UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS
ESCUELA DE INGENIERÍA INFORMÁTICA

TRABAJO FINAL DE GRADUACIÓN PARA OPTAR POR EL GRADO DE BACHILLERATO EN INGENIERÍA EN SISTEMAS

“Propuesta para un Programa de Formación en Ciberseguridad para la Población del Liceo de Pavas”

Luis Andrés Montero Madriz
SUSTENTANTE

Henry Rodríguez Chacón

TUTOR

Sede Central

Agosto, 2024

DEDICATORIAS

Este trabajo final de graduación se lo dedico primeramente a Dios, ya que a pesar de que se presentaron algunos inconvenientes en el camino, me dio la fuerza y la dirección para ejecutar las acciones necesarias para llegar hasta este momento y me permite culminar una meta determinante para seguir creciendo como profesional.

También se lo dedico a mis hijos que, sin ellos darse cuenta, son pilares fundamentales en mi vida, a diario me impulsan a superarme y esforzarme y me enseñan a valorar y a sentirme agradecido por lo afortunado que soy de tenerlos, lo cual me da el combustible necesario y me motiva a mejorar para ser su ejemplo de vida.

AGRADECIMIENTOS

Un sincero agradecimiento a Georgina Fonseca Marín, que me acompañó en es este largo y retador camino, el cual estuvo cargado de momentos de estrés y alegría. Su apoyo, confianza y paciencia han sido fundamentales y son parte importante en este logro, ya que ella se convirtió, en un sostén para no flaquear y continuar fortalecido hasta el final. Su ayuda incondicional en cada una de las etapas del proceso fue vital para llegar hasta acá.

También, quisiera expresar mi gratitud a todas las personas que contribuyeron con el desarrollo de mi investigación. Agradezco a los estudiantes, docentes y padres de familia de la institución en la cual se realizó la propuesta, ya que fueron muy importantes en el proceso de recopilación de datos para desarrollar el proyecto.

Finalmente, quiero extender mi agradecimiento a la dirección de carrera y a cada uno de los profesores que me brindaron su apoyo y retroalimentación en el desarrollo del trabajo final de graduación, ya que han contribuido de manera sustancial para culminar esta meta.

Tabla de contenidos

RESUMEN EJECUTIVO 17
CAPÍTULO I. INTRODUCCIÓN 18
Planteamiento del Problema 18
Objetivos 19
Objetivo General 19
Objetivos Específicos 19
Justificación 20
Viabilidad Técnica 22
Viabilidad Operativa 22
Viabilidad Económica 23
Viabilidad Legal 24
Proyecciones 24
Alcances 25
Alcance Funcional 26
Alcance Metodológico 28
Alcance tecnológico 28
CAPÍTULO II. MARCO REFERENCIAL 29
Papel de la ciberseguridad en el ciberespacio 30
Importancia, fundamentos y conceptos de la ciberseguridad 31
Tipos de amenazas que se encuentran en el ciberespacio 32
Malware 32
Ingeniería social 33
Ataques a aplicaciones web 34
Ataques a la cadena de suministro 35
Ataques DoS 35
Ataques MitM 36
Recomendaciones para evitar ser víctimas de los ciberdelincuentes 36
Situación actual de Costa Rica en ciberseguridad 38
Plan Nacional de Ciberseguridad 40
La ciberseguridad y el impacto en los jóvenes 42
Importancia de la educación en ciberseguridad en edades tempranas 42

Peligro al que se enfrentan los jóvenes en el ciberespacio en la actualidad 43
Ciberbullying / Ciberacoso 44
Grooming 45
Sexting 46
Fake News 47
Publicación de información privada 47
Papel de las redes sociales y las plataformas digitales en los adolescentes 48
La educación en ciberseguridad en edades tempranas a nivel mundial 50
Israel, un ejemplo en programas de formación en ciberseguridad 52
Reino Unido, líder en ciberseguridad en Europa 53
Estados Unidos, implementado estrategias de educación en ciberseguridad 56
Costa Rica y su educación en ciberseguridad 58
Malla curricular, Programa Nacional de Formación Tecnológica 60
Los docentes, figuras importantes en la formación de los adolescentes en ciberseguridad 61
Impacto vocacional para la elección de carreras tecnológicas 64
Desarrollo integral en la formación de los jóvenes 65
Los padres como actores vitales en la formación de seguridad en línea de los adolescentes 66
Importancia de una política en ciberseguridad en el Liceo de Pavas 69
CAPÍTULO III. MARCO METODOLÓGICO 72
Enfoques de Investigación 72
Enfoque cuantitativo 72
Enfoque cualitativo 73
Enfoque mixto 73
Enfoque de investigación seleccionado 74
Tipos de Investigación 74
Investigación exploratoria 75
Investigación descriptiva 75
Investigación correlacional 75
Tipo de investigación seleccionado 76
Fuentes de Información 76
Fuentes primarias 76
Fuentes secundarias 77

Fuentes terciarias 77
Fuentes de información seleccionadas 78
Variables 78
Población 80
Muestra 81
Instrumentos de Recolección de Datos 82
CAPÍTULO IV. ANÁLISIS DE RESULTADOS 83
CAPÍTULO V. PROPUESTA 91
Guía de Ciberseguridad para Estudiantes del Liceo de Pavas 93
Guía de Ciberseguridad para Padres de Familia del Liceo de Pavas 95
Guía de Ciberseguridad para Profesores y Personal Administrativo de Liceo de Pavas 96
Política de Seguridad de la Información para el Liceo de Pavas 97
Lineamiento para la gestión y control de accesos físicos 97
Lineamiento de protección de información sensible 98
Lineamiento para la gestión de redes seguras 99
Lineamiento para la gestión de los equipos y antivirus 99
Lineamiento para la gestión de contraseñas seguras 100
Lineamiento de respaldo de datos 100
Lineamiento de gestión de terceros 101
Lineamiento para el uso de controles de filtrado web 101
Lineamiento para la gestión de las redes sociales 102
CAPÍTULO VI. CONCLUSIONES Y RECOMENDACIONES 103
Conclusiones 103
Recomendaciones 105
REFERENCIAS 109
APÉNDICE A. ENCUESTA PARA ESTUDIANTES 116
APÉNDICE B. ENCUESTA PARA PADRES DE FAMILIA 119
APÉNDICE C. ENCUESTA PARA DOCENTES 122
APÉNDICE D. GUÍA DE ENTREVISTA SEMIESTRUCTURADA 124
APÉNDICE E. GUÍA DE CIBERSEGURIDAD PARA ESTUDIANTES DEL LICEO DE PAVAS 125
APÉNDICE F. GUÍA DE CIBERSEGURIDAD PARA PADRES DE FAMILIA Y ENCARGADOS DEL LICEO DE PAVAS 161

APÉNDICE F. GUÍA DE CIBERSEGURIDAD PARA PROFESORES Y PERSONAL ADMINISTRATIVO DEL LICEO DE PAVAS 183

APÉNDICE H. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL LICEO DE PAVAS 203

Tablas

Tabla 1 Costos del recurso humano del proyecto 23
Tabla 2 Cuadro de variables de la investigación 79

Figuras

Figura 1 Porcentaje de docentes que conversa con sus estudiantes acerca de las actividades en línea 84
Figura 2 Conocimiento de los docentes acerca de los derechos del uso de datos personales en medios digitales 85
Figura 3 Redes sociales más utilizadas por los jóvenes del Liceo 87
Figura 4 Porcentaje de estudiantes que dice haber sido víctimas de ciberacoso 87
Figura 5 Porcentaje de estudiantes que tiene conocimientos en amenazas cibernéticas 88
Figura 6 Formación que reciben los jóvenes por parte de los profesore acerca de los riesgos en línea 89

RESUMEN EJECUTIVO

El proyecto de investigación consiste en una Propuesta para un Programa de Formación en Ciberseguridad para la Población del Liceo de Pavas, la cual es una institución conformada por una población estudiantil de aproximadamente 1600 estudiantes y cuenta con 120 colaboradores entre personal docente y administrativo. En la actualidad, los jóvenes están expuestos a una ola creciente de delincuencia digital, donde carecen de herramientas para afrontarla y gestionar temas como el ciberacoso, sexting, estafas, suplantación de identidad, ataques de malware y phishing.

Actualmente, los adolescentes tienen prácticas riesgosas en las redes sociales, generando un intercambio excesivo de información, donde desconocen la sensibilidad de brindar datos personales, ubicación y otros; por esto, es importante agudizar los sentidos y el conocimiento de los estudiantes de manera prioritaria para formar una sociedad informada.

Adicionalmente, tanto padres de familia como el personal docente y administrativo carecen de conocimiento en temas de seguridad en línea, lo cual limita la educación, acompañamiento y supervisión que puedan brindar a los adolescentes. Además, dicha institución carece de una política para el manejo de la seguridad de la información, activos o recursos.

El alcance de la propuesta es brindar a cada uno de los actores implicados en la cadena de valor, fundamentos para ejecutar mecanismos de prevención y protección contra las amenazas que se enfrentan a diario en el ciberespacio, por medio de guías formativas y una política de seguridad de la información en la institución educativa.

El tipo de investigación es descriptiva, pues se detallan propiedades, características y datos importantes sobre la importancia de la formación en ciberseguridad en adolescentes, basándose en programas educativos nacionales e internacionales. Además, por medio de los instrumentos de recolección de datos se exponen las carencias de conocimiento en ciberseguridad de los diferentes actores.

Finalmente, se destaca que es de suma importancia ejecutar e implementar programas formativos en las instituciones de educación pública, que fomenten el conocimiento de la seguridad en línea, creando una sociedad informada desde edades tempranas y a su vez, impactando de manera trasversal a los otros implicados en el proceso educativo, como lo son los padres de familia y personal docente.

CAPÍTULO I. INTRODUCCIÓN

Planteamiento del Problema

La propuesta será desarrollada en el Liceo de Pavas, el cual se ubica en Lomas del Río, Pavas, es una institución de dirección 3 conformada por una población estudiantil de 1600 a 2000 estudiantes, siendo esta la categorización de mayor rango; brinda educación de tercer ciclo y educación diversificada, su matrícula anual ronda aproximadamente los 1650 estudiantes y cuenta con 120 colaboradores entre personal docente y administrativo.

En la era digital, los riesgos son inherentes, por ende, es vital tener conocimiento y prácticas de seguridad en el ciberespacio, principalmente en una edad tan vulnerable como lo es la adolescencia. Lo anterior, porque los jóvenes están expuestos a una ola creciente de delincuencia digital, donde carecen de herramientas para afrontar y gestionar temas como el ciberacoso, sexting, estafas, suplantación de identidad, ataques de malware, phishing y otras problemáticas que cada vez van filtrándose de manera más ingeniosa y casi indetectables.

Ante esta realidad, los adolescentes son afectados por prácticas riesgosas en las redes sociales, generando un intercambio excesivo de información, donde desconocen de la sensibilidad de brindar datos personales, ubicación y otros, los cuales se convierten en insumos para un posible ataque. Por lo que, es pertinente agudizar los sentidos y el conocimiento de los estudiantes para formar una sociedad actual y futura informada.

Según la II Encuesta Kids Online (2023) desarrollada por el Instituto de Investigaciones Psicológicas y la Fundación Paniamor, un 40 % de la población encuestada aseguró haber sido víctima de acoso por parte de un amigo o amiga; el 34,3 % de algún desconocido; un 20 % de los encuestados señaló haber sido maltratado por alguien y el 12 % de los adolescentes entrevistados indicó haber recibido mensajes con contenido sexual.

A nivel país, considerando la exposición tan grande a la que están sometidos los jóvenes en el mundo digital es esencial analizar, comparar y aprender acerca de las buenas prácticas de países líderes en la materia, pues es la base del desarrollo de una propuesta más robusta de capacitación en el tema y permite formar desde edades tempranas a los ciudadanos para que funjan como escudos humanos de los ataques cada vez más notorios y principalmente en espacios donde se mueven los estudiantes, como lo son las redes sociales.

Costa Rica está dando sus primeros pasos en la formación en ciberseguridad por medio de la iniciativa denominada “Estrategia Nacional de Ciberseguridad” (MICITT 2023-2027); sin embargo, no existe una educación robusta para formar en edades tempranas y especialmente a los adolescentes acerca de este tópico. Si bien es cierto, la malla curricular actual en formación tecnológica del Ministerio de Educación Pública se robusteció, los temas en ciberseguridad se ven como un eje trasversal de los módulos educativos (Programa Nacional de Formación Tecnológica, 2024).

Adicionalmente, tanto padres de familia como el personal docente y administrativo del Liceo Pavas carecen de conocimiento en temas de seguridad en línea, lo cual limita la educación, acompañamiento y supervisión que se pueda brindar a los adolescentes. Sobre esta misma línea, en la institución no existe una política para el manejo de la seguridad de la información, activos o recursos, además los estudiantes carecen de conocimientos acerca de los riesgos a los que se enfrentan en el ciberespacio y no existe una cultura consciente de la prevención y protección que los forme ante los desafíos futuros en el panorama digital.

Objetivos

Objetivo General

Elaborar una propuesta para un programa de formación en ciberseguridad para la población del Liceo de Pavas, con el fin de dotarlos de fundamentos y conceptos, por medio de guías educativas y una política de seguridad de la información.

Objetivos Específicos

Investigar los programas educativos en los países líderes en ciberseguridad, como Israel, Estados Unidos y Reino Unido.

Analizar el Programa Nacional de Formación Tecnológica en el Sistema Educativo Costarricense y su enfoque en ciberseguridad.

Conocer los riesgos y amenazas a las que están expuestos los jóvenes del Liceo de Pavas en el ciberespacio.

Comprender los desafíos a los que se enfrentan los profesores y personal administrativo en materia de ciberseguridad.

Identificar los mecanismos de prevención que deben implementarse por parte de los padres de familia para proteger a sus hijos de las amenazas cibernéticas.

Determinar las brechas en seguridad de la información, activos y recursos educativos que existen en la institución.

Justificación

El auge del mundo digital y el crecimiento acelerado de plataformas de interacción digital hacen que, en paralelo a este desarrollo, crezcan también los riesgos a los que se impone la sociedad y es aquí donde la ciberseguridad cumple un papel vital a nivel de prevención y manejo de crisis. Por lo que, tal y como se cita en el artículo de *Cisco Umbrella's Top 10 Cybersecurity Tips* por parte de Bellón (2024), el eslabón más débil en cualquier sistema de seguridad es la persona, por esta razón, la formación en ciberseguridad viene a ser imperante y un eje clave de responsabilidad ciudadana; independientemente de la condición socioeconómica o de variables demográficas y psicográficas, pues todos están expuestos a los riesgos en el ciberespacio y por esto, es esencial crear una sociedad informada desde edades tempranas, para ir cerrando las brechas de seguridad digital.

En los últimos años, Costa Rica ha experimentado un aumento en los ciberataques, lo cual ha generado un impacto en la economía digital y en la seguridad nacional, tal y como lo indica la ministra Paula Bogantes del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en la Estrategia Nacional de Ciberseguridad (p. 3).

Actualmente, el país se encuentra dando sus primeros pasos en esta materia, por medio de la Estrategia Nacional de Ciberseguridad, que viene a establecer un plan de acciones individuales y colectivas, para reforzar la gobernanza de la seguridad en línea y mitigar las amenazas en el ecosistema digital, en donde el país y sus ciudadanos están expuestos.

La educación de esta materia desde la adolescencia es muy importante, por el amplio acceso a internet que tiene una gran parte de esta población y por el uso de las redes sociales, que conduce a que los jóvenes se encuentran en un punto en donde sus actividades en línea tienen consecuencias en el mundo real. En esta misma línea, los adolescentes deben hacer frente a una serie de amenazas

cibernéticas, como lo son el ciberacoso, ciberbullying, grooming, phishing, suplantación de identidad, entre otras, lo cual los convierte en una población vulnerable, es por esto, por lo que se vuelve necesario que conozcan los riesgos a los que se enfrentan y es vital educarlos y guiarlos en esta etapa para su desarrollo como ciudadanos digitales informados.

Según las cifras de la II Encuesta Kids Online, desarrollada por el Instituto de Investigaciones Psicológicas y la Fundación Paniamor se evidencia una alarmante realidad que cada vez está en crecimiento, por ello, el objetivo de la propuesta es ser un instrumento de formación para los estudiantes, a nivel de ciberseguridad, también para los padres de familia, pues la encuesta arrojó que existe una mayor supervisión parental en los niños menores de 12 años, mientras que, para la población adolescente, la cual presenta mayores habilidades en el uso del internet, existe menos mediación parental. Esto exhibe que se debe fomentar la participación y colaboración de los padres en la promoción de hábitos seguros y de técnicas de prevención para que tanto ellos como sus hijos no sean víctimas de las amenazas cibernéticas.

Unos actores muy importantes en la formación de los jóvenes son los docentes y el personal administrativo, ya que a nivel institucional ellos son los encargados de brindar las herramientas formativas en estos temas, el dilema es que en muchas ocasiones ellos carecen de educación en materia de ciberseguridad y en lugar de fomentar una cultura de protección y prevención frente a riegos, se vuelven uno más en el ecosistema de población vulnerable.

Según lo establece la Ley Nº8968, Protección de la Persona Frente al Tratamiento de sus Datos Personales (2011), la manipulación que se ejerce sobre los datos sensibles de las personas es muy delicado, por lo que, el rol que ejercen los docentes es importante, ya que estos almacenan y transmiten información confidencial de los estudiantes y muchos mantienen un manejo inadecuado de la información, lo que se traduce en una violación a la ley.

Adicionalmente, el centro educativo tiene una enorme responsabilidad en la protección de datos sensibles de los estudiantes y padres de familia, así como otros aspectos de confidencialidad, como lo son la información financiera de la institución, por ello es fundamental velar por proteger los activos y recursos educativos ante ciberdelincuentes, piratas informáticos o personas internas maliciosas que buscan robarlos, manipularlos o destruirlos con diversos fines, como extorsión, espionaje o sabotaje; considerando esto, la propuesta formula la elaboración de una política de ciberseguridad para el Liceo de Pavas, que permita mitigar los riesgos a través de la ejecución de acciones concretas.

La propuesta brinda a cada uno de los actores implicados en la cadena de valor, fundamentos para ejecutar mecanismos de prevención y protección contra las amenazas que se enfrentan diariamente en el ciberespacio.

Viabilidad Técnica

La propuesta para el programa de formación es posible, dado que actualmente el Liceo de Pavas cuenta con 6 profesores que imparten materias de tecnología, bajo un programa establecido por el Ministerio de Educación Pública, el cual establece un cronograma semanal de 3 lecciones para cada estudiante y con este proyecto se aprovecharía parte de este tiempo para impartir la guía con el contenido y temas a tratar a los estudiantes, así como otros espacios que ellos determinen para capacitar a los profesores en general, al personal administrativo y padres, con el fin de dotarlos de herramientas y que de esa manera, detecten, eviten y aborden posibles casos de ciberacoso, estafas, robo de identidad, fraude en línea y desinformación, así como leyes y normas.

Viabilidad Operativa

La ciberseguridad es un tema que atañe a todos, por lo que, con el fin de ser ciudadanos digitales informados y ser escudos humanos ante las amenazadas a las que se está expuestos, se plantea está propuesta diseñada para los actores principales, a saber: estudiantes, profesores, personal administrativo y padres de familia; la educación se brindará a través de los profesores que imparten las materias de tecnología, ya que cuentan con la formación académica necesaria y las herramientas para explicar, desarrollar el programa y entender los nuevos conocimientos que aporte la propuesta.

