Al final de este laboratorio, los estudiantes podrán:***

- usa BOLT para abrir una cerradura de combinación.
- Describa dos métodos que usan los piratas informáticos ilegales para descifrar contraseñas.
- explicar cómo formar contraseñas seguras y fáciles de recordar.

## VERDE 2 *Introducción a la criptografía: cifrado Pigpen*


¿Alguna vez has pasado notas en un código secreto? Bueno, las computadoras se comunican todo el tiempo en mensajes encriptados.

***Al final de este laboratorio, los estudiantes podrán:***

- usa BOLT y el cifrado de la pocilga para enviar mensajes secretos a tus compañeros de clase.
- explicar cómo el texto sin formato se cifra en texto cifrado y luego se descifra de nuevo en texto sin formato.
- cifrar y descifrar mensajes con BOLT y el cifrado pigpen.

## VERDE 3 *El turno de César: ¿César dice qué?*


En palabras del antiguo líder romano, Julio César, “RljvnRbjfRlxwzdnanm”. ¡¿¡¿Esperar lo?!?! Resulta que César a menudo encriptaba sus comunicaciones y uno de los cifrados más conocidos, el Cambio de César, lleva su nombre.

***Al final de este laboratorio, los estudiantes podrán:***

- cifrar y descifrar mensajes con Caesar Shift.
- manipular un programa BOLT de JavaScript para explorar la criptografía.
- identificar las características de los cifrados fuertes.

## VERDE 4 *¡Multiplícalo! Módulo aritmético y cifrados*


Aprende sobre el cifrado de multiplicación, un cifrado monoalfabético. En el proceso, se familiarizará con la aritmética modular y comenzará a comprender su importancia para la criptografía moderna.

***Al final de este laboratorio, los estudiantes podrán:***

- cifrar y descifrar mensajes con un cifrado de multiplicación.
- use la operación de módulo para calcular el resto.

## VERDE 5 *Desfile de la carrera de ciberseguridad*


Respondedores de incidentes, criptógrafos, probadores de penetración; Uno de estos podría ser el título de su trabajo en el futuro.

***Al final de este laboratorio, los estudiantes podrán:***

- identificar diferentes carreras de ciberseguridad.
- comprender dónde y qué carreras tienen una gran demanda.
- explicar los detalles de una carrera de ciberseguridad de su elección.

# CONSEJOS DE TECNOLOGÍA

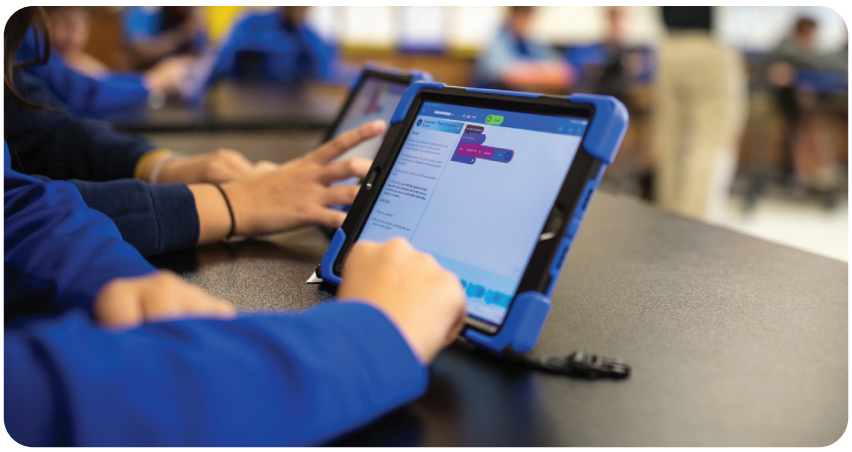
## La aplicación Sphero Edu

Descarga la aplicación The Sphero Edu aquí .

## Crear clases y asignar actividades

Cree una cuenta de maestro para que pueda configurar y administrar clases como educador. Tienes algunas opciones para administrar tus clases:

- **Códigos de clase (recomendado)**
  Si prefiere que los estudiantes trabajen en tareas sin un nombre de usuario y contraseña, distribuya códigos de clase. Simplemente ingrese un nombre de clase y el código de clase se generará automáticamente. Proporcione a los estudiantes el código de clase para acceder a sus tareas y continuar trabajando en sus programas. A diferencia de las clases estándar, el progreso del estudiante se guarda en la clase en lugar de en una cuenta. Aprende más **aquí** .
- **Clase estándar**
  Cree cuentas de estudiantes manualmente o cargando un CSV. Estas cuentas de estudiantes incluyen nombres de usuario y contraseñas individuales para cada estudiante. En este modelo, puede asignar actividades a los estudiantes para que las completen, pero no puede asignar programas directamente. Todo el trabajo de los estudiantes se guarda en su cuenta personal y no en la clase en sí.
- **Usuarios de Google o Clever**
  Puedes sincronizar automáticamente tus clases con Sphero Edu. Ver más información **aquí** .



## Robots de carga

Los robots Sphero BOLT se cargan mediante carga inductiva en la base provista. Para cargar, coloque su robot en la base de carga con el lado pesado hacia abajo. Verá una luz azul parpadeando en la base para indicar que se está cargando. BOLT necesitará hasta 6 horas para una carga completa, pero el tiempo variará según el nivel actual de la batería y sabrá que está cargada cuando la luz azul deje de parpadear.

## Solución de problemas

- Asegúrese de que el firmware del robot esté actualizado. Si se requiere una actualización de firmware, comenzará automáticamente después de que se conecte a un dispositivo.
- Cargue robots y dispositivos la noche antes de usarlos en clase.
- Asegúrate de que la aplicación Sphero Edu esté actualizada.
- Reinicie su robot Sphero manteniendo presionado el botón del cargador y retirando el robot de la base de carga, luego vuelva a colocarlo en la base de carga.

## Apoyo

Sphero está empoderando a los futuros creadores del mañana y preparándolos para el éxito. No podríamos estar más entusiasmados con el futuro de la educación y el papel que estamos desempeñando. Para obtener más información sobre Sphero y participar en nuestra comunidad, puede encontrar enlaces a recursos adicionales a continuación.

- **Blog de esfero -** Visita nuestro **blog de educación** para actualizaciones, consejos y sugerencias.
- **Apoyo -** Visita nuestro **Pagina de soporte** para preguntas frecuentes y consejos y trucos para la solución de problemas.
- **Contáctenos -** Para cualquier soporte adicional o ayuda contáctenos **aquí** .