Por medio de la propuesta, se pretende cambiar la manera en la que se abordan los temas de vulnerabilidad digital de los estudiantes, así como el manejo de los datos y activos que se dan en la institución; también se busca despertar la conciencia en los padres de familia sobre las alertas que deben tener presentes a nivel de ciberseguridad, para establecer los controles para monitorear y fomentar una cultura de prevención y protección frente a los riesgos y amenazas del ciberespacio.

En cuanto al personal docente y administrativo, estos serán formados por los profesores de tecnologías, se les dará a conocer los cambios que deban hacer a nivel de manejo de la información

que se determinen en la política. Por lo que, dentro del alcance del proyecto no se contempla la formación, entrenamiento o ejecución de las guías a desarrollar.

Viabilidad Económica

La propuesta no tiene costo, dado que es investigativa y se cuenta con los insumos gratuitos para fundamentarla, de la misma manera, la institución no debe incurrir en gastos de horas extras o en personal adicional, pues se capacitará al recurso humano actual para llevar a cabo la propuesta, asimismo, se aprovecharán los espacios ya definidos (lecciones, reuniones de personal y reuniones con padres de familia) para impartir la formación.

En cuanto a la política, está dicta las directrices que deben seguirse para resguardar la seguridad de la información de los estudiantes y el personal que labora en la institución, esto generará cambios en el tratamiento de los datos y no implica un gasto extra para el personal docente, administrativo ni tampoco para la institución.

Es importante mencionar que, la propuesta no tendrá ningún costo; sin embargo, a continuación, se detallará cuál sería el costo y el tiempo que requiere cada entregable, para esto se utiliza la lista de salarios mínimos del Ministerio de Trabajo y Seguridad Pública, en la cual un Programador en computación (sin título), obtiene una remuneración diaria de ¢15.613,91.

Tabla 1

Costos del recurso humano del proyecto.

Entregables	Días	Costo
Realizar una comparación de los contenidos de los programas educativos.	5	¢78.069,55
Elaborar una guía de conceptos para los docentes y personal administrativo.	10	¢156.139,1
Desarrollar una guía de formación básica para los padres de familia del Liceo de Pavas.	6	¢93.683,46
Construir una guía de contenido y temas por tratar para los estudiantes.	10	¢156.139,1
Elaborar una Política de Ciberseguridad para el Liceo de Pavas.	8	¢124.911,28
Total	**39**	**¢608.942,49**

Fuente: elaboración propia, 2024.

Viabilidad Legal

De acuerdo con el tipo y formato de la propuesta, se cuenta con la viabilidad legal, dado que esta se basa en leyes que respaldan la investigación y fungen como marco legal para la propuesta de política para el Liceo y para fundamentar y justificar la razón de ser de la investigación.

A continuación, se detallan las leyes sobre las cuales se fundamenta este apartado:

- Ley 8148 Adición de los artículos 196 BIS, 217 BIS y 229 BIS al Código Penal.
- Ley N.°4573 para reprimir y sancionar los delitos informáticos de la Asamblea Legislativa de la República de Costa Rica del año 2001.
- Ley de Derechos de Autor 6683 por parte de la Asamblea Legislativa de la República de Costa Rica del año 1982.
- Ley 8968 sobre la protección de la persona frente al tratamiento de sus datos personales.
- Ley 7739. Código de la Niñez y la Adolescencia, Asamblea Legislativa de Costa Rica, 1998.
- Ley 9452. Convenio sobre la Ciberdelincuencia (Budapest, 2017).
- Ley 8934. Ley de Protección de la Niñez y la Adolescencia frente al contenido nocivo de Internet y otros medios electrónicos. (Asamblea Legislativa de Costa Rica, 2011).

Proyecciones

Se espera que, con la presente propuesta de investigación, los estudiantes del Liceo de Pavas adquieran herramientas en ciberseguridad que les permita ser ciudadanos digitales informados, que conozcan acerca de cómo tener comportamientos saludables en el ciberespacio, así como lograr identificar las posibles riesgos y vulnerabilidades que resulten del uso de redes sociales, aplicaciones y sitios web, como lo son el grooming, el ciberacoso, el sexting y otros.

En la misma línea, la propuesta busca desarrollar el pensamiento crítico-analítico, el cual es una habilidad blanda que demanda el mundo profesional actual; además, pretende mejorar sus destrezas en prácticas seguras de creación de contraseñas, protección de cuentas y datos, identificación de ciberestafas y suplantación de identidad.

Actualmente, hay una escasez de profesionales en el campo de la ciberseguridad, al ser una carrera de alta demanda mundial, por ende, con la propuesta de formación se busca generar de manera indirecta, que los estudiantes realicen una exploración profesional y se inclinen por carreras de esta índole, que incluso puede facilitarles su inserción laboral y al ser carreras bien remuneras, brindarles la posibilidad de mejorar su condición socioeconómica, considerando que son estudiantes que pertenecen a una población que es socialmente vulnerable.

El impacto para la institución y su personal docente y administrativo se enfoca en dos vías, la primera, que con los conocimientos en ciberseguridad y la política puedan ser instrumentos de guía y oficiales de ciberseguridad para los estudiantes y que logren identificar amenazas cibernéticas en las que se vean expuestos, además, que puedan apoyar y erradicar posibles conductas de ciberacoso, conductas de riesgo y enseñar a los estudiantes a activar sus alertas, mientras navegan en la web.

En una segunda vía, la propuesta busca que los profesores y personal administrativo apliquen prácticas seguras de manejo de datos sensibles de cada estudiante, la protección de activos y recursos educativos; por lo que, estos datos son insumos atractivos para los depredadores cibernéticos que los utilizan para diversos fines como sabotajes, destrucción, ingeniería social, espionaje y delitos contra los menores.

En cuanto al impacto de la propuesta de formación para los padres de familia, se pretende que genere un acercamiento con sus hijos, con el fin de supervisarlos y guiarlos para lograr establecer límites en cuanto al tiempo de uso en las plataformas digitales, manejo y control de la adicción a la tecnología y supervisar el uso de internet y la información que comparten.

Finalmente, la propuesta tiene un enfoque social que impacta a la población estudiantil y sus familias, pues al pertenecer a una comunidad de riesgo social, es primordial brindarles una guía sobre la importancia de la ciberseguridad y enseñarles cómo prevenir conductas peligrosas en línea.

Alcances

El alcance de la presente investigación es generar una propuesta para el programa de formación en ciberseguridad para la población del Liceo de Pavas, la cual busca integrar a los diferentes actores del centro educativo: los estudiantes, el personal docente y administrativo, así

como los padres de familia y la institución como tal, dentro de dicho entregable se plantea la generación de una política de ciberseguridad para el Liceo.

Adicionalmente, se desea generar una conciencia colectiva acerca de la importancia de mantener prácticas seguras en línea y acerca de los distintos factores claves que deben ejecutarse a nivel de la protección en el ciberespacio.

Alcance Funcional

Nombre del apartado	Descripción del apartado
Informe y análisis de los programas educativos en ciberseguridad a nivel internacional en edades tempranas. Análisis del Programa Nacional de Formación Tecnológica en el Sistema Educativo Costarricense.	Realizar una comparación de los contenidos de programas educativos en ciberseguridad de Israel, Reino Unido y Estados Unidos con el Programa Nacional de Formación Tecnológica propuesto por el MEP, con el fin de realizar una propuesta práctica en Ciberseguridad para el Liceo de Pavas.
Alfabetización digital del personal docente y administrativo del Liceo de Pavas en materia de ciberseguridad.	Elaborar una guía de formación en conceptos fundamentales en ciberseguridad para los docentes y personal administrativo del Liceo de Pavas, con el fin de dotarlos de herramientas que les permita tener un papel formativo en los estudiantes, ya que es determinante que los profesores conozcan los riesgos a los que se expone la juventud en el mundo digital y puedan detectar, evitar y abordar posibles casos de ciberacoso, estafas, robo de identidad, fraude en línea y desinformación, así como leyes y normas.
Concientización a los padres de familia sobre los riesgos y prevenciones en el mundo digital.	Desarrollar una guía de formación básica para los padres de familia del Liceo de Pavas, con el fin de educarlos para que sean ciudadanos informados y puedan orientar y supervisar a sus hijos, aplicando controles parentales, así como conocimiento de las

	diversas amenazas en línea a las que están expuestos los jóvenes en la actualidad.
Estrategia de educación y capacitación en Ciberseguridad para los estudiantes de secundaria del Liceo de Pavas.	Construir una guía de contenido y temas a tratar para los estudiantes de décimo y undécimo del Liceo de Pavas, en conceptos y fundamentos en materia de ciberseguridad. Diseñar el programa "Ciber Embajadores" en el cual, los estudiantes de décimo y undécimo que sean formados en materia de ciberseguridad serán los encargados de transmitir los conocimientos adquiridos a la comunidad estudiantil de sétimo, octavo y noveno, fomentando el aprendizaje activo y al mismo tiempo, educando a los más jóvenes en materia de ciberseguridad para prepararlos ante el transitar del mundo digital y para ser la siguiente generación de ciber embajadores.
Política de Seguridad de la Información para el Liceo de Pavas.	Elaborar una Política de Ciberseguridad para el Liceo de Pavas, con el fin de proteger los activos y recursos educativos, puesto que las instituciones educativas almacenan y procesan una gran cantidad de datos confidenciales, como registros de estudiantes, información sensible en temas disciplinarios o emocionales, así como información financiera, entre otros. Estos datos suelen ser el objetivo de ciberdelincuentes, piratas informáticos o personas internas maliciosas que buscan robarlos, manipularlos o destruirlos con diversos fines, como extorsión, espionaje o sabotaje.

Fuente: elaboración propia, 2024.

Alcance Metodológico

Se desarrollará la propuesta bajo una adaptación de la metodología ágil, esto implica dividir el proyecto en fases de corto plazo (*sprints*), con el objetivo de obtener resultados rápidos y efectivos. Además, se dará un seguimiento diario, donde se revisará el cumplimiento de lo definido, respetando las etapas del ciclo de vida del proyecto, el cual consta de una etapa de inicio que consiste en la elaboración del anteproyecto, en donde se define el planteamiento del problema, los objetivos, justificación y las proyecciones, para determinar los alcances y viabilidad de la propuesta.

Posteriormente, se pasa a la fase de planificación, donde se realiza la estructura de tareas a ejecutar, se elabora el cronograma de entregables y se plantea la ruta a seguir para finalmente, continuar con la ejecución, en la cual se pone en marcha el plan creado en la etapa anterior y se desarrollan los entregables, que serán evaluados en el ciclo de cierre de la propuesta.

Alcance tecnológico

A nivel tecnológico no tiene una implicación directa, ya que consiste en una propuesta de investigación, para esta se utilizará una computadora portátil de uso personal, que cuenta con un paquete básico de Office y para el desarrollo de las guías se hará uso de la herramienta gratuita de diseño gráfico, Canva.

CAPÍTULO II. MARCO REFERENCIAL

La digitalización representa un cambio radical en esta nueva era, la humanidad se encuentra viviendo una etapa incierta en la que lo único indiscutible es la velocidad a la que avanza, pero ha venido a establecer nuevas reglas y maneras de realizar distintas acciones, además ha traído consigo progresos importantes que han contribuido a la humanidad de una manera decisiva; sin embargo, también ha impactado de manera negativa e irreversible en muchos aspectos.

Las plataformas digitales han sustituido las formas de cómo hacer las cosas, en la actualidad para comprar un libro ya no se necesita ir a una tienda física, las redes sociales se han encargado de ser los "nuevos noticieros 24-7", por lo que, actualmente no se necesita tener propiedades para arrendar como lo ha demostrado Airbnb, puesto que los transportes han sido revolucionados por herramientas como Uber que a su vez, impactan de manera colateral a otras industrias como la alimentaria, ofreciendo facilidades de entrega de pedidos.

En la era del internet es importante conocer el concepto de "ciudadanía digital" y comprender el funcionamiento y los principios que rigen el entorno digital, por lo que, según la guía "¿Cómo ejercer una ciudadanía digital responsable?" (2021): "significa adquirir conocimientos y desarrollar actitudes, habilidades y competencias fundamentales para la vida en democracia, incluyendo el conocimiento de las reglas y responsabilidades de la convivencia en el mundo digital" (p. 3).

Como ciudadanos digitales se tiene deberes y derechos y es por esto, por lo que, es fundamental comprender los principios de interacción, uno de ellos es la libre expresión, pues si bien es cierto el ciberespacio se ha convertido en un espacio en donde la comunicación se ha ampliado, existen límites que no se pueden sobrepasar para no dañar o afectar a otros usuarios.

En ese contexto, es donde radica la importancia de practicar valores en línea, como la empatía y la tolerancia, ya que son vitales para entender que no todos los usuarios deben pensar de la misma manera y aunque no se compartan ciertos criterios, hay que respetar a todos por igual, ya que todo lo que se haga o se diga puede repercutir en la vida de los demás.

Para profundizar y comprender más a detalle la huella de la digitalización en la era actual, es necesario conocer algunas estadísticas relevantes, según el sitio web *We Are Social* en colaboración con Meltwater (2024), donde se detalla en su informe del primer trimestre los siguientes datos:

> Las Naciones Unidas indican que en la Tierra viven hoy en día 8.100 millones de personas. La población mundial aumentó en 74 millones el año pasado, lo que supone un crecimiento anual del 0,9 %. El número de usuarios únicos de teléfonos móviles asciende a 5.65 billones, lo que significa que el 69,7 % de la población mundial utiliza un teléfono móvil. Los usuarios únicos de móvil crecieron un 2,4 % en los últimos 12 meses, gracias a 133 millones de nuevos usuarios.
>
> Los usuarios de Internet han ascendido a 5.44 billones, con 178 millones de nuevos usuarios en el último año, lo que eleva la tasa de penetración mundial de Internet al 67,1 %, esto significa que más de 2 de cada 3 habitantes de la Tierra están ahora conectados. El número de usuarios de Internet también sigue creciendo, y las últimas cifras apuntan a un aumento interanual del 3,4 %.
>
> El análisis muestra que el uso activo de las redes sociales también sigue creciendo, habiendo plataformas que han añadido más de 250 millones de nuevas identidades de usuario únicas desde el año pasado. El total mundial de usuarios alcanzó los 5.070 millones a principios de abril de 2024, una cifra un 5,4 % superior a la de abril de 2023 (párr. 11-13).

A partir de la cita anterior, la tecnología trae consigo múltiples beneficios que facilitan la vida de los consumidores, pero también presentan una serie retos y desafíos, como por ejemplo, resguardar la información y la seguridad de la red. Por lo que, ante la creciente conectividad y el intercambio de datos, las empresas y los usuarios necesitan garantizar la protección de sistemas contra accesos no autorizados y el uso inapropiado de información, así como la protección de datos personales y la administración de contraseñas y autenticación segura.

Papel de la ciberseguridad en el ciberespacio

En los últimos años ha surgido la ciberseguridad como un tema de mucha fuerza, nació desde los años 60 y se ha vuelto vital, debido a los constantes cambios tecnológicos y las amenazas a las que enfrenta la humanidad en la era digital. Ante esto, es importante entender que engloba el concepto y según el artículo titulado: “¿Qué es la ciberseguridad?” Cisco (2024) destaca que: “la ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo

general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; extorsionar a los usuarios o interrumpir la continuidad del negocio" (párr. 1).

La seguridad digital es un proceso diseñado para identificar las amenazas y los riesgos con el fin de atacarlos o mitigarlos evitando daños irreversibles; los recursos tecnológicos son fundamentales para que las organizaciones funcionen de manera óptima; el mundo empresarial está cada día más interconectado y es ahí donde radica la importancia de la disponibilidad y la confidencialidad de la información, ante esto se requiere una política robusta en materia de ciberseguridad para que las organizaciones eviten ser afectados por un impacto significativo.

Importancia, fundamentos y conceptos de la ciberseguridad

En un mundo donde todo está interconectado, la ciberseguridad juega un rol fundamental, la dependencia que existe hacia los sistemas de información, el desarrollo del internet de las cosas (IoT) y el crecimiento exponencial en temas de inteligencia artificial (IA) provoca mayor exposición a las múltiples amenazas cibernéticas que emergen diariamente de una manera desproporcionada, atacando vulnerabilidades y buscando la manera de cómo afectar a los usuarios.

Además, los ciberataques van desde robos de identidad hasta la afectación de servicios críticos en los diferentes países y es allí donde la ciberseguridad es un escudo ante este panorama, según el sitio web de Kaspersky (2024), se mencionan algunos conceptos importantes para clasificar la seguridad:

> La seguridad de red es la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista. La seguridad de las aplicaciones se enfoca en mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad de la información protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito. La seguridad operativa incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría (párr. 2).

En un mundo donde la información personal y empresarial se guarda y transmite digitalmente, la ciberseguridad es fundamental para proteger datos sensibles y salvaguardar la privacidad, además es necesario mantener actualizados los programas, sistemas operativos y aplicaciones en los dispositivos, así como ser ciudadanos informados.

Las empresas deben invertir en medidas de ciberseguridad robustas y mantenerse actualizados con las últimas tendencias y amenazas, por lo tanto, es fundamental enfrentar con éxito, los desafíos cibernéticos en constante evolución.

Tipos de amenazas que se encuentran en el ciberespacio

Es vital entender las amenazas y mecanismos que utilizan para explotar las vulnerabilidades en la red, infraestructura y sistemas, por lo que, según el sitio web de la empresa *Check Point* (2024) en su artículo titulado: *Tipos de amenazas de ciberseguridad*, los principales tipos de amenazas a las que se enfrenta la población actualmente incluyen malware, ingeniería social, exploits de aplicaciones web, ataques a la cadena de suministro, ataques de denegación de servicio y ataques de intermediario, por lo que, a continuación, se describirá en qué consisten cada una de estas amenazas.

Malware

Es un software malicioso que se puede utilizar para lograr muchos objetivos diferentes, con el fin de dañar los sistemas de computación o a sus usuarios. Según detalla *Check Point* (2024), algunos de los tipos de malware más comunes son:

- Ransomware es un malware que cifra los archivos de un dispositivo infectado utilizando una clave de cifrado que sólo el atacante conoce, luego se exige un rescate a la víctima a cambio de la clave de cifrado necesaria para restaurar sus datos.
- El malware troyano pretende pasar desapercibido, por ejemplo, una descarga de un software gratuito, al realizarse la descarga, se ejecuta el troyano en su computadora y acciona su funcionalidad maliciosa.
- Los Remote access trojan (RATs) son un tipo de troyano diseñado para servir como punto de acceso para ataques de seguimiento; una vez que el malware se ejecuta en la computadora

infectada, proporciona al atacante acceso y control remotos, lo que le permite descargar otro malware, robar datos confidenciales o realizar otras acciones.

- Spyware es un software espía diseñado para espiar y recopilar información sobre el usuario de una computadora infectada. Está diseñado para robar credenciales de usuario, datos financieros y otra información sensible.
- Cryptojacking, las criptomonedas utilizan métodos de minería para crear nuevos bloques en la cadena de bloques, estos procesos computacionales son realmente costosos, este tipo de malware utiliza el poder computacional de la víctima para crear bloques y ganar criptomonedas para el atacante.

El malware es una amenaza muy peligrosa, se puede utilizar para múltiples acciones maliciosas como engañar a la persona afectada para obtener información personal, con el fin de cometer robo de identidad, adquirir información de tarjetas de crédito u otros datos financieros de los consumidores; también para tomar el control de múltiples computadoras y llevar a cabo ataques de denegación de servicio en redes ajenas o infectar dispositivos y utilizarlos para minar criptomonedas. Es por esto, por lo que, los usuarios deben estar alertas e informarse de los riesgos en línea y ejecutar acciones que mitiguen estos.

Ingeniería social

Los ataques utilizan trucos, coerción y otras formas de manipulación psicológica para lograr que el objetivo haga lo que el atacante quiere. Según se menciona en el sitio web de *Check Point* (2024), algunos ejemplos de tácticas comunes de ingeniería social incluyen:

- Phishing son ataques que utilizan técnicas de ingeniería social para intentar engañar al destinatario, para que realice una acción que beneficie al atacante. Los mensajes de phishing (enviados por correo electrónico, redes sociales, aplicaciones de comunicaciones corporativas u otras plataformas de mensajería) generalmente están diseñados para engañar a un objetivo, para que haga clic en un enlace malicioso, abra un archivo adjunto malicioso o entregue información confidencial, como credenciales de inicio de sesión.
- Spear phishing son ataques de phishing que están dirigidos a una persona o grupo en particular y utilizan información sobre su objetivo para hacer más creíble el pretexto del mensaje de phishing.

- Smishing son ataques de phishing realizados mediante mensajes de texto SMS. Estos ataques aprovechan las características de los dispositivos móviles, como el uso común de servicios de acortamiento de enlaces (como bit.ly) y la capacidad de pasar el mouse sobre un enlace para verificar su destino en mensajes SMS.
- Vishing, estos ataques utilizan muchas de las mismas técnicas que el phishing, pero se realizan por teléfono. El atacante intenta que el objetivo realice alguna acción o entregue datos confidenciales, como la información de la tarjeta de pago o las credenciales de inicio de sesión.

Ante esto, las estrategias y métodos de ingeniería social se fundamentan en el estudio de la psicología humana, manipulando los emociones y reacciones de las víctimas, de manera que inducen a las víctimas a realizar acciones que se utilizan como "portillo" para fines maliciosos. Este tipo de amenazas resultan muy difíciles de prevenir, por lo que, es vital crear una cultura donde se concientice de los peligros de estos ataques.

Ataques a aplicaciones web

Constituyen una parte importante de la superficie de ataque digital de cara al público, algunas de las vulnerabilidades más comunes y de alto impacto en las aplicaciones web, descritas en el sitio web de *Check Point* (2024) son las siguientes:

- **Inyección SQL (SQLI):** se utiliza al interactuar con una base de datos, mezcla datos e instrucciones, a menudo separados por comillas simples (') o dobles (“). Los atacantes proporcionan deliberadamente datos corruptos que se utilizan en una consulta SQL, lo que permite al atacante controlar la acción realizada en la base de datos.
- **La ejecución remota de código (RCE):** son aquellas que permiten a un atacante ejecutar código en el sistema que aloja una aplicación vulnerable. Por ejemplo, un atacante puede aprovechar una vulnerabilidad de desbordamiento de búfer para ejecutar sus comandos maliciosos.
- **Scripting entre sitios (XSS):** consiste en incrustar *scripts* junto con los datos que definen el contenido y la estructura de la página web. Los ataques aprovechan la inyección, el control de acceso u otras vulnerabilidades para insertar *scripts* maliciosos en una página.

Las aplicaciones en línea son fundamentales en el mundo empresarial actual, ya que favorecen la interacción, incrementan la eficiencia, simplifican las transacciones e impulsan las operaciones de las empresas; los ataques dirigidos a aplicaciones web han incrementado en su nivel

de especificidad y automatización, ahí radica la importancia de la ejecución de mecanismos de control y prevención para evitar que se materialicen los riesgos.

Ataques a la cadena de suministro

Ataques a la cadena de suministro que explotan las relaciones de una organización o institución con partes externas. Según se menciona en el sitio web de *Check Point* (2024), algunas de las formas en que un atacante puede aprovechar estas relaciones de confianza incluyen:

- **Acceso de terceros:** las empresas suelen permitir que sus proveedores y otras partes externas tengan acceso a sus entornos y recursos de TI. Si un atacante puede obtener acceso a la red de un socio confiable, puede explotar el acceso legítimo del socio a los sistemas.
- **Software externo de confianza:** todas las empresas utilizan software de terceros y lo permiten dentro de su red; por lo que, si un atacante puede insertar código malicioso en software de terceros o una actualización de este, ese código malicioso puede ser de confianza dentro del entorno de la organización, proporcionando acceso a datos confidenciales y sistemas críticos.
- **Código de terceros:** casi todas las aplicaciones incorporan bibliotecas y códigos de fuente abierta y de terceros. Este código externo puede incluir vulnerabilidades explotables.

Ante esto, es importante identificar a tiempo un ataque a la cadena de suministro para garantizar que los efectos sean mínimos y puedan revertirse. Por lo que, mediante el empleo de herramientas actualizadas, es posible identificar todos los tipos de ataques a la cadena de suministro.

Ataques DoS

Los ataques de denegación de servicio (DoS) están diseñados para interrumpir la disponibilidad de un servicio. Según el sitio web de *Check Point* (2024), las amenazas DoS más comunes son las siguientes:

- **Ataques DoS distribuidos (DDoS):** en un Ataque DDoS, varias máquinas envían muchas solicitudes de spam a un servicio, el atacante puede provocar desbordamientos en la red y ocasionar que el servicio no esté disponible para los usuarios legítimos.

- **Ataques ransom DoS:** en un Ataque RDoS, el atacante exige un rescate para no realizar el ataque contra una organización o para detenerlo cuando está en curso.

Los ataques de denegación de servicio buscan perjudicar a las organizaciones y dañar sus recursos, ya sea por motivos ideológicos o con el objetivo de obtener beneficios económicos. Actualmente, han pasado a ser una herramienta arsenal de los delincuentes cibernéticos, cuyas consecuencias pueden ser muy variadas.

Ataques MitM

Los ataques Man-in-the-Middle (MiTM) se centran en interceptar comunicaciones. Según el sitio web de *Check Point* (2024), algunas amenazas de MitM son las siguientes:

- **Ataque de hombre en el medio (MiTM):** es un ataque en el cual, el atacante intercepta el tráfico entre su origen y destino. Si el tráfico no está protegido mediante cifrado y firmas digitales, el atacante podría leer y modificar el tráfico interceptado.
- **Ataque de hombre en el navegador (MiTB):** en este el atacante aprovecha la vulnerabilidad del navegador de un usuario para implantar un código malicioso en el navegador. Esto permite que el atacante lea o modifique los datos, antes de que el usuario los visualice o los envíe al servidor.

La evolución digital y un mundo cada vez más interconectado conlleva una serie de beneficios, pero al mismo tiempo aumenta la complejidad de la ciberdelincuencia y la explotación de las vulnerabilidades de seguridad. Ante este panorama, es crucial estar al tanto de las mejores técnicas de ciberseguridad para protegerse contra los ataques MITM y otros ciberdelincuentes. Además, tener un software antivirus potente para proteger los datos y mantenerse seguros.

Recomendaciones para evitar ser víctimas de los ciberdelincuentes

Como se detalló anteriormente en el entorno digital existen una serie de amenazas, estás tienen como único fin dañar a los usuarios y cada día evolucionan a una velocidad impresionante, es por esto, por lo que, resulta fundamental conocer las medidas preventivas que se pueden ejecutar para no ser víctimas de la ciberdelincuencia y así, ser ciudadanos digitales informados y responsables.

Las contraseñas son de los eslabones más débiles en temas de ciberseguridad, se suelen elegir contraseñas cortas, fáciles de adivinar y que no cumplen con recomendaciones necesarias en temas de seguridad, como se menciona en el artículo titulado: “Las 15 mejores reglas de seguridad y qué no hacer en línea” de la empresa Kaspersky, líderes en temas de seguridad cibernética indican que las contraseñas deben tener una longitud de al menos 12 caracteres, con una combinación de caracteres, entre letras mayúsculas y minúsculas, además de símbolos y números. También, señalan que no se deben usar secuencias de números (“1234”) o información personal que alguien conozca, como la fecha de nacimiento o el nombre de una mascota.

También es recomendable el uso de administradores de contraseñas, con el fin de tener un lugar seguro en donde almacenar estas. Otro mecanismo de protección es el habilitar la autenticación multifactor (MFA), el cual es un método que solicita a los usuarios que proporcionen dos o más métodos de verificación para acceder a una cuenta en línea, esta alternativa disminuye la probabilidad de que pueda producirse un ciberataque. Por lo que, es una buena práctica usar contraseñas o códigos de acceso, pero también existen alternativas complementarias, como el uso de lectores de huellas digitales o tecnología de escaneo facial en la mayoría de los dispositivos.

Es muy importante mantener el software de los dispositivos actualizado, pues tanto los sistemas operativos como las aplicaciones realizan de manera periódica, actualizaciones o cambios de versión, con el fin de mitigar las amenazas y reducir las vulnerabilidades en los sistemas. Otro mecanismo fundamental es el uso de software de seguridad o antivirus para proteger los dispositivos y datos, bloqueando las amenazas más comunes, como los virus y el malware. Continuando sobre la línea de los dispositivos, es fundamental hacer copias de seguridad de la información personal importante, en discos duros externos o en la nube y crear nuevas copias de seguridad con regularidad.

Los ataques de malware o estafas por medio de *phishing* son de los más comunes y están asociados a acciones que realizan los usuarios por descuido, como se detalla en el artículo de la empresa Kaspersky (2024) donde se rescata que: “es esencial navegar de forma consciente y evitar ciertos tipos de contenido en línea, como los vínculos de fuentes no confiables y los correos electrónicos spam, los cuestionarios en línea, el ciberanzuelo, las ofertas “gratuitas” o los anuncios no solicitados” (párr. 15).

Es necesario pensar bien antes de visitar un nuevo sitio web o descargar cualquier archivo que no sea de fuentes confiables u oficiales, también comprobar las carpetas de descargas con regularidad y verificar si existen archivos desconocidos en el sistema.

Un portillo muy amplio para los ataques cibernéticos radica en los descuidos al navegar en internet, por esto es necesario asegurarse de que los sitios web que se visitan sean confiables, comprobando que las URL deben comenzar con “https” en lugar de “http” (la “s” significa “seguro”), además que tengan el ícono de candado en la barra de direcciones y validar que no contengan errores ortográficos o gramaticales.

Adicionalmente, es recomendable revisar la configuración de las políticas de privacidad de los sitios web y de las aplicaciones, con el fin de entender qué información del usuario será recopilada.

Situación actual de Costa Rica en ciberseguridad

El panorama en ciberseguridad de Costa Rica refleja una gran cantidad de desafíos y progresos en la protección de la información sensible y la infraestructura tecnológica del país, en los últimos años ha estado marcado por una serie de amenazas cibernéticas, por lo que, es importante recordar los eventos del año 2022, en los cuales la seguridad nacional se vio vulnerada por una serie de ataques a las principales organizaciones del estado.

El laboratorio de análisis e inteligencia de amenazas de Fortinet (FortiGuard Labs), desarrolló el *Informe global sobre el panorama de amenazas de 2H de 2023*, este reveló unas cifras que muestran la razón por la cual el país debe avanzar de una manera más acelerada en temas de abordaje y prevención en ciberseguridad, pues se detalla que Costa Rica sufrió 882 millones de intentos de ciberataques en el año 2023. Además, parte del análisis aloja una presencia destacada de amenazas a aplicaciones vinculadas a Microsoft Office. Entre los sectores más apetecidos por los cibercriminales están la Banca y Finanzas, seguido por el Gobierno.

Costa Rica cuenta con una serie de leyes y regulaciones relacionadas con la ciberseguridad; sin embargo, el proyecto de Ley de Ciberseguridad (expediente 23.292) únicamente ha sido dictaminado, sin fecha de trámite legislativo para su aprobación y preocupaciones, ya que cuenta con muchas falencias, como lo indica Masís (2024), fundadora de Tech Secure AI, quien fungió como asesora de la Comisión de Ciencia y Tecnología de este poder de la República.

El proyecto tiene falencias y queda pequeño. La forma en la que las medidas están estructuradas actualmente, pensando en una Dirección Nacional de Ciberseguridad, se quedan cortas ante realidades como las que está enfrentando el país con situaciones, por ejemplo, como las amenazas de ciberseguridad a nivel mundial y el decreto de 5G. Con lo pequeño que se está quedando el proyecto de ley y con lo lento que el asunto se está moviendo ante una tecnología que se mueve a años luz, esa Dirección ya debería tener definidos temas claves como estructura y organigrama para ir avanzando y lamentablemente, no se ha logrado.

Se pueden considerar otras leyes que tienen alguna relación como la Ley de Delitos Informáticos y Conexos (Ley N°9048), que penaliza delitos como el acceso no autorizado, la interceptación ilegal de datos y la difusión de virus informáticos; la Ley sobre la protección de la persona frente al tratamiento de sus datos personales (Ley N°8968), que establece bases y principios para garantizar el derecho que tiene toda persona a la protección de sus datos personales.

También es importante mencionar el Convenio sobre la Ciberdelincuencia, Budapest (2017) (Ley N°9452) donde su objetivo general es la "Prevención y acción en los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, por medio de la tipificación de esos hechos" (art. 7-9).

Por otra parte, es vital citar la Ley de Protección de la Niñez y la Adolescencia frente al contenido nocivo de Internet y otros medios electrónicos (Asamblea Legislativa de Costa Rica, 2011) (Ley N°8934), el propósito de esta ley es salvaguardar a los menores de contenido inapropiado en entornos electrónicos y regular la protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos. Está ley es aplicable a lugares de acceso público con computadoras conectadas a Internet utilizadas por menores de edad, además la ley reglamenta la administración de estas computadoras, incluyendo navegadores y servicios de comunicación en red.

Por otro lado, establece medidas, como programas de bloqueo, para prevenir el acceso a sitios y comunicaciones que puedan ser perjudiciales para la niñez y la adolescencia. Ley de protección de la imagen, la voz y los datos personales de las personas menores de edad (Ley N°10238), la cual establece que se impondrá de diez a sesenta días de multa a quien difunda, divulgue o utilice imágenes, la voz o los datos personales de una persona menor de edad, de

cualquier modo que se haga y que permita la identificación de la persona menor de edad, sin el consentimiento expreso de las personas responsables legales.

Como parte del crecimiento exponencial en aspectos digitales no se puede dejar de lado la firma digital, que permite firmar los documentos digitales y que tengan la misma validez legal que los documentos firmados a mano, facilitando trámites en línea como contratos, solicitudes o pagos de servicios sin necesidad de imprimir papeles.

Ante esto, en el país existe la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Ley N°8454), que respalda esta práctica. Además, existen otros esfuerzos en curso para fortalecer la legislación y promover la protección de datos personales; sin embargo, los esfuerzos llevan años sin mayor avance.

Plan Nacional de Ciberseguridad

Como parte de los esfuerzos que se están realizando a nivel país para proporcionar un ecosistema digital confiable que contribuya al esfuerzo global por mitigar y prevenir riesgos de amenazas en el ciberespacio, se estableció la nueva Estrategia Nacional de Ciberseguridad 2023-2027, como lo indica la ministra Paula Bogantes del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT, 2024) al señalar que:

> Costa Rica ha experimentado un aumento significativo en los ciberataques los cuales han tenido un impacto en la economía digital y la seguridad nacional. Como respuesta a estas amenazas en constante evolución, el Gobierno de la República ha optado por replantear su enfoque de atención por medio de una Estrategia Nacional de Ciberseguridad robusta y efectiva (p. 3).

A nivel normativo, la estrategia se encuentra respaldada por una serie de leyes, regulaciones, decretos y convenios, algunos mencionados anteriormente, que establecen un marco legal y regulatorio, para desarrollar una legislación integral en materia de ciberseguridad y promover un entorno cibernético seguro y confiable.

Adicionalmente, como parte del marco normativo se otorga al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) la rectoría en temas de ciencia, tecnología, telecomunicaciones y gobernanza digital en el país, se establecen normas técnicas y se crean varias instancias que abordan temas relacionados como el Consejo Interinstitucional sobre

Terrorismo (CISTE), la Comisión Nacional de Seguridad en Línea (CNSL) y el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) bajo el MICITT. Por lo que, como se menciona en la Estrategia Nacional de Ciberseguridad (MICIIT, 2023-2027):

> El objetivo general de la estrategia es desarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC´s para lograr un entorno más seguro y confiable para todos los habitantes del país (p. 19).

La estrategia está alineada estratégicamente con varios instrumentos de política pública y de planificación nacional. Conforme a lo establecido en la Estrategia Nacional de Ciberseguridad (MICIIT, 2023-2027):

> Por una parte, con el marco estratégico relacionado con los sectores de ciencia, innovación, tecnología y telecomunicaciones que hace énfasis en el desarrollo de la sociedad y economía costarricense. Por otra parte, con el marco estratégico que promueve el cese de toda desigualdad y la integración de una perspectiva de género en el quehacer de las instituciones públicas para la construcción de una sociedad incluyente en todos los ámbitos de la vida costarricense (p. 25).

Por otro lado, la estrategia está fundamentada en cuatro enfoques estratégicos nacionales que se mencionan a continuación, a saber: enfoque en toda la sociedad, en la gestión y mitigación de riesgos, en los derechos humanos y centrado en el ser humano, estos ayudan a guiar la toma de decisiones. Seguidamente, es sumamente importante referirse a los pilares sobre los cuales está estructurado dicho plan y que ayudan a orientar y guiar las líneas de acción y están constituidos de la siguiente manera: reforzar la gobernanza de ciberseguridad, adecuar el marco jurídico cibernético, fortalecer la protección de infraestructuras y la ciber resiliencia nacional, reforzar las capacidades del ecosistema de ciberseguridad y cooperar en el entorno digital.

En el año 2022, Costa Rica se vio expuesta a una serie de amenazas cibernéticas que mostraron el estado real de la instituciones del estado en ese campo y sus vulnerabilidades, esto significó un antes y un después y obligó a tomar acciones urgentes para mitigar el riesgo, aún más en una era que está en constante cambio y con un entorno digital que evoluciona a pasos agigantados, por lo tanto, es necesario comprometerse como nación desde la ciudadanía, como una

población educada e informada, reforzando la gobernanza en ciberseguridad nacional y garantizando una economía segura y estable.

La ciberseguridad y el impacto en los jóvenes

La tecnología es una herramienta poderosa de desarrollo para las sociedades y sus habitantes y es así como la digitalización y el desarrollo digital han venido a cerrar las brechas educacionales e informativas en los jóvenes; si bien es cierto, no es un aspecto que se deba ni quiera frenar, pues cada vez más la seguridad representa un reto en los jóvenes, ante esto, se les debe dar las bases para fomentar el uso y aprovechamiento amplio del avance tecnológico, pero de la mano y del acompañamiento necesario para que desarrollen el pensamiento crítico que les permita discernir en el océano de amenazas en las que se enfrentan en el ciberespacio.

Según datos del Fondo de las Naciones Unidas para la Infancia (UNICEF):

> un 79 % de los jóvenes de entre 15 y 24 años tenían conexión a internet en 2023, en comparación con el 65 % del resto de la población mundial, lo que denota, sin duda que, la juventud es la mayor impulsora de la conectividad a nivel mundial (párr. 1).

Por esto, es labor de los gobiernos, dotar de herramientas y protección a su población más joven, garantizar el cumplimiento de los marcos legales dictados para la seguridad en línea y realizar alianzas mundiales que les permitan estar a la vanguardia de los principales programas e iniciativas internacionales en torno a la ciberseguridad.

Alianzas como la iniciativa de Protección Infantil en Línea (COP, por sus siglas en inglés) de la Unión Internacional de Telecomunicaciones y de la cual Costa Rica es miembro, por medio del MICITT; desarrolla recomendaciones y orientación para apoyar a los estados miembros, en sus esfuerzos por crear un entorno en línea seguro para niños y jóvenes.

De la misma manera, las leyes como la 8968, 8934 y la 10238 vienen a delimitar el marco legal de protección de los jóvenes en el mundo digital y a velar por los derechos de esta población vulnerable.

Importancia de la educación en ciberseguridad en edades tempranas

El mundo digital está en constante desarrollo y expansión, generando cada vez más nuevas plataformas de interacción y avances tecnológicos que impulsan a las personas de todas las edades

a migrar a la digitalización, por esta razón, resulta urgente educar no solo sobre cómo utilizar y sacar provecho a estas ventajas tecnológicas, sino sobre los riesgos y vulnerabilidades a las que se está expuestos.

Dicha educación y concientización debe nacer cada vez entre niños y adolescentes, debido al acceso que los jóvenes tienen cada vez más a dispositivos electrónicos, así también como los señala Irvin Sáenz, instructor en Academia de Tecnología UCR, la educación temprana en ciberseguridad cobra relevancia actualmente, debido al incremento en ataques cibernéticos en los últimos años, así como a los constantes avances en Inteligencia Artificial, Big Data y otras tecnologías afines que han venido tomando mayor trascendencia.

Con este auge tecnológico, es necesario estimular el desarrollo crítico y analítico en los adolescentes, pues este les permitirá evitar ser presas fáciles de los ciber depredadores, así como detectar actividades inusuales que pueden poner en riesgo su seguridad. De la mano con este aspecto, el pensamiento crítico les permite identificar y romper con las conductas riesgosas que pueden tener en el ciberespacio, como lo son el manejo seguro de contraseñas o determinar la información prudente para compartir en las redes sociales.

Peligro al que se enfrentan los jóvenes en el ciberespacio en la actualidad

En la actualidad, los jóvenes se enfrentan a una serie de riesgos y amenazas, internet puede ser un entorno muy nocivo y peligroso para este segmento de la población que se considera vulnerable, según el informe de Seguridad Online de Microsoft (2024), el 74 % de los adolescentes encuestados afirma haber experimentado algún riesgo en internet y el 39 % de los adolescentes declaró haber sido víctima de incitación al odio en internet; posterior a experimentar una situación de riesgo en internet, el 60 % de los adolescentes habló con alguien al respecto; el 71 % lo hizo con sus padres; el 32 % con amigos y el 14 % con otro adulto que no eran sus padres.

Entre los riesgos más comunes, destacan la información errónea (*fake news*) y la desinformación, así como el ciberacoso, abusos, discurso de odio, amenazas de violencia, la exposición a contenidos sobre suicidio y autolesiones. Por lo que, las nuevas generaciones están expuestas a nuevos desafíos a medida que comienzan a explorar internet, entre las amenazas más comunes que afrontan las adolescentes se encuentran las siguientes:

Ciberbullying / Ciberacoso

Consiste en una forma de hostigamiento, agresión o acoso que se realiza por medios digitales, puede darse en diferentes aplicaciones, videojuegos, redes sociales, blogs y algunas otras plataformas y tiene un impacto irreversible a nivel emocional en algunos de los adolescentes, puede causar depresión, estrés, ansiedad, baja autoestima, así como aislamiento social.

Según cifras de la Organización de las Naciones Unidas (ONU) y la Fundación Telefónica, el 55 % de los jóvenes latinoamericanos ha sido víctima de ciberacoso. Como se detalla en el sitio web de Mcafee (2024), en el artículo *Ciberacoso: causas, riesgos y cómo evitarlo*, se detallan los diferentes tipos de ciberacoso que se mencionan a continuación, a saber:

- **Acoso en línea:** involucra la repetición de comportamientos maliciosos para causar daño emocional a la víctima. Ejemplos de este comportamiento son comentarios ofensivos, amenazas e intimidaciones.
- **Doxxing:** es cuando se publica información personal o confidencial sobre una persona sin su consentimiento, con la intención de causar daño, vergüenza o miedo.
- **Exclusión en línea:** este tipo de ciberacoso ocurre cuando una persona es deliberadamente excluida de un grupo en línea.
- **Cyberstalking:** se refiere a la persecución en línea, a menudo acompañada de amenazas a la seguridad personal de la víctima.

Según la II Encuesta Kids Online (2023), desarrollada por el Instituto de Investigaciones Psicológicas y la Fundación Paniamor, un 40 % de los jóvenes aseguró haberlo recibido por parte de una amiga/o y el 34,3 % de algún desconocido. Las aplicaciones y plataformas en las cuales se da más el ciber acoso son: mensajes de texto, audio y WhatsApp (61,6 %); seguido de los mensajes personales de Instagram (19,2 %) y en los juegos por Internet (17,2 %).

Ante este panorama, resulta importante saber qué acciones tomar en caso de ser víctima de este tipo de riesgo, como se menciona en el artículo *¿Qué hacer cuando tu hijo(a) adolescente sufre de acoso online?*, de la empresa Meta, donde se indica que es necesario establecer estrategias de control y ejecución, donde no deben pasar por alto este tipo de situaciones y siempre se debe acusar al acosador, para esto es fundamental recopilar toda la información que se pueda sobre lo sucedido y reconocer quiénes estuvieron involucrados, por lo que, en caso de que las acciones se realicen desde un centro educativo, es importante realizar la denuncia en el área respectiva y

adicionalmente, si el acoso se está realizando desde alguna aplicación o sitio web, se debe reportar y de inmediato, bloquear al que está cometiendo dicho acto.

Finalmente, tanto los padres y madres de familia como los docentes de los centros educativos son un punto importante de contacto y de control para prevenir y ejecutar medidas, esto va desde enseñarles en qué consiste este riesgo, cómo evitar ser víctimas o perpetradores, así como escucharlos y establecer un espacio seguro en el cual, ellos puedan expresarse y brindarles herramientas en caso de pasar por esto y de esa manera, saber cómo enfrentarlo y buscar ayuda.

Grooming

Según se menciona en el artículo Grooming, del Instituto Nacional de Ciberseguridad de España:

> es una práctica en la que un adulto se hace pasar por un menor en Internet o intenta establecer un contacto con niños y adolescentes que dé pie a una relación de confianza, pasando después al control emocional y, finalmente al chantaje con fines sexuales (párr. 1). Son estrategias con el objetivo de explotar o acosar sexualmente a los menores. Es implementado por los llamados "groomers", quienes pueden buscar introducir al menor en ambientes de prostitución y explotación sexual.

Según se detalla en un artículo de Delfino (2023), en su sitio web, en la Unidad de Análisis Criminal del Organismo de Investigación Judicial (OIJ), entre el 2017 y septiembre del 2023, se han recibieron 426 denuncias por grooming o seducción de menores por medios electrónicos, identificando a 486 víctimas (412 mujeres, 66 hombres y 9 de género no definido). De ellas, 309 tienen entre 12 y 17 años, 87 son menores de 12 años y 91 no tienen registro de edad. Sin embargo, este número podría subestimar la realidad, ya que muchas víctimas no denuncian por temor, vergüenza o falta de conocimiento sobre el tema.

Como medida ante este tipo de amenaza que enfrentan los jóvenes, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) anunció el pasado 23 de noviembre de 2023, el lanzamiento de la Guía contra el Grooming como una iniciativa y parte de la ejecución de la Estrategia Nacional de prevención y respuesta a la explotación y abuso sexual de niñas, niños y adolescentes en línea 2023-2027.

En el artículo anterior, se detallan algunas alternativas para prevenir este tipo de riesgo en línea, como por ejemplo, establecer hábitos de navegación, en cuestión de horarios de uso y sitios que visitan, también es importante que los jóvenes comprendan la relevancia de no hablar ni aceptar a desconocidos y no brindar información personal.

Además, es vital que reflexionen sobre el uso de la cámara en sus dispositivos y del envío de fotos o videollamadas. Este acompañamiento debe ir ligado a fomentar un ambiente en dónde los jóvenes se sientan cómodos y seguros compartiendo sus experiencias en línea y que sientan que no serán juzgados si no apoyados.

Sexting

Como lo indica el sitio web HealthyChildren.org (2022), en el artículo *Sexteo: cómo hablar con sus hijos del riego de enviar mensajes con contenido sexual*: “es el envío o recepción de imágenes, videos o mensajes de texto sexualmente explícitos a través de un teléfono inteligente, computadora, tableta, videojuego o cámara digital” (párr. 1). También puede considerarse como una forma de acoso sexual en la que una niña, niño o adolescente puede ser presionado a enviar una foto a su pareja, quien después la distribuye sin su consentimiento.

Esto puede traer una serie de riesgos asociados como ciberbullying, grooming, sextorsión o chantaje a menores de edad, mediante mensajes intimidatorios que amenazan con difundir imágenes o videos sexuales generados por las propias víctimas, donde la intención de los extorsionadores es continuar con la explotación sexual y/o mantener relaciones sexuales, lo que puede provocar un daño en la reputación de la víctima y el ir deteriorando su imagen pública.

Esta práctica es muy frecuente en los jóvenes, es dónde radica la importancia que tienen los padres y formadores en la prevención de estas prácticas, en un entorno digital en el cual es casi imposible controlar, como se menciona en el artículo Sexting, del Instituto Nacional de Ciberseguridad de España, donde se destaca que es necesario hacerlos partícipes de las implicaciones y riesgos de proteger la privacidad, además es necesario crear conciencia del peligro de esta práctica, para que aprendan a saber decir no y darles herramientas para no ceder ante la presión social, promoviendo una autoestima saludable y a conocer su valor, sin depender de la opinión de los demás.

Fake News

Según el artículo *¿Cómo identificar noticias falsas?* del sitio web de Kaspersky (2024), el término "noticias falsas": "se refiere a la información falsa o engañosa que se disfraza de noticia legítima" (párr.1). La desinformación puede propagarse ampliamente a través de las redes sociales y las interacciones de la vida real e incluso, puede llegar a los medios de comunicación respetados. Las noticias falsas se propagan con rapidez, debido a que normalmente están diseñadas para llamar la atención y apelar a las emociones, es por ello, por lo que, generalmente presentan afirmaciones o historias excéntricas que provocan enojo o temor.

Por lo que, antes de compartir o leer algún artículo o noticia en internet es necesario verificar la fuente, comprobando que proviene de un medio confiable y de buena reputación, incluso si es escrito por un autor reconocido; además comprobar los hechos, como por ejemplo, si es de fechas recientes, si los datos o estadísticas concuerdan con otros contenidos similares o si por el contrario, no existen otros sitios con la misma información. También, es vital desarrollar la capacidad de tener un pensamiento crítico que ayude a la población en general a discriminar todo el contenido que se está en línea y ser factores de cambio para evitar la desinformación.

Publicación de información privada

La información que se publica puede tener una gran repercusión y difusión. Los jóvenes pueden verse expuestos al publicar información personal en línea, por ejemplo, en sus perfiles de redes sociales, que no debe exponerse al público. Esta información puede incluir desde fotos de momentos personales incómodos hasta la dirección de su domicilio. Por ello, es necesario que comprendan la importancia de mantener altos niveles de privacidad y controlar la información que se transmite y a quién se transmite.

El saber cómo prevenir este tipo de riesgo es vital, ya que lo que se sube a internet jamás se borra, aunque hagan creer que si, como lo menciona INCIBE en su artículo *Privacidad* señalando que: "la prevención siempre comienza fomentando una comunicación sana con los menores y haciéndoles partícipes de los riesgos a los que se enfrentan al administrar su información personal en Internet" (párr.12). Para ello, es fundamental aprender a diferenciar qué tipo de contenidos pueden ser públicos y cuáles se deben mantener en privado.

Por lo tanto, conocer y utilizar las opciones de privacidad y seguridad de las redes sociales es un mecanismo de defensa que permite estar protegido ante este tipo de riesgo. Además, es fundamental fomentar un pensamiento crítico, el cual no solo consiste en pensar en la propia privacidad, sino también en la de los demás, puesto que, a la hora de compartir información de otras personas, es necesario pedir permiso y guardar su intimidad.

Riesgos silenciosos en el mundo digital

Los jóvenes se enfrentan a otros riesgos que actúan de manera silenciosa, aunque no se les evalúa de la misma forma, pueden afectar el desarrollo de los jóvenes, como lo es la pérdida de tiempo, pues actualmente los menores de edad consumen gran parte de su día en dispositivos electrónicos, lo que provoca que muchos de ellos pierdan el enfoque en sus estudios, familia y otras actividades relevantes. La exposición a contenidos nocivos es un tipo de amenaza a la cual se exponen las niñas, niños y adolescentes, de forma intencionada o accidental, además a contenido violento, de índole sexual o generador de odio.

Otro riesgo silencioso es la distorsión de la realidad, las redes sociales se han encargado de mostrarnos una realidad irreal, son comentadas por los influencers que en ocasiones promueven una realidad alterada y muchos jóvenes en su afán de parecerse a ellos, adquieren comportamientos inadecuados, basados en comparaciones sociales y en una percepción distorsionada de la propia imagen.

Finalmente, no hay que dejar de lado uno de los principales enemigos de los jóvenes en actualidad, como lo son las adicciones a las redes sociales, donde el uso abusivo de las redes sociales puede causar daños como trastornos en el sueño, sedentarismo, aislamiento e incluso, irritabilidad o cambios en la conducta, este punto se desarrollará de forma más detallada en la próxima sección.

Papel de las redes sociales y las plataformas digitales en los adolescentes

Las Redes Sociales forman parte de la vida cotidiana y representan en muchos casos una extensión del mundo físico al digital, durante la etapa de la adolescencia las redes toman un papel protagónico en la forma en la que los jóvenes se relacionan con sus pares y con el mundo exterior;

por lo que, utilizan sus perfiles y publicaciones como una forma de expresión, crítica, denuncia ante problemáticas y causas sociales que los mueven, así como la manifestación de sus hobbies y de su estilo de vida. El acompañamiento por parte de los educadores y padres de familia o cuidadores es vital para prevenir o accionar sobre posibles amenazas o conductas de riesgo en los que pueden estar inmersos.

Tal y como lo indica el sitio web FasterCapital (2024) en el artículo *Ciberseguridad educativa proteger a los emprendedores del mañana* una guía para la ciberseguridad en la educación, donde se señala qu la enseñanza no se trata sólo de adquirir conocimientos y habilidades, sino también de desarrollar valores y éticas que guíen el comportamiento y las decisiones de los individuos y grupos en el mundo digital.

Es aquí donde la ciberseguridad juega un papel importante, pues apoya y concientiza sobre el cumplimiento de valores como respeto, responsabilidad, honestidad y equidad, que vienen a ser vulnerados en plataformas digitales como las redes sociales y que es vital que como sociedad se formen ciudadanos digitales informados y responsables, con el amplio conocimiento de las consecuencias que pueden generar tener ciertas conductas en el ciberespacio.

Por esto, los jóvenes deben de entender las implicaciones que pueden tener en el mundo real sus prácticas y actividades, es aquí donde se vuelve protagonista el ciberacoso. Según el estudio *Ciberacosadores: un estudio cuantitativo con estudiantes de secundaria* (2018), de los 950 estudiantes encuestados en edades entre los 11 y 18 años, un 6.4 % se pueden considerar ciberacosadores, aunque un 23.3 % ha realizado alguna de las conductas propias de los ciberacosadores (mensajes o llamadas ofensivas o amenazantes, difundido fotos o videos de alguna persona sin su autorización, difamación, entre otros). Esto muestra la importancia que genera una educación y concientización amplia de cómo conductas que parecen inofensivas o que se han normalizado, pueden afectar seriamente al otro y traer consecuencias mayores no solo a la vida del acosado, sino también del acosador.

Las Redes Sociales y el uso excesivo en una etapa tan crucial como la adolescencia, están provocando ansiedad y disminución de la autoestima. Según como lo indica Child Mind Institute en su artículo *¿Cómo afecta el uso de las redes sociales a los adolescentes?*, en una encuesta llevada a cabo por la Royal Society of Public Health (2023), se preguntó a jóvenes entre 14 y 24 años en Gran Bretaña, de qué manera las plataformas de las redes sociales tenían un impacto en su

salud y bienestar, los resultados de la encuesta encontraron que Snapchat, Facebook, Twitter e Instagram aumentaban los sentimientos de depresión, ansiedad, mala imagen corporal y soledad.

Si a todo lo anterior se le suma la posibilidad de sufrir de ciberacoso, grooming o alguna otra amenaza cibernética, se destaca que la intervención por parte de los adultos que los rodean como los padres de familia y profesores, es vital pues estas manifestaciones pueden llegar a tener consecuencias que incluso, pueden poner en riesgo la vida de los adolescentes, por caer en desórdenes alimenticios por la alta expectativa en torno a su imagen corporal, sufrir de rechazo y discriminación por publicaciones o comentarios xenofóbicos, así como llegar a sufrir de ciberbullying desproporcionado y ocasionar daños irreversibles como atentar con su vida o el suicidio.

En un estudio realizado en España sobre el *Acoso escolar y ciberacoso en la infancia y la adolescencia* (2023), se arrojan datos alarmantes en los cuales, el porcentaje de quienes reconocen haberse hecho daño físico intencionadamente por consecuencias del ciberacoso, es del 28,5 % en las víctimas y del 27,8 % en los acosadores. Por lo que, el hecho de vivir ciberacoso, como víctima o como acosador se asocia a un riesgo considerablemente mayor de conductas autolesivas, sin diferencias significativas entre víctimas y acosadores.

Ante esta problemática, es crucial que los padres y los adolescentes estén conscientes de las ventajas y desventajas de las redes sociales y trabajen juntos para maximizar lo positivo y minimizar los peligros. Los padres pueden ayudar a sus hijos a identificar y controlar el acoso en línea, establecer límites saludables en su uso de las redes sociales y educarlos en cómo usarlas de manera segura y responsable.

La educación en ciberseguridad en edades tempranas a nivel mundial

La seguridad cibernética en la educación es fundamental para resguardar a los jóvenes en un entorno digital siempre cambiante. Es necesario abordar las amenazas, instruir a los adolescentes y preparar a los educadores para crear un entorno digital seguro para la totalidad de las personas. En un mundo donde la tecnología está presente en todas partes y la inteligencia artificial avanza rápidamente, es crucial pensar en la relevancia de la ciberseguridad en la enseñanza formal de niños y adolescentes.

Hoy en día, las nuevas generaciones son apodados como “nativos digitales” y se encuentran expuestos a dispositivos electrónicos y plataformas en línea desde edades tempranas. A pesar de que su relación con la tecnología es natural, quizá no comprenden el impacto o las implicaciones del uso inadecuado y es de suma importancia que adquirieran conciencia y que lleguen a ser ciudadanos digitales responsables y empoderados.

A nivel mundial se han establecido una serie de programas para educar a la población en temas de ciberseguridad en edades tempranas, como se menciona en el documento *Educación en Ciberseguridad - Planificación del futuro mediante el desarrollo de la fuerza laboral* (2020), publicado por la Organización de Estados Americanos (OAS):

> En América Latina, los gobiernos de Argentina, Brasil, Chile, Colombia, Costa Rica, Guatemala, México, Panamá, Paraguay y República Dominicana han publicado o actualizado sus estrategias nacionales de ciberseguridad. Estas estrategias abarcan un marco de creación de capacidades y líneas de acción para fortalecer la educación en ciberseguridad (p. 12).

En el mismo documento se señala cómo dichas estrategias fundamentan algunos de sus objetivos en temas de educación, como lo es el caso de la estrategia nacional de Argentina que se centra en la concienciación y la educación en ciberseguridad y cuatro de los siete objetivos de la Política Nacional de Seguridad de la Información de Brasil se relacionan con la investigación y desarrollo. Asimismo, los marcos nacionales de ciberseguridad de Chile y Colombia abarcan la educación como una característica clave para mejorar la madurez de la ciberseguridad e identifican acciones específicas.

Si bien es cierto, en América Latina se están haciendo esfuerzos para reforzar la educación en ciberseguridad, pero aún falta mucho terreno por recorrer, hay otras potencias que han avanzado de manera más acelerada en estos tópicos, como lo es el caso de países como Israel, que han desarrollado una serie de programas en formación desde la niñez, en su intento por ser líder mundial en tecnología y seguridad digital; otra nación que está ejecutando una serie de iniciativas para este segmento de la población son los Estados Unidos, con el fin de formar jóvenes que puedan encarar los desafíos actuales y futuros en materia de ciberseguridad.

Por otra parte, en Europa hay naciones que están integrando la educación cibernética, por medio de cursos básicos en ciberseguridad en los planes de estudios escolares y ejecutando campañas de sensibilización sobre la desinformación, con el fin de integrar la alfabetización digital

en las aulas y mejorar el aprendizaje a través de diferentes programas educativos. A continuación, se mencionan algunos programas de los países líderes en esta materia y se destaca lo que se está implementando en Costa Rica en tópicos cibernéticos.

Israel, un ejemplo en programas de formación en ciberseguridad

En cuanto a lo que están haciendo las potencias en esta materia se debe nombrar de primera mano a Israel, que ha venido desarrollando una serie de planes educativos en edades tempranas, mucho de esto como respuesta a las diferencias sociopolíticas con los diferentes países del medio oriente, con el fin de estar protegidos a nivel de inteligencia militar y preparar a los jóvenes en posibles carreras de defensa.

El programa insignia de educación en este campo es Magshimim, lanzado en el año 2010 por la Fundación Rashi, una organización filantrópica centrada en apoyar a los jóvenes israelíes desfavorecidos y que ha sido copatrocinado por el Ministerio de Defensa israelí desde el año 2013, que como lo detallan en su sitio web: "tiene como objetivo, impulsar el cambio social creando oportunidades para que los jóvenes de la periferia sobresalgan en la ciber tecnología" (párr.1). Este programa fue reconocido como un programa nacional de educación cibernética, luego de un exitoso programa piloto de dos años.

Este programa se desarrolla durante tres años para estudiantes de secundaria de 10º, 11º y 12º y se centra en la enseñanza de materias tecnológicas de alto nivel junto con habilidades de autoaprendizaje y trabajo en equipo, a lo largo de tres años, donde trabajan en proyectos de programación, implementan protocolos criptográficos, realizan ingeniería inversa de malware y estudian la arquitectura y el diseño de redes informáticas.

Como se menciona en el sitio web de la Fundación Rashi (2024):

> el conocimiento y las herramientas que adquieren mejoran sus posibilidades de unirse a las unidades tecnológicas de élite de las FDI y de continuar una carrera en alta tecnología. De esta manera, el programa aborda la creciente demanda de expertos en ciberseguridad y al mismo tiempo sirve como un verdadero trampolín hacia la movilidad social (párr. 1).

Los estudiantes de este programa están siendo preparados para ingresar a las ramas cibernéticas de élite de las Fuerzas de Defensa de Israel durante su servicio militar obligatorio. En

particular, los adolescentes de Magshimim que esperan unirse a la Unidad 8200, el equipo de inteligencia y ciberseguridad.

Otro de los programas ofrecidos por dicha fundación es Mamriot que busca brindar oportunidades para que las mujeres jóvenes desarrollen sus talentos en estos campos, cerrando la brecha de género en la alta tecnología, promoviendo la movilidad social en Israel e impulsando el crecimiento de la economía. Está dirigido a niñas de secundaria y es desarrollado por el Centro de Educación Cibernética en colaboración con el Cuerpo de Inteligencia de las Fuerzas de Defensas de Israel (FDI).

Uno de los objetivos principales es educar a los jóvenes, para que puedan ser escudos humanos y posteriormente, sirvn a la nación, para esto es necesario que se promuevan planes de alfabetización desde el inicio de los años de secundaria; el programa StarTech para estudiantes de 7º, 8º, 9º fue desarrollado por el Cyber Education Center y se destaca que:

> este programa ofrece a los participantes muchas oportunidades para expresar sus habilidades e ideas. Adquieren herramientas prácticas en diversos campos: escribir código en diferentes lenguajes de programación, crear juegos de computadora, gráficos por computadora y aplicaciones móviles, y otras tecnologías actualizadas (párr. 1).

Si bien es cierto estos programas no son impartidos por entidades del gobierno, muchos de ellos son copatrocinados por estas, ya que son los principales interesados en la formación de los jóvenes, fomentando una serie de habilidades cibernéticas y preparando a los jóvenes en carreras de alta demanda.

Reino Unido, líder en ciberseguridad en Europa

El Reino Unido es uno de los países líderes en términos de ciberseguridad, posee ecosistemas tecnológicos muy desarrollados. El sector es prioritario para el Reino Unido y por ello, el Gobierno británico lanzó en febrero del año 2022 su nueva Estrategia Nacional de Ciberseguridad. En la estrategia se desarrollan las acciones y se fijan objetivos para reforzar las distintas áreas gubernamentales y empresariales, apalancándose en la educación de edades tempranas, con el fin de crear una reserva de talento que responda a la necesidad de capacidades actuales y futuras.

En el año 2017 se creó el Centro Nacional de Ciberseguridad del Reino Unido (NCSC), con el fin de convertirse en la autoridad nacional en el ámbito de la ciberseguridad y como parte de sus principales responsabilidades, se establece el desarrollo de la educación, como se menciona en la Estrategia Nacional de Ciberseguridad (2022) con la intención de: "promover el crecimiento de las capacidades y las inversiones en la cibernética facilitando las bases técnicas para cada nivel de educación en ciberseguridad y apoyando y haciendo partícipe a la industria, catalizando las inversiones hacia el sector de la cibernética" (p. 41).

El Reino unido ha venido desarrollando una serie de esfuerzos en materia de educación en ciberseguridad, por medio del Department for Digital, Culture, Media and Sport (DCMS), esto engloba un plan de acciones y programas educativos que motivan a los niños y jóvenes a tomar conciencia y comprometerse con la ciberseguridad.

En el año 2017 se fundó un programa que venía a responder a esa necesidad educativa, este se llamaba *Cyber Schools Programme*, estaba dirigido a jóvenes de 14 a 18 años, como se menciona en el sitio web del gobierno, en el artículo *Cyber Schools Programme* (2017):

> La economía del Reino Unido se vuelve cada vez más digital, la seguridad cibernética es fundamental para la seguridad nacional y continúa desempeñando un papel importante para garantizar que el Reino Unido sea un lugar seguro para hacer negocios. Existe una necesidad crítica de aumentar la disponibilidad de habilidades en seguridad cibernética, por lo que el Departamento de Cultura, Medios y Deportes (DCMS) está invirtiendo hasta £20 millones en un ambicioso Programa de Escuelas Cibernéticas (párr. 1).

El NCSC lidera el programa CyberFirst, que ofrece una variedad de actividades para que los jóvenes aprendan sobre el apasionante mundo de la seguridad cibernética, incluidos cursos gratuitos para todos los grupos de edad de 11 a 17 años y un plan de becas y aprendizaje universitario, por lo que, como parte de este programa, el gobierno del Reino Unido lanzó en febrero del año 2022, el proyecto Cyber Explorers, para dotar a los alumnos de las habilidades y conocimientos necesarios para seguir cursos de informática, abriendo una gama de oportunidades de formación adicional y empleo.

Según se menciona en el sitio web del gobierno en el artículo *Tens of thousands of students receive free training to build cyber skills* (2023), el ministro en ciberseguridad, vizconde Camrose, señalo que:

> El creciente sector cibernético del Reino Unido es donde comenzarán las innovaciones tecnológicas y los descubrimientos digitales del futuro. Es por eso que nos enfocamos en derribar las barreras de entrada y crear nuevas oportunidades para que los jóvenes adquieran las habilidades y conocimientos que podrían impulsar carreras emocionantes en el ámbito cibernético. Más de 2000 escuelas en todo el país ya están inscritas en Cyber Explorers, lo que significa que decenas de miles de alumnos pueden beneficiarse de los recursos que se ofrecen, y queremos asegurarnos de que aún más tengan esa oportunidad este año (párr. 5-6).

El gobierno se encuentra comprometido con la educación. ya que reconoce que los esfuerzos del hoy son las recompensas del mañana, ante un campo que crece de una manera explosiva, cada minuto perdido cuenta, así como se describe en el artículo antes mencionado donde se indica que:

> El gobierno del Reino Unido está invirtiendo en la próxima generación de profesionales cibernéticos y expertos en seguridad, ayudando a los jóvenes a desarrollar las habilidades y los conocimientos apreciados por un sector cibernético del Reino Unido valorado en £10,5 mil millones (párr. 10).

Aunado a lo anterior, Chris Ensor, subdirector de desarrollo cibernético del NCSC, menciona lo siguiente:

> La industria cibernética del Reino Unido está creciendo rápidamente, pero como resultado se enfrenta a una escasez de habilidades, razón por la cual es tan importante contar con iniciativas como Cyber Explorers que trabajan para descubrir talento cibernético y apoyar a los jóvenes de todo el país a explorar las oportunidades profesionales que ofrece esta industria. la próspera industria tiene para ofrecer.

Finalmente, el gobierno del Reino Unido en su afán por lograr una estrategia integral en edades tempranas también establece una serie de estándares de seguridad cibernética para escuelas y colegios, para mitigar los impactos operativos y financieros que pueden ocasionar incidentes y ataques cibernéticos en los centros educativos, accediendo de manera no autorizada a recursos tecnológicos con fines perjudiciales.

Estados Unidos, implementado estrategias de educación en ciberseguridad

En la sociedad globalizada y tecnológica en la que se vive actualmente, la educación es cada vez más vulnerable a los ataques cibernéticos, debido a la omnipresencia de la tecnología en la cotidianeidad. Por lo que, a pesar de que cualquier entidad con activos digitales está en riesgo, las instituciones educativas son especialmente vulnerables, puesto que los jóvenes estudiantes desprevenidos suelen ser sus principales objetivos, convirtiéndolos en blancos fáciles.

Según un informe publicado en el sitio web de la Oficina de Responsabilidad Gubernamental de Estado Unidos (2022), los impactos financieros en las escuelas pueden ser amplios. Los funcionarios informaron pérdidas monetarias a los distritos escolares que oscilaron entre $50,000 y $1 millón producto de gastos causados por un incidente cibernético.

Además, existe una estrategia nacional para combatir los ciberataques liderada por el Departamento de Seguridad Nacional (DHS) y la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA). Como parte de esa estrategia, el Departamento de Educación es responsable de coordinar y colaborar con los esfuerzos de ciberseguridad de las escuelas públicas K-12 con otras entidades federales, como el FBI y el DHS, así como con entidades estatales, locales y tribales.

Si bien es cierto, dichas estrategias no están enfocadas en la enseñanza de ciberseguridad a los estudiantes, impactan de manera directa sobre los recursos tecnológicos de las instituciones, ocasionando encarecimiento de la educación, pero al mismo tiempo un llamado de atención a los jóvenes para crear conciencia del uso de las herramientas tecnológicas, ya que un accionar indebido de alguno de ellos puede traducirse en riesgo materializado para el centro educativo.

Estados Unidos también está implementado programas de formación para los jóvenes, por medio de la iniciativa NICE. Como se detalla en el documento *Educación en Ciberseguridad - Planeación del futuro mediante el desarrollo de la fuerza laboral* (2020), elaborado por la Organización de los Estados Americanos:

> El Plan nacional de implementación de educación en ciberseguridad para los niveles de primaria a secundaria tiene como finalidad: alentar a los estudiantes a participar en actividades relacionadas con la ciberseguridad ayudar a educadores a incorporar conceptos de ciberseguridad en las clases y, por último, ayudar a los estudiantes de los niveles primaria y secundaria a identificar oportunidades profesionales en el

> campo de la ciberseguridad. Además, este plan también fomenta la participación de la comunidad en la creación de una campaña de concientización sobre la carrera en ciberseguridad, dirigida a educadores, estudiantes, padres, administradores y consejeros (p. 20).

Para ejecutar este plan *The National Integrated Cyber Education Research Center* (NICERC) ofrece planes de estudio gratuitos para que los educadores integren conceptos de seguridad cibernética en la formación en el aula y también, brinda oportunidades de desarrollo profesional para los maestros.

El Centro Nacional Integrado de Investigación en Educación Cibernética (NICERC) ahora llamado CYBER.ORG, ha creado un programa de educación cibernética K-12 con contenido apropiado para la edad que se alinea con los estándares estatales para la educación El impacto de ese trabajo se mide en miles de docentes y estudiantes con más contenido, recursos y capacitación que impulsarán la fuerza laboral cibernética para el futuro.

Al respecto, CYBER.ORG (2020) menciona que:

> CYBER.ORG es una organización de desarrollo de la fuerza laboral en ciberseguridad que se dirige a estudiantes K-12 con conciencia sobre carreras cibernéticas, recursos curriculares y desarrollo profesional docente. El Departamento de Seguridad Nacional de los Estados Unidos apoya a CYBER.ORG a través de una subvención de la Agencia de Seguridad e Infraestructura de Ciberseguridad (CISA) para desarrollar y distribuir planes de estudio de ciencias cibernéticas, STEM e informática a educadores de todo el país (párr. 14).

La formación en ciberseguridad equipa a las generaciones venideras para un entorno digital globalizado, fomentando una cultura consciente y segura y los prepara para enfrentar los desafíos del futuro, promoviendo una cultura de prevención y protección ante los peligros del ciberespacio, es por esto, por lo que, hay que imitar las mejores prácticas implementadas por países líderes en este campo, adaptando estrategias que apliquen al propio entorno, reconociendo que independientemente del área geográfica, todos se pueden enfrentar a los mismos riesgos y amenazas en el ciberespacio.

Costa Rica y su educación en ciberseguridad

El pasado noviembre se presentó por parte del presidente de la República, Rodrigo Chaves y la ministra de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), Paula Bogantes, la Estrategia Nacional de Ciberseguridad 2023-2027, la cual como se indica en el sitio web del MICITT (2023): "busca asegurar un ecosistema nacional de ciberseguridad seguro, resiliente e inclusivo y proteger de manera efectiva al país, como también a las instituciones del Estado, así como a la ciudadanía ante ciber amenazas y ataques" (párr. 14). Además, la estrategia consta de cinco pilares y uno de ellos se enfoca en la educación, capacitación y concientización, ya que forman parte vital de una estrategia robusta e integral.

Según MICITT (2023), el presidente Rodrigo Chaves expresó lo siguiente:

> lo que aprendimos de los ataques pasados nos permiten prepararnos con mayor madurez y rigurosidad, por lo que estamos construyendo una armadura que protegerá al país de las organizaciones cibercriminales y de las personas que sin ningún escrúpulo pueden intentar atacarnos nuevamente. Por eso, creamos esta estrategia, para recubrir la seguridad informática del país con una coraza ante posibles amenazas (párr. 14).

Como parte de los esfuerzos que se están realizando a nivel país por dotar a los jóvenes de formación en el campo de la tecnología, se rescata lo establecido por el Consejo Superior de Educación (CSE), el cual aprobó el Programa Nacional de Formación Tecnológica (PNFT), que será una nueva asignatura que se impartirá en todos los centros educativos del país a partir del año 2024, como se menciona en el MICITT, en el artículo Consejo Superior de Educación, donde se aprueba el nuevo Programa Nacional de Formación Tecnológica (2023):

> El PNFT es una asignatura incluida en la malla curricular, y por tanto deberá ser aprobada para pasar el año, los programas anteriormente vigentes eran considerados un apoyo al docente, pero no tenían evaluación sumativa y no recibían una calificación, por lo que en ocasiones los estudiantes los asumían con un menor nivel de compromiso (párr. 2).

Como se menciona en la nota Consejo Superior de Educación se aprueba el nuevo Programa Nacional de Formación Tecnológica (2023), donde el objetivo principal en palabras del viceministro académico, Melvin Chaves Duarte es: "introducir y fortalecer desde primera infancia

la tecnología, el pensamiento computacional y la resolución de problemas, forma a las personas estudiantes como creadoras de tecnología capaces de solucionar los problemas de los próximos años" (párr. 4).

Este programa se fundamenta en tres ejes transversales, uno de ellos es el desarrollo del pensamiento computacional para la resolución de problemas y según se indica en la nota: "se fomenta la capacidad de las personas estudiantes para abordar problemas complejos de manera lógica y eficiente, preparándolos para enfrentar los desafíos del mundo tecnológico" (párr.7), el segundo es el de ciudadanía y ética digital, el cual "promueve el uso responsable y ético de la tecnología, equipando a los estudiantes con las habilidades necesarias para navegar de manera segura en el ciberespacio y participar de manera constructiva en la sociedad digital" (párr. 7). El último eje que impacta el programa es el de emprendimiento e innovación y como se menciona en la nota: "se inspira a los estudiantes a ser emprendedores y pensadores innovadores, alentando la creatividad y la capacidad de generar soluciones tecnológicas" (párr. 7).

El Programa Nacional de Formación Tecnológica abarca cuatro áreas específicas de estudio, que se abordan en diversos módulos en los diferentes ciclos educativos. Como se menciona en la nota se utiliza tres metodologías activas, a saber: "el aprendizaje por juegos, el aprendizaje por retos y el pensamiento de diseño (*design thinking*)" (párr. 8). Las áreas que abarcan el programa son las siguientes: ciencia de datos e inteligencia artificial, programación y algoritmos, computación física y robótica, apropiación tecnológica y digital.

Por lo que, como se ha descrito anteriormente, la malla curricular actual en formación tecnológica del Ministerio de Educación Pública se robusteció, lo cual es muy relevante en la formación pública de las futuras generaciones, siempre y cuando se actúe con el compromiso y rigurosidad y en la correcta ejecución del programa.

Sin embargo, los temas en ciberseguridad se ven como un eje trasversal de los módulos educativos y no se contemplan como modelo independiente de formación, lo cual sigue dejando vacíos sustanciales en la formación en temas cibernéticos, ante esto es importante mencionar que en siete colegios técnicos del país se brinda la especialidad en Ciberseguridad, pero por la dinámica institucional de estos centros son muy pocos los jóvenes a nivel nacional que tienen acceso a este tipo de formación.

Malla curricular, Programa Nacional de Formación Tecnológica

El Programa de estudio de Formación Tecnológica de Costa Rica establece su punto de partida para la creación del plan de estudios, centrado en el aprendizaje de tecnologías. La persona docente actúa como guía en la construcción de conocimientos y en el desarrollo de competencias para que el estudiante pueda integrarse adecuadamente en una sociedad digital a nivel global con su identidad nacional.

Según se menciona en el sitio web del Ministerio de Educación Pública, en el documento *Programa de Formación Tecnológica en el Sistema Educativo Costarricense* (2023), el sustento de dicho programa radica en que:

> Se fundamenta en varios referentes nacionales e internacionales que promueven la inclusión de las tecnologías en educación y que buscan que esta sea actualizada, relevante y acorde con las demandas del siglo XXI. En la era digital actual, la accesibilidad y la habilidad para utilizar las tecnologías de forma responsable, efectiva y segura son componentes clave para el éxito personal y profesional en la población estudiantil (p. 28).

Como se mencionó anteriormente, en este programa se definieron cuatro áreas de conocimiento, para fomentar y desarrollar la enseñanza y también, promover una actitud de aprendizaje continuo y de innovación digital, las cuales según el documento *Programa de Formación Tecnológica en el Sistema Educativo Costarricense* (2023) se describen a continuación:

Apropiación tecnológica y Digital: esta área desarrolla la adquisición de conocimientos, habilidades y destrezas en el uso de las tecnologías y herramientas digitales que permiten a las personas estudiantes accesar, gestionar, comprender, integrar, comunicar, evaluar y crear recursos digitales de forma segura y eficaz, para aprovecharlas en su desarrollo personal, académico y profesional.

Programación y Algoritmos: desde esta área se desarrolla la aplicación de conceptos de programación de computadora y el uso de algoritmos, que introduce a las personas estudiantes en el mundo de la tecnología y la informática, brindándoles conocimientos necesarios para comprender y utilizar la programación como una herramienta para resolver problemas, desarrollando prácticas y actitudes propias del pensador computacional que pueden transferir a otros contextos de su vida personal, académica o profesional.

Computación física y Robótica: esta área desarrolla la integración de conceptos de informática, programación, electrónica y robótica para comprender y utilizar la tecnología en su entorno físico, brindando la oportunidad de aprender a través de la construcción y programación de artefactos físicos o robots, desarrollando habilidades en programación, pensamiento computacional y resolución de problemas, al tiempo que promueve la creatividad, la colaboración y el aprendizaje activo.

Ciencias de Datos e Inteligencia Artificial: esta cuarta área desarrolla el estudio, análisis y comprensión de los datos, combinando la estadística, las matemáticas, la programación y el conocimiento de dominio, con el objetivo de analizar grandes conjuntos de datos y extraer información relevante para la toma de decisiones, lo que implica el desarrollo de competencias de análisis y visualización de datos, Inteligencia Artificial y conocimientos en ciberseguridad, para resolver problemas complejos y mejorar procesos en diferentes campos, como negocios, investigación científica, medicina, entre otros (pp. 41-42).

Es relevante mencionar que, de estas cuatro áreas de estudio en la única que se abarca de manera más significativa los temas de ciberseguridad es en apropiación tecnológica y digital, la cual cuenta con una subárea de estudio llamada "seguridad y privacidad digital", que según se menciona en el documento *Programa de Formación Tecnológica en el Sistema Educativo Costarricense* (2023) su objetivo es: "aplicar medidas que aseguren la protección de información personal, así como la que terceras personas ponen en su conocimiento, resguardando la privacidad o confidencialidad" (p. 44).

El programa abarca muchos temas de estudio distribuidos en las cuatro áreas definidas, el Ministerio de Educación Pública asigna un área por institución, ya que no sería posible formar a los jóvenes en todos estos tópicos, a lo largo de su ciclo lectivo en secundaria, de igual manera este es su primer año de ejecución, por lo que, el proyecto está en etapas iniciales y por eso, es importante analizar y monitorear el desarrollo y cumplimiento de este, ya que como es de conocimiento general, la educación pública del país contiene algunas brechas educativas.

Los docentes, figuras importantes en la formación de los adolescentes en ciberseguridad

La reciente pandemia trajo consigo la virtualidad en todas las áreas: profesional, laboral y académica, generando también el crecimiento del uso de las redes sociales y la tecnología entre los

adolescentes, según el Centro Nacional de Investigación de la Opinión, de la Universidad de Chicago, en su investigación titulada: *How Diverse Communities of Young People Think About the Multifaceted Relationship Between Social Media and Mental Health* (2023), se incluyen a 1.274 adolescentes (de 14 a 17 años) y adultos jóvenes (de 18 a 22 años) y concluyó lo siguiente:

> Casi una cuarta parte de los participantes informó usar las redes sociales casi constantemente durante todo el día, lo que nos muestra como los jóvenes dividen su tiempo entre el mundo virtual y el físico y la relevancia que tiene el ciberespacio en sus vidas, por esto la importancia de educarlos como ciudadanos digitales informados ante todas las amenazas que puedan encontrar (p. 13).

Además, concluyen que más de un tercio de los jóvenes en 30 países han reportado haber sufrido acoso cibernético y 1 de cada 5 falta a la escuela a causa de ello; según datos de la Unicef, es importante el papel que cumplen los profesores como formadores en habilidades blandas, como la capacidad analítica y resolución de problemas por mencionar algunos y es vital frenar la ola de violencia digital a la que se enfrentan los estudiantes actualmente.

Sumado a esto, en su artículo *La seguridad de la infancia y la juventud en la red*, la Unicef (2023) destaca que: “alrededor del 80 % de niñas y niños de 25 países han expresado sentirse en peligro de abuso o explotación sexual en línea” (párr. 4). Es aquí donde el personal docente tiene un papel protagónico como barrera de protección ante situaciones de riesgo en la que se vean inmersos los jóvenes, con el fin de abordarlos de manera oportuna y evitar no solo una posible exclusión educativa, sino también problemas de depresión, ansiedad y conductas que pongan en riesgo su vida por temas de bullying.

Conforme al informe, *Estadísticas Mundiales de Bullying* (2021) desarrollado por Miglino (2021), director de la Fundación Bullying Sin Fronteras: “el acoso escolar y el ciberbullying son causantes directos de más de 200,000 muertes, ya sea por homicidio o por inducción al suicidio cada año y las redes sociales son su gran aliado” (párr. 1).

Por ende, la construcción de capacidades en los jóvenes en materia de ciberseguridad es muy importante; así como la observación y atención de los profesores para identificar cambios en la conducta de los estudiantes que salten alertas, para entonces enseñarles cómo pueden evitar ser presas de estos ataques que afecten su integridad física, emocional y social.

El desarrollo de habilidades para gestionar situaciones de ciberacoso y el brindar herramientas para enfrentarlo, es una labor posible desde las aulas, pues independientemente de la

materia que brinde el profesor, la ciberseguridad es tema de todos y los docentes vienen a ser posibles escudos humanos, por esto su papel como actores formadores es fundamental para ayudar a desarrollar el pensamiento crítico de los estudiantes y ser formadores de conciencia.

Un caso notable es el de Finlandia, país destacado en Europa por ser el menos vulnerable a los ataques de noticias falsas, de acuerdo con el artículo *How Finland starts its fight against fake news in primary schools* (2020), de Henley que explica como esto lo han hecho posible gracias a la educación que imparten en edades tempranas en colegios, desde el año 2016, en las clases de matemáticas, los alumnos aprenden lo fácil que es mentir en estadística. En arte, ven cómo se puede manipular el significado de una imagen. En historia, analizan campañas de propaganda notables, mientras que los profesores de finlandés trabajan con ellos sobre las muchas formas en que las palabras pueden usarse para confundir y engañar.

Kivinen (2020) detalla lo siguiente:

> El objetivo son ciudadanos y votantes activos y responsables, Pensar críticamente, verificar, interpretar y evaluar toda la información que recibes, dondequiera que aparezca, es crucial. Lo hemos convertido en una parte central de lo que enseñamos, en todas las materias.
>
> Solo porque es algo bueno o algo agradable no significa que sea verdad o sea válido, mencionó una profesora finlandesa, a su clase, cuando les mostró a los estudiantes tres videos de TikTok y debatieron las motivaciones de los creadores y el efecto que los videos tuvieron en ellos (párr. 4-5).

En la educación secundaria los docentes, desde su trinchera, pueden generar conciencia y desarrollar el pensamiento crítico de los estudiantes mientras tienen prácticas cotidianas y durante el aprendizaje de materias académicas que parecieran no tienen relación alguna, deben cuestionarse como incluyen elementos de ciberseguridad para incentivar el carácter analítico en los adolescentes, lo cual les permitirá tener herramientas que cuando naveguen en el mundo digital, les funcionen para encender sospechas de posibles situaciones que los pongan en riesgo.

Sin embargo, hay un trabajo vital por realizar y es crear esta conciencia personal en los profesores, pues muchos carecen de conocimientos tecnológicos, por ende, hacen un uso muy reducido de herramientas tecnológicas en las aulas, además desconocen que incluso ellos pueden incurrir en prácticas riesgosas en la web.

Según la encuesta Kids Online 2023, en Costa Rica, la institución escolar no está promoviendo habilidades digitales ni oportunidades, así como tampoco está dando acompañamiento, a pesar de que la investigación muestra un mayor uso sistemático en el aula y una mayor mediación activa de la persona docente favorece las oportunidades y habilidades.

Los estudiantes pasan la mayor parte de su día en las aulas, por lo que, es importante que encuentren en los profesores y la institución un apoyo y orientación ante las problemáticas que se enfrentan en línea, por esto, para que los profesores sean guías activos para los estudiantes, se debe velar por que ellos reciban formación básica en ciberseguridad e identifiquen conductas sospechosas, ciberbullying, ciberacoso y otras amenazas a las que se ven expuestos los jóvenes.

Ante este aspecto, toma relevancia que los docentes conozcan a nivel legislativo como en Costa Rica se ampara la seguridad en línea, saber que se cuenta con el código de la niñez y la adolescencia que enmarca los derechos que tienen los jóvenes, en cuanto a la protección de sus datos, así como su integridad física. De igual manera, la Ley de Protección de la Niñez y la Adolescencia frente al contenido nocivo de Internet y otros medios electrónicos donde se torna vital la ciberseguridad.

Finalmente, el tener un conocimiento básico de las leyes que los protegen, en caso de ser víctimas de alguna amenaza en el mundo digital, dotarlos de herramientas para proteger y velar por los derechos de los estudiantes y dar un abordaje correcto de las distintas situaciones que se puedan presentar.

Impacto vocacional para la elección de carreras tecnológicas

El acelerado desarrollo tecnológico viene acompañado de la necesidad de formar profesionales en esta área y con esto, la ciberseguridad toma un papel protagónico pues, con el nacimiento de nuevas plataformas y redes sociales para interactuar laboral y personalmente, aparecen las amenazas y los depredadores digitales buscan maneras más ingeniosas de atacar.

En la nota “Ciberseguridad se dispara: sector creció 350 % en la demanda de talento a nivel mundial”, del periódico *La República* (2024) manifiestan: “que la demanda en profesionales de Ciberseguridad ha crecido un 350 %, de acuerdo con la firma investigadora Cybersecurity Ventures” (párr.1), adicionalmente, exponen lo siguiente:

> La tecnología tendrá un papel fundamental en el futuro del mercado laboral. Las ingenierías y en específico el área de la ciberseguridad crecen a pasos agigantados. Debido a esta coyuntura, es necesario pensar en la formación de profesionales integrales, no solo reforzando la parte académica, si no también desarrollando las habilidades blandas que les abrirán más opciones en los diferentes sectores donde se desarrollen (párr. 3).

Por lo tanto, es muy importante que los estudiantes se formen en conocimientos básicos de ciberseguridad y otros temas tecnológicos, pero también que los profesores al conocer sobre la demanda tan grande que existe actualmente, pueden ser orientadores y guías vocacionales para los estudiantes, de manera que se impulse a las nuevas generaciones desde el ámbito formativo y posteriormente, como consejeros profesionales.

Esto les permitiría tener desde la secundaria, herramientas y conocimientos sobre qué demanda el mundo laboral y cómo pueden irse formando hasta llegar a una educación superior. Según el diario *Infobae* (Parada, 2024):

> Mucho se ha hablado de la formación en carreras STEM (Ciencia, Tecnología, Ingeniería y Matemáticas, por sus siglas en inglés), y no es para menos, datos del Labor Departament de los Estados Unidos señalan que para el año 2029 habrá cerca de 3.2 millones de puestos de trabajo relacionados con estas áreas, sin embargo, no todo es color rosa, también se ha analizado que la cantidad de estudiantes que se matriculan a estas carreras viene disminuyendo (párr. 1).

Por esto, educar y enseñar en edades tempranas despierta la curiosidad y el interés por estas ramas, les augura un buen futuro profesional y laboral y les insta a ser los futuros desarrolladores del mundo digital.

Desarrollo integral en la formación de los jóvenes

El crecimiento digital en la actualidad va más allá de un tema tecnológico, ya que impacta otros aspectos de manera transversal, como los son las habilidades blandas, las cuales son esenciales para navegar y gestionar todos los componentes asociados; por lo que, no solo basta con comunicarse si no saber hacerlo de manera efectiva; es vital tener la habilidad de resolver conflictos, ser empáticos y desarrollar esa creatividad y liderazgo, en un entorno donde las

competencias sociales son fundamentales para crecer de manera profesional y determinar el desempeño en diferentes situaciones.

Adicionalmente, la resolución de problemas es una habilidad que se convierte en prioritaria, según la UNICEF (2022), en su guía *Las 12 habilidades transferibles*, lo define como: "es la capacidad para identificar una dificultad, tomar medidas lógicas a fin de encontrar una solución deseada, así como supervisar y evaluar la implementación de tal solución" (p. 10). Está relacionada con otras habilidades, como el pensamiento crítico y la creatividad y es altamente valorada en entornos académicos, laborales y de la vida en general.

Otra de las habilidades que se vuelve fundamental en esta era digital es la comunicación, la cual se define como: "la comunicación puede definirse como la capacidad para compartir significados a través del intercambio de información y comprensión común, lo cual es clave para todas las demás habilidades" (p. 24). El saber comunicarse comprende un conjunto de aptitudes básicas que permiten relacionarse con los demás de forma efectiva. Estas no solo se refieren a ser un buen orador, sino también a desarrollar la escucha activa, establecer contacto visual de manera efectiva y natural, ser asertivos al comunicar una idea y entender las diferentes perspectivas.

Finalmente, el saber tomar el control de sí mismos es de suma importancia, ya que se encuentra relacionado de manera directa con otras habilidades: "se puede definir como la habilidad para reconocer y controlar emociones, sentimientos e impulsos. Incluye diversas habilidades interrelacionadas, con aplicabilidad en ámbitos familiares, escolares, laborales y sociales" (p. 20). Además, el autocontrol fomenta la autoeficacia y la conciencia propia, lo que contribuye a mejorar las relaciones y la calidad de vida en general.

Los padres como actores vitales en la formación de seguridad en línea de los adolescentes

Los principales protagonistas en la vida de los adolescentes son sus padres o cuidadores, en ellos recae la educación de valores, así como ser guía para detectar conductas inusuales, riesgosas e incluso, ser observadores y generar cercanía con sus hijos, esto les permite apoyarlos en caso de sufrir alguna amenaza en la que se puedan ver envueltos, mientras navegan en la red. De acuerdo con el informe *Impacto de la tecnología en la adolescencia. Relaciones, riesgos y oportunidades* (2021) de la Unicef se mencionan cifras alarmantes y se destaca:

> La relación que tienen los jóvenes con la tecnología y sus distintas plataformas es incluso mayor que los adultos, y por esta razón es que se convierten en portillos vulnerables a sufrir de ciberataques, pues el 90 % se conecta a Internet diariamente (p. 4).

Este estudio fue realizado a más de 50.000 adolescentes de 265 colegios en España y muestra cifras alarmantes que los padres de familia en su gran mayoría desconocen por su poca cercanía y buena relación con sus hijos, más del 40 % de los adolescentes asegura haber recibido mensajes de contenido erótico/sexual, 1 de cada 10 ha recibido alguna proposición sexual por parte de un adulto y 1 de cada 5 podría estar sufriendo ciberacoso.

El problema no solo radica en a forma en que los jóvenes están siendo atacados en el mundo digital, sino que aunque un 25 % de los encuestados asegura tener discusiones con sus padres, madres o cuidadores por la tecnología al menos una vez a la semana, los propios jóvenes indican que solo un 29 % les ponen límites o normas sobre el uso de Internet y de las pantallas.

De la misma manera, los jóvenes al sentirse más libres en el ciberespacio reaccionan con conductas más desinhibidas y distintas a las que tienen en el mundo real, por esto res que la supervisión del uso de dispositivos electrónicos es una labor que deben realizar los padres para identificar acciones como el ciberacoso, sexting, suplantación de identidad, sextorsión, entre otros.

Otras cifras que señalan la misma problemática se dan en el estudio *Ciberacosadores: Un estudio cuantitativo con estudiantes de secundaria, Universidad de Murcia* (2018): “donde se entrevistaron a 950 estudiantes de Educación Secundaria Obligatoria con edades comprendidas entre los 11 y los 18 años, arroja que el 23,3 % de los encuestados, había indicado haber realizado una o más conductas de ciberacoso hacia otros” (p. 137).

En esta misma encuesta, se muestra como el ciberacoso está asociado al hecho de tener un dispositivo electrónico o la computadora en el cuarto, pues al estar en solitario las acciones de este tipo incrementan, el 29 % de los jóvenes encuestados que habían cometido ciberacoso, tenían un dispositivo en su habitación, este dato bajaba al 20 % de los que no tenían este acceso.

En Costa Rica, estas cifras no están alejadas de esta realidad, donde el 15 % de los jóvenes entre 15-17 años reportan haber experimentado maltrato, tanto de manera física como virtualmente, tal como lo detalla, la II Encuesta Nacional Kids Online (2024), donde un 40 % de los adolescentes asegura recibir el abuso por parte de una amiga o amigo y el 34,3 % de algún desconocido. Las aplicaciones y plataformas en las cuales se da más el ciber acoso son mensajes de texto, audio y

WhatsApp (61,6 %); seguido de los mensajes personales de Instagram (19,2 %) y en los juegos por internet (17,2 %).

Otro factor preocupante que arrojó el estudio es como el 12 % de los adolescentes participantes de la encuesta indicó haber recibido mensajes de contenido sexual. Además, el 3 % aceptó haber recibido este contenido por parte de personas mayores de edad (este porcentaje equivaldría a 10.224 personas del total de la población entre 13 y 17 años encuestada).

Sin embargo, según el informe *Factores detonantes de acoso escolar entre estudiantes de colegios públicos académicos* realizado por el Ministerio de Educación Pública (2023) de Escalante (2023) se menciona que:

> El tema familiar es aún una debilidad, pues no se ha logrado una participación total en los procesos para prevenir y mitigar el acoso, evidencia de esto, son las respuestas dadas por los padres de familia entrevistados, sobre la participación en algunas acciones que implementa el colegio en cuanto a esta problemática de una muestra de 85 encuestados solo 12 padres-madres/encargados dijeron participar.
>
> Por otro lado, menos de la mitad los padres-madres de familia o encargados han recibido información sobre diversos temas correspondientes al acoso escolar en reuniones por parte del centro educativo y menos de la mitad menciona que conocen la actuación para la atención de situaciones de violencia y riesgo en los centros educativos (p. 77).

Esta desinformación o falta de información e involucramiento, tanto de las instituciones como de los papás hace que los jóvenes estén menos amparados ante los peligros del mundo digital. Según la II Encuesta Nacional Kids Online (2024), los padres de familia o cuidadores reportan habilidades digitales similares y puntajes similares de uso problemático del teléfono celular. Este aspecto limita el papel de las personas cuidadoras, tanto en la promoción de oportunidades de uso como en la prevención ante riesgos y posibles daños.

Por esto, es vital proporcionar a las familias, padres y cuidadores, herramientas y apoyo para ejercer su labor educativa y de acompañamiento de manera eficiente, de manera que puedan comprender los riesgos en los que están expuestos sus hijos, conocer cómo pueden evitar que sean víctimas o victimarios y dar a conocer la manera en la que pueden hacer denuncias, en caso de que sus hijos sean víctimas de algún acosador digital.

Importancia de una política en ciberseguridad en el Liceo de Pavas

En el primer semestre del 2022 Costa Rica sufrió varios ataques cibernéticos a instituciones gubernamentales, esto dejó en evidencia la poca capacidad de respuesta y vacíos en temas de ciberseguridad en las diferentes instituciones, pues si bien es cierto muchas de ellas cuentan con políticas y controles establecidos para prevenir y mitigar riesgos cibernéticos, la aplicación de estos medios no se está realizando de forma adecuada o quizá no se están ejecutando.

Según una nota publicada en el sitio web del *Semanario Universidad*, Bermúdez (2023) menciona las siguientes estadísticas:

> En el informe DFOE-CAP-OS-00001-2023, la Contraloría analizó la emergencia cibernética provocada el año pasado por ataques informáticos a instituciones públicas, y realizó una cuantificación del riesgo cibernético en el sector público, evaluando en 251 instituciones las prácticas básicas, así como su exposición a riesgos en esta área (vulnerabilidad) y los niveles de riesgo que enfrentan (amenazas).
>
> El balance de la Contraloría detectó que solo en un 31,5 % los niveles de vulnerabilidad y amenazas son bajos, mientras que en un 40,2 % es medio, y en un 28,3 % es alto. Es decir, en un 68,5 % tienen niveles que deben atenderse, ante el aumento de este tipo de amenazas. Aunado a ello, se detectó que únicamente un 10,7 % de las instituciones había identificado la información sensible que manejaba, y de este porcentaje minoritario, tan solo un 15 % la encriptaba (párr. 2-4).

Estos ataques se dieron a ciertas instituciones importantes del estado, que forman parte de la base institucional del país por su relevancia en funciones y manejo de información, a partir de los incidentes el gobierno se ha ocupado de generar estrategias para mitigar riesgos y reducir el impacto.

El Ministerio de Educación Pública cuenta con la Política en Tecnologías de la Información (2020), que busca garantizar la protección, la confidencialidad, la integridad y la disponibilidad de la información en las actividades realizadas, alineando la seguridad de TI con la seguridad del Ministerio de Educación Pública; estructurada de manera teórica, pero que es poco aplicable y específica en prácticas diarias en los colegios públicos del país.

Las escuelas o colegios del país no han sufrido ataques relevantes en materia de ciberseguridad, a pesar de que cuentan con una serie de vulnerabilidades, dado que no se cuenta

con una estructura tecnológica robusta y en la mayoría de instituciones no existe una política de seguridad de información que garantice un adecuado acceso a los recursos, así como un uso correcto de la información que cumpla con los principios de confidencialidad, disponibilidad e integridad de los datos; un ejemplo muy claro es el Liceo de Pavas, que al no existir una guía clara ejecutan acciones que pueden exponer de manera significativa, los recursos tecnológicos y por ende, el manejo de la información no es el más eficiente.

Ante esto, es importante medir el impacto que puede tener un ataque y cómo puede interrumpir las operaciones educativas, sin duda, esto afecta a los estudiantes, sus familias y a los profesores; además pueden dar lugar a la divulgación y el robo de información personal de los estudiantes y empleados de la institución, ya que recopilan y almacenan mucha información personal sobre estudiantes y el personal docente y administrativo.

En el sitio de web de la Oficina de Responsabilidad del Gobierno de Estados Unidos (2022), se mencionan unas cifras reveladoras:

> En diciembre de 2021, un proveedor de las Escuelas Públicas de Chicago fue víctima de un ataque de ransomware en el que se reveló información personal de más de 500.000 estudiantes y miembros del personal. Los datos incluían nombres de estudiantes, escuelas, fechas de nacimiento, géneros, números de identificación escolar, números de identificación estatales de estudiantes e información de cursos de años escolares anteriores.
>
> En febrero de 2021, las Escuelas Públicas de Winthrop en Massachusetts fueron víctimas de un ataque de denegación de servicio que interrumpió el aprendizaje y la enseñanza en las redes y sistemas web del distrito. Esto incluía correos electrónicos, plataformas de aprendizaje y servicios de videoconferencia, todo lo cual se volvió esencial para la educación durante la pandemia, cuando las clases se impartían de forma remota.
>
> De manera similar, en septiembre de 2020, las Escuelas Públicas del Condado de Miami-Dade fueron víctimas de una serie de ataques de denegación de servicio. Esto interrumpió el aprendizaje y la enseñanza en las redes y sistemas basados en la web del distrito. Los funcionarios de Connecticut informaron que un distrito escolar tuvo que cerrar durante 3 o 4 días, debido a un incidente de ciberseguridad (párr. 7).

Para hacer frente a estos retos, las escuelas y colegios necesitan adoptar una estrategia completa de ciberseguridad que contemple directrices precisas, tecnología moderna y programas educativos para alumnos, padres de familia y empleados. Esto incluye la implementación de buenas prácticas, el análisis de riesgos y vulnerabilidades en la institución, así como promover una cultura de seguridad de la información en el centro educativo para proteger la información y garantizar un entorno digital seguro para todos los actores implicados, lo cual se puede ejecutar estableciendo una política clara y adaptada para cada institución.

Existen algunas normas o estándares en temas de seguridad de la información y ciberseguridad, una de ellas es la norma ISO/IEC 27002:2022, la cual proporciona una referencia de una serie de controles de seguridad de la información. Esta norma pertenece a la familia ISO/IEC 27000, que sirve como referencia a un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de sistemas de gestión de la seguridad de la información.

Según se detalla en el sitio web de ISO (2022):

> ISO/IEC 27002 ofrece buenas prácticas y objetivos de control relacionados con aspectos clave de la ciberseguridad, como el control de acceso, la criptografía, la seguridad de los recursos humanos y la respuesta ante incidentes. Esta norma sirve de modelo práctico para las organizaciones que deseen proteger eficazmente sus activos de información contra las ciber amenazas. Al seguir las directrices de ISO/IEC 27002, las empresas pueden adoptar un enfoque proactivo de la gestión de riesgos de ciberseguridad y proteger la información crítica del acceso no autorizado y la pérdida (párr. 1).

Si bien es cierto, muchos de los controles que se detallan en la norma no aplican para ciertas instituciones educativas, este marco de buenas prácticas sirve como referencia y base para establecer controles necesarios para mitigar vulnerabilidades y amenazas a las que están expuestas sus recursos tecnológicos y su información, debido a los desafíos que se enfrentan en la actualidad en el panorama digital.

CAPÍTULO III. MARCO METODOLÓGICO

Enfoques de Investigación

Es importante definir el concepto de investigación, por lo que, Hernández-Sampieri (2020) lo conceptualizan como el "conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno o problema con el resultado (o el objetivo) de ampliar su conocimiento. Esta concepción se aplica por igual a los enfoques cuantitativo, cualitativo y mixto" (p. 4).

La investigación es un procedimiento riguroso, meticuloso y organizado en el que se busca resolver problemas. Además, mantiene un orden que asegura la generación de nuevos razonamientos lógicos y posibles soluciones prácticas orientadas a ampliar y generar entendimiento.

Enfoque cuantitativo

La investigación cuantitativa se basa en técnicas estructuradas y busca la medición de variables definidas. Hernández-Sampieri (2020) lo detalla de la siguiente manera:

> Representa un conjunto de procesos organizado de manera secuencial para comprobar ciertas suposiciones. Cada fase precede a la siguiente y no podemos eludir pasos, el orden es riguroso, aunque desde luego, podemos redefinir alguna etapa. Parte de una idea que se delimita y, una vez acotada, se generan objetivos y preguntas de investigación, se revisa la literatura y se construye un marco o perspectiva teórica. De las preguntas se derivan hipótesis y determinan y definen variables; se traza un plan para probar las primeras (diseño, que es como "el mapa de la ruta"); se seleccionan casos o unidades para medir en estas las variables en un contexto específico (lugar y tiempo); se analizan y vinculan las mediciones obtenidas (utilizando métodos estadísticos), y se extrae una serie de conclusiones respecto de la o las hipótesis (p. 6).

El enfoque cuantitativo busca la mayor objetividad posible en todo el proceso o ruta, además sigue un patrón predecible y estructurado y pretende describir, explicar y predecir los

fenómenos investigados, buscando regularidades y relaciones causales entre elementos (variables), con el fin de conocer o capturar la realidad o fenómeno estudiado.

Enfoque cualitativo

La investigación cualitativa analiza datos no numéricos para interpretar el significado, por medio de la recolección de información basada en la observación de comportamientos naturales, discursos o respuestas abiertas para la interpretación de los resultados posteriormente.

Hernández-Sampieri (2020), lo define como:

> El enfoque cualitativo también estudia fenómenos de manera sistemática. Sin embargo, en lugar de comenzar con una teoría y luego "voltear" al mundo empírico para confirmar si esta es apoyada por los datos y resultados, el investigador comienza el proceso examinando los hechos en sí y revisado los estudios previos, ambas acciones de manera simultánea, a fin de generar una teoría que sea consistente con lo que está observando que ocurre. De igual forma, se plantea un problema de investigación, pero normalmente no es tan específico como en la indagación cuantitativa. Va enfocándose paulatinamente. La ruta se va descubriendo o construyendo de acuerdo con el contexto y los eventos que ocurren conforme se desarrolla el estudio (p. 7).

En este enfoque se plantea un problema, pero no se sigue un proceso preestablecido con claridad y predomina la lógica o razonamiento inductivo, además el proceso de indagación resulta más flexible y se desplaza entre la experiencia, la acción y los resultados y resulta interpretativa, pues pretende encontrar sentido a los fenómenos, por lo que, puede interpretar que el enfoque se basa en métodos de recolección de datos no estandarizados al inicio o no completamente predeterminados.

Enfoque mixto

La investigación mixta es una metodología de investigación que combina el método cuantitativo y cualitativo, en este se recopilan, analizan y se integran datos de ambos mundos, con

el fin de comprender de una manera más detallada la problemática, ampliando el umbral del objeto de estudio y profundizando en los resultados obtenidos.

Hernández-Sampieri (2020) detalla lo siguiente:

> Los métodos mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (metainferencias) y lograr un mayor entendimiento del fenómeno bajo estudio (p. 612).

Al utilizar ambos métodos se realiza una triangulación en la recolección de datos, ante la complejidad de la investigación para garantizar la resolución de discrepancias y cerrar brechas o puntos débiles de los otros métodos, por lo que, al desarrollar varios instrumentos se proporciona un entendimiento más completo de los hallazgos encontrados.

Enfoque de investigación seleccionado

El enfoque seleccionado para la presente investigación es el enfoque mixto, ya que la propuesta se basará en las investigaciones, recopilación de datos, información comparativa, así como las encuestas que se realizarán a los actores de la investigación: estudiantes, personal docente y administrativo y padres de familia, para de esa manera, obtener la información necesaria, con el fin de definir el foco y el sustento de la propuesta.

Así mismo, la bibliografía utilizada se basa en normas, leyes y programas de formación nacionales e internacionales, que buscan estandarizar y generar un marco de referencia para las instituciones públicas, privadas y los ciudadanos sobre ciberseguridad.

Tipos de Investigación

La escogencia del tipo de investigación determinará los pasos a seguir del estudio, las técnicas y métodos a emplear en este. En general, determina todo el enfoque de la investigación influyendo en instrumentos y hasta en la manera de cómo analizar los datos recaudados.

A continuación, se detallarán los tipos de investigación exploratoria, descriptiva y correlacional y en cuál de estos se clasifica la propuesta.

Investigación exploratoria

Cuando la investigación de la literatura muestra que hay guías no investigadas e ideas poco profundizadas sobre el tema en cuestión o bien, si se desea indagar sobre temas y áreas desde nuevas perspectivas se está ante una investigación exploratoria.

Según Hernández-Sampieri (2017), los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o que no se ha abordado antes (p. 82). Su función es familiarizar al investigador con el estudio y dar a conocer fenómenos que son poco conocidos y abren la posibilidad de realizar estudios más especializados y profundos.

Investigación descriptiva

Según Hernández-Sampieri (2017), con los estudios descriptivos se busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis (p. 76).

Los estudios descriptivos muestran todas las aristas de un fenómeno, suceso, comunidad, contexto o situación. En esta clase de estudios, el investigador debe ser capaz de definir o al menos visualizar, qué se medirá (conceptos, variables y componentes) y sobre qué o quiénes se recolectarán los datos (personas, grupos, comunidades, objetos, animales o hechos).

Investigación correlacional

Una investigación correlacional es un método de estudio a través del cual se determina cómo dos variables se relacionan. Cabe destacar que, el investigador no interviene en las variables, ya que se trata de un estudio no experimental.

Hernández-Sampieri (2017) destacan que:

> La utilidad principal de los estudios correlacionales es saber cómo se puede comportar un concepto o una variable al conocer el comportamiento de otras variables vinculadas. Las correlaciones pueden ser positivas (directamente proporcionales) o negativas (inversamente proporcionales). Si es positiva, significa

> que los casos que muestren altos valores en una variable tenderán también a manifestar valores elevados en la otra variable. Si es negativa, casos con valores elevados en una variable tenderán a mostrar valores bajos en la otra (p. 78).

El objetivo principal consiste en determinar si las variables están relacionadas entre sí, ya sea positiva o negativamente o bien, si son variables independientes. Además, no profundiza sobre las causas de dicho vínculo y al ser un método no experimental, el investigador no interviene.

Tipo de investigación seleccionado

La presente propuesta es de tipo descriptiva, pues se detallarán propiedades, características y datos importantes sobre la importancia de la formación en ciberseguridad en adolescentes, además se hará en una población específica (Liceo de Pavas) y el estudio se realizará en el año 2024. Asimismo, busca investigar y analizar los programas en educación sobre ciberseguridad, tanto a nivel nacional como internacional.

Por otra parte, por medio de las encuestas se conocerá el nivel de conocimiento y las amenazas cibernéticas a las que está expuesta la población en estudio. Por lo que, con el análisis de la información recolectada se robustecerá el planteamiento del problema y servirá de parámetro para definir y argumentar la propuesta de formación.

Fuentes de Información

Una fuente de información es todo aquello que proporciona datos para reconstruir hechos y las bases del conocimiento. Las fuentes de información son un instrumento para el conocimiento, la búsqueda y el acceso de a la información.

Según Dankhe (1986), pueden ser clasificadas en tres tipos: fuentes primarias, secundarias y terciarias. A continuación, se detallarán cada uno de estas.

Fuentes primarias

Son consideradas la base principal de la investigación académica. Estas fuentes proporcionan datos originales y sin interpretación directamente relacionados con el tema de

estudio. Constituyen el objetivo de la investigación bibliográfica o revisión de la literatura y proporcionan datos de primera mano (Dankhe, 1986).

Según Sampieri (2017), un ejemplo de éstas son los libros, antologías, artículos de publicaciones periódicas, monografías, tesis y disertaciones, documentos oficiales, reportes de asociaciones, trabajos presentados en conferencias o seminarios, artículos periodísticos, testimonios de expertos, películas, documentales y videocintas. Por lo tanto, utilizar fuentes primarias permite realizar análisis críticos y extraer conclusiones.

Fuentes secundarias

Este tipo de fuentes son las que ya han procesado información de una fuente primaria. Este procesamiento se puedo dar por medio de la interpretación, análisis o extracción de la información de las fuentes primarias. Según Sampieri (2017), consisten en compilaciones, resúmenes y listados de referencias publicadas en un área de conocimiento en particular (son listados de fuentes primarias).

Fuentes terciarias

Las fuentes de información terciarias son herramientas de referencia que recopilan y organizan información que provienen de fuentes primarias y secundarias. Estas fuentes proporcionan una visión general y resumida del conocimiento existente sobre un tema, facilitando el acceso rápido a información clave.

Según Sampieri (2017), se tratan de documentos que compendian nombres y títulos de revistas y otras publicaciones periódicas, así como nombres de boletines, conferencias y simposios; nombres de empresas, asociaciones industriales y de diversos servicios (pertinentes para las ciencias de la conducta; por ejemplo, directorios de empresas que se dedican a cuestiones de recursos humanos, mercadotecnia y publicidad, opinión pública, etc.); títulos de reportes con información gubernamental; catálogos de libros básicos que contienen referencias y datos bibliográficos; y nombres de instituciones al servicio de la investigación (organismos nacionales e internacionales que financian proyectos de investigación, agencias de investigación, etc.). Son útiles para detectar fuentes no documentales como organizaciones que realizan o apoyan estudios, miembros de asociaciones científicas (quienes pueden asesorar en un campo en particular),

instituciones de educación superior, agencias informativas y dependencias del gobierno que efectúan investigaciones.

Fuentes de información seleccionadas

Para el desarrollo de la propuesta se utilizan principalmente fuentes de información primarias y secundarias. En el caso de las primarias, se hace uso de libros, informes técnicos, documentos oficiales de las entidades públicas, así como leyes.

Adicionalmente, se hace uso de sitios web en los cuales, se realizan análisis de primera mano y en tiempo real en temas de ciberseguridad, así como de artículos de sitios prestigiosos con información relevante que detalla el tema a tratar. Finalmente, las fuentes de información secundarias que se utilizan sirven como base para ampliar las investigaciones y estudios realizados de primera mano y son un complemento para sintetizar el contenido de fuentes primarias.

Variables

Según Sampieri (2017), “una variable es una propiedad o característica de fenómenos, entidades físicas, hechos, personas u otros seres vivos que puede fluctuar y cuya variación es susceptible de medirse u observarse.” (p. 82). También menciona que las variables adquieren valor para la investigación científica, cuando llegan a relacionarse con otras variables, es decir, si forman parte de una hipótesis o una teoría.

Además, los tipos de variables vienen determinados por el dato que representa. Las variables están definidas de tres maneras: conceptual, operacional y experimental. Por lo que, de acuerdo con Sampieri (2020): “la definición conceptual o constitutiva es la acordada y validada por una comunidad científica o profesional. Generalmente estas definiciones se encuentran en diccionarios especializados, páginas electrónicas con respaldo institucional y publicaciones” (p. 87).

En cuanto a la definición de una variable operacional, Sampieri (2020) detalla lo siguiente: “constituye el conjunto de procedimientos que describe las acciones que un investigador debe realizar para recibir las impresiones sensoriales, las cuales indican la existencia de un concepto teórico en mayor o menor grado” (p. 88).

A continuación, se analizarán las variables en las cuales se estructura la propuesta, definiéndolas a nivel conceptual, operacional y experimental, partiendo desde los objetivos específicos.

Tabla 2

Cuadro de variables de la investigación

Objetivo Específico	**Variable**	**Variable Conceptual**	**Variable Experimental**	**Variable Operacional**
Investigar los programas educativos en los países líderes en ciberseguridad, Israel, Estados Unidos y Reino Unido.	Programas educativos internacionales	Un programa educativo es un documento que permite organizar y detallar un proceso pedagógico.	Guía de Observación	Observación
Analizar el Programa Nacional de Formación Tecnológica en el Sistema Educativo Costarricense y su enfoque en ciberseguridad.	Programa educativo nacional	Un programa educativo es un documento que permite organizar y detallar un proceso pedagógico.	Guía de Observación	Observación
Conocer los riegos y amenazas a las que están expuestos los jóvenes del Liceo de Pavas en el ciberespacio.	Riesgos y amenazas digitales	Según el sistema jurídico costarricense un riesgo: Probabilidad de que se presenten pérdidas, daños o consecuencias económicas, sociales o ambientales en un sitio particular y durante un periodo definido. Se obtiene al relacionar la amenaza con la	Guía de Encuestas	Encuestas

		vulnerabilidad de los elementos expuestos.		
Comprender los desafíos a los que se enfrentan los profesores y personal administrativo en materia de ciberseguridad.	Desafíos digitales	Comprensión de los desafíos y la brecha existente en las competencias a nivel de ciberseguridad en los decentes.	Guía de Encuestas	Encuestas
Identificar los mecanismos de prevención que deben implementarse por parte de los padres de familia para proteger a sus hijos de las amenazas cibernéticas.	Mecanismos de prevención	Según el diccionario de la RAE, prevención es la preparación y disposición que se hace anticipadamente para evitar un riesgo o ejecutar algo.	Guía de Encuestas	Encuestas
Determinar las brechas en seguridad de la información, activos y recursos educativos que existen en la institución.	Política en ciberseguridad	Según lo define IBM, la política de seguridad define qué es lo que se desea proteger y qué espera de los usuarios del sistema.	Guía de Entrevistas	Cuestionario

Fuente: elaboración propia, 2024.

Población

Según Sampieri (2017), la población se define como un: "conjunto de todos los casos que concuerdan con determinadas especificaciones y del cual se extrae la muestra" (p. 147). La

población delimita el conjunto de personas con sus características definidas de donde se obtiene la información necesaria que dará sustento e información para estructurar el proyecto de investigación.

En la presente propuesta, la población de estudio comprende tres grupos: el primero de ellos son todos los estudiantes activos del Liceo de Pavas, que cursan los años 7, 8, 9, 10 y 11; el segundo grupo es el personal docente y administrativo que labora para el Liceo de Pavas y el tercer grupo son los padres de familia de los estudiantes activos de 7, 8, 9, 10 y 11 de la institución.

Muestra

Sampieri (2020) indica que: "una muestra es un subgrupo de la población o universo que interesa, sobre el cual se recolectarán los datos pertinentes y debe ser representativo de la población estudiada (de manera probabilística, para que se generalicen los resultados encontrados en la muestra a la población o cualitativamente, para comenzar" (p. 128).

A continuación, se detallará la fórmula utilizada en poblaciones finitas, que se empleará para determinar el tamaño de la muestra.

Fórmula para calcular la muestra: K^2*(N*p*q) / (e^2(N-1)) + (K^2*(p*q))

n= tamaño de la muestra.
N= tamaño de la población.
K= nivel de confianza.
p= proporción esperada.
q= probabilidad de fracaso.
e= precisión (margen de error)

En el caso de la propuesta, la recolección de los datos para generar la muestra se realizará a través de tres grupos de control: estudiantes, padres de familia y docentes y personal administrativo, como lo menciona Sampieri (2020): "al determinar la unidad de muestreo o análisis apropiada, el interés se centra en "qué" o "quiénes", es decir, en los participantes, objetos, sucesos o situaciones del estudio, lo cual depende del planteamiento y los alcances de la investigación" (p. 129). Enseguida, se puntualizará en los cálculos realizados para determinar la muestra según corresponda.

En el caso de la muestra de los estudiantes, la población es de 1600, con un nivel de confianza del 90 % y un margen de error del 5 %, dado que no se conoce el valor de la proporción esperada y la probabilidad de fracaso, por lo que, se optará por una desviación estándar de 0,5, que garantizará que el tamaño de la muestra sea lo suficientemente grande, para obtener una muestra de 233 estudiantes.

En cuanto a los profesores y personal administrativo, la institución cuenta con 120 colaboradores, por lo tanto, se utilizará un nivel de confianza del 90 % y un margen de error del 5 %, dado que no se conoce el valor de la proporción esperada y la probabilidad de fracaso, ante esto se optará por una desviación estándar de 0,5 para una muestra de 84 personas.

Para realizar el cálculo de la muestra en padres de familia, se tomará como referencia una población de 200 personas, debido a que se desconocen variables como la cantidad de padres que tienen más de un hijo en la institución, el nivel de escolaridad y la disponibilidad para facilitar la información; por lo que, bajo este escenario se utilizará un nivel de confianza del 90 % y un margen de error del 5 %, dado que no se conoce el valor de la proporción esperada y la probabilidad de fracaso, así que se optará por una desviación estándar de 0,5, lo cual da una muestra de 116 padres de familia o encargados.

Instrumentos de Recolección de Datos

La recolección de datos dentro de una investigación radica en reunir y medir información de diversas fuentes, con la finalidad de obtener un panorama general del objeto de estudio. La obtención de estos datos puede realizarse a través de diferentes técnicas e instrumentos como la observación, cuestionarios, entrevistas, entre otros. En el caso de la propuesta se recopilarán datos por medio de encuestas, definidas para los diferentes grupos involucrados.

De acuerdo con Sampieri (2017), “un cuestionario es un conjunto de preguntas respecto a una o más variables que se van a medir. El contenido de las preguntas de un cuestionario es tan diverso como los aspectos que evalúa. Fundamentalmente, se consideran dos tipos de preguntas: cerradas y abierta” (p. 155). Según Hernández-Samperi (2017), las principales características que deben tener las preguntas son las siguientes:

- Claridad, precisión y ser comprensibles para quienes las responden.
- Deben evitarse términos amplios, confusos, ambiguos y de doble sentido.

- Brevedad, porque las preguntas largas se vuelven tediosas, tardan más tiempo y distraen al participante.
- **Sensibilidad:** pues no pueden incomodar a la persona encuestada ni hacerla sentir amenazada, además el entrevistado nunca debe sentir que se le enjuicia.
- **Neutralidad:** las preguntas no habrán de inducir las respuestas y se tienen que evitar preguntas tendenciosas.
- Es recomendable evitar preguntas que nieguen el asunto que se interroga.
- No deben hacerse preguntas racistas o sexistas, ni que ofendan o denigren a los participantes (p. 157).

Se utilizarán las encuestas como instrumento principal de recolección de datos, dado que permiten tener una respuesta precisa y general acerca de varios temas, sobre la información que se busca recabar y analizar. Al ser una muestra amplia, permite la masividad y facilita el muestreo, así mismo, por su característica facilita la tabulación de los datos y posterior análisis de estos.

En este estudio, se realizarán las encuestas que se encuentran en la sección de apéndices a los tres grupos de control: estudiantes (Apéndice A), padres de familia (Apéndice B) y docentes (Apéndice C). Los estudiantes se abordarán solicitando el apoyo de los profesores para que brinden un espacio durante las clases para completarlas y lograr la muestra necesaria. Además, se solicitará por medio del equipo administrativo, colaboración para brindar las encuestas a los profesores y con lo que respecta a los padres de familia o encargados, se le hará llegar por medio de los estudiantes.

Por lo que, con el fin de gestionar de manera correcta los datos y con la finalidad de cumplir con los principios de confidencialidad, integridad y disponibilidad, se elaborará una política de seguridad de la información para el Liceo de Pavas para proteger los activos y recursos educativos, ya que almacenan y procesan una gran cantidad de datos confidenciales, como registros de estudiantes, información sensible en temas disciplinarios o emocionales, información financiera, entre otros. Por lo tanto, para conocer la gestión que realiza la institución en esta materia, se realizará una entrevista a la encargada del centro educativo (Apéndice D).

CAPÍTULO IV. ANÁLISIS DE RESULTADOS

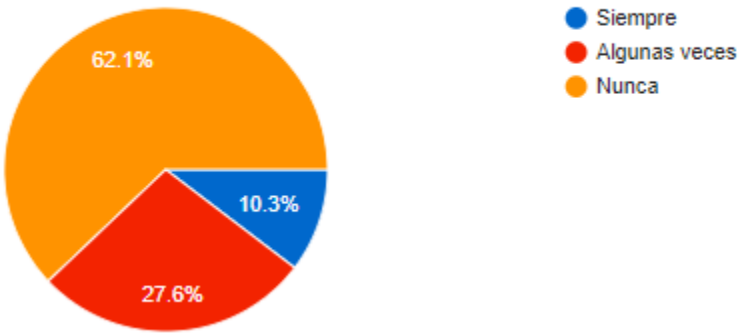
Se utilizaron las encuestas como parte de los instrumentos de recolección de datos, se aplicaron de forma diferenciada por cada grupo control: estudiantes, padres de familia y docentes;

estas arrojaron datos muy interesantes que fortalecen la razón de ser de la investigación y la propuesta, ya que revelan datos de la población en estudio, con respecto a las prácticas en el mundo digital y de la seguridad en línea.

Un dato muy relevante es que solo el 38 % de los docentes ha tenido conversaciones con sus estudiantes acerca de las actividades en redes sociales e internet, lo cual muestra una deficiente cultura acerca de instruir a los jóvenes en estos temas; adicionalmente, mencionan que un 27 % de sus estudiantes los han buscado para manifestarle que han sido víctimas de acoso en línea y aunque no es un porcentaje tan alto, las variables pueden estar ligadas, ya que no sienten la confianza de acudir a ellos, ya que no son un fuente de apoyo o instrucción en este tópico.

Figura 1.

Porcentaje de docentes que conversa con sus estudiantes acerca de las actividades en línea.



Fuente: elaboración propia, 2024.

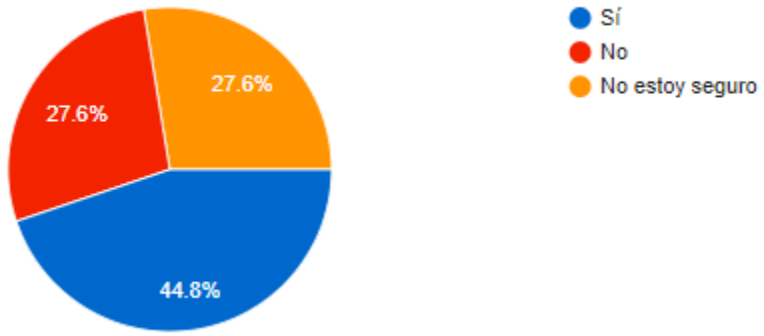
Otra conclusión importante es que el 38 % de los docentes no sabe que es un “virus”, “malware” o “código malicioso” y el 54 % no sabe cómo identificar cuando su celular o computadora tiene malware/código malicioso, este dato revelador muestra que existe desconocimiento en los profesores, lo cual es preocupante, ya que ellos deberían guiar a los jóvenes y ser facilitadores de conocimiento. Además, según los datos recopilados el 85 % de los docentes se conectan a redes wifi-públicas, exponiendo sus datos y dispositivos a las amenazas inherentes que conlleva este tipo de acciones, como interceptación de datos sensibles, malware, virus, entre otros riesgos de seguridad.

Otro dato interesante es el uso de las redes sociales y cómo esto está asociado a un tema generacional, los docentes mencionan que el 89 % usa Facebook, un 61 % Instagram y un 96 % WhatsApp como sus principales medios; el 54 % tiene alguna de sus redes como públicas y el 50 % de ellos, cuándo lee una noticia o artículo, no verifica la fuente, esto se asocia a la difusión de las famosas “fake news” y sus consecuencias, las cuales son muy delicadas, ya que debilitan y deterioran la credibilidad de los medios y ayudan al crecimiento de la desinformación.

Una de las preguntas realizadas con respecto al conocimiento de los derechos como usuarios de medios sociales y digitales, destaca que el 39% de los docentes tienen desconocimiento acerca del tema, lo cual es alarmante, ya que esto conlleva consecuencias como abuso, malas prácticas, fraudes, suplantación de identidad, desinformación y falta de control, al no existir el criterio suficiente para tomar acciones legales, en caso de existir un mal manejo de los datos personales por terceros; ante esto es fundamental conocer y ejercer estos derechos para protegerse de un entorno digital peligroso.

Figura 2.

Conocimiento de los docentes acerca de los derechos del uso de datos personales en medios digitales.



Fuente: elaboración propia, 2024.

En cuanto a los padres de familia, el 96 % es de género femenino; un 52 % ronda entre 31-40 años; un 37 % entre los 41-50 años y solo el 9% tiene la universidad completa, lo cual muestra una baja escolaridad y esto a su vez, se relaciona con carencias en temas de alfabetización digital.

Desde luego, el desconocimiento no se asocia con el género, pero si existe una brecha entre hombres y mujeres, en temas de educación, como lo menciona el estudio titulado: “Igualdad de Género en Costa Rica: Hacia una mejor distribución del trabajo remunerado y no remunerado”, publicado por la Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2024), este señala que las jóvenes costarricenses tienen menos probabilidades de estudiar en campos como tecnología e ingenierías, lo que se conoce como carreras STEM.

Un dato fundamental es el uso de las redes sociales, donde el 94 % de los padres de familia utiliza las mismas; un 50 % de ellos las utiliza más de una hora diaria; el 85 % usa Facebook; un 46 % Instagram y un 99 % utiliza la aplicación de mensajería WhatsApp. Estos números muestran la importancia de la educación en ciberseguridad en los padres de familia, ya que según la encuesta el 34 % comparte noticias o artículos con solo haber leído el título y un 66 % no verifica la fuente.

Otra conclusión importante es que el 58 % de los padres no sabe que es un “virus”, “malware” o “código malicioso” y el 74 % no sabe cómo identificar cuando su celular o computadora tiene malware/código malicioso; por lo que, al igual que los docentes este dato muestra que existe desconocimiento en este tema, lo cual es un portillo para padres y jóvenes, ya que carecen de medidas y acciones para evitar estas amenazas. Adicionalmente, según los datos recopilados el 42 % de los padres se conectan a redes wifi-públicas, exponiendo sus datos y dispositivos a las diferentes amenazas cibernéticas.

Entre los resultados más importantes de la encuesta realizada a los padres, se detalla que solo 45 % establece límites de tiempo y uso a sus hijos en redes sociales, mientras más de la mitad de ellos no ejerce ningún tipo de supervisión en los jóvenes. El 52 % de los padres mencionaron que sus hijos no reciben orientación en el colegio sobre los peligros a los que están expuestos al navegar en internet o redes sociales, estos números no muestran como muchos de ellos no poseen ningún tipo de restricción en cuanto a temas digitales por parte de los actores formativos, es decir, padres y docentes.

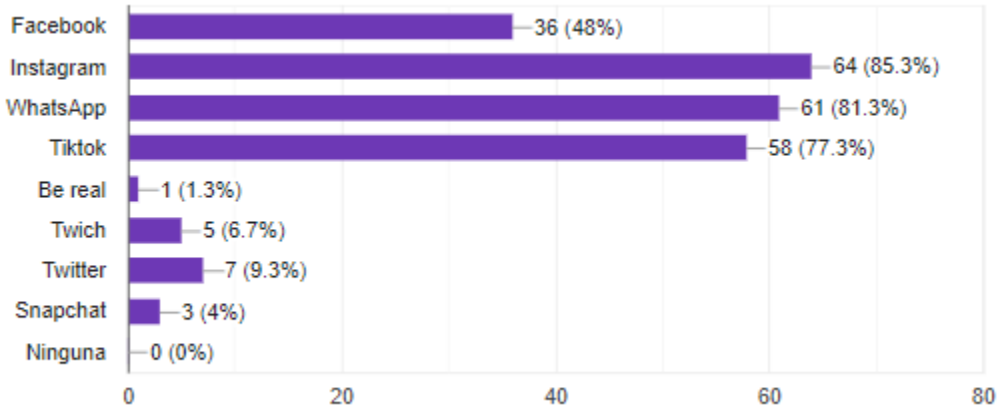
En cuanto al conocimiento en temas de los derechos que como usuario tienen solo el 55 % comprende del tema, pero evaluando las métricas anteriores existe cierta contradicción, ya que ejercen acciones que los colocan en vulnerabilidad en el ecosistema digital.

En cuanto a los estudiantes, el 82 % destina más de una hora en redes sociales, la distribución de uso es del 43 % en Facebook, un 85 % en Instagram y el 75 % en TikTok a su vez, el 80 % utiliza WhatsApp como aplicación de mensajería, por lo que, es interesante que en padres

y docentes la aplicación de mayor uso es Facebook, pero las principales redes que usan los adolescente son Instagram y TikTok, lo cual colabora al desconocimiento en temas de seguridad en línea de ciertas aplicaciones y hace que los jóvenes se encuentren más expuestos y vulnerables por la ausencia de instrucción.

Figura 3.

Redes sociales más utilizadas por los jóvenes del Liceo.

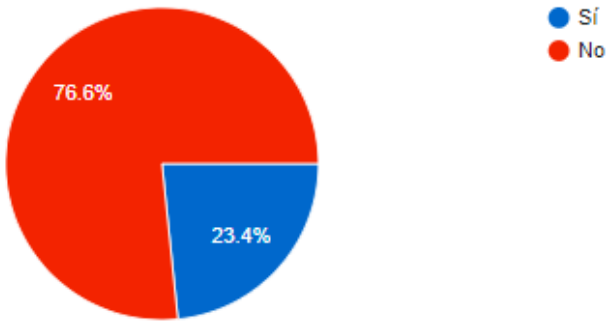


Fuente: elaboración propia, 2024.

Siguiendo con el tema de las redes sociales, el 20 % de los jóvenes tiene alguna de sus redes como públicas y el 72 % acepta o sigue a desconocidos, sumado a este dato que el 27 % ha recibido contenido explícito como fotos, videos o audios sin su consentimiento y el 21 % menciona haber sido víctima de ciberacoso, por lo tanto, estos datos permiten entender la exposición a la que se encuentran los adolescentes y que los lleva a ser víctimas de amenazas, como ciberacoso, sexting, grooming, publicación de información privada, entre otras.

Figura 4.

Porcentaje de estudiantes que dice haber sido víctimas de ciberacoso.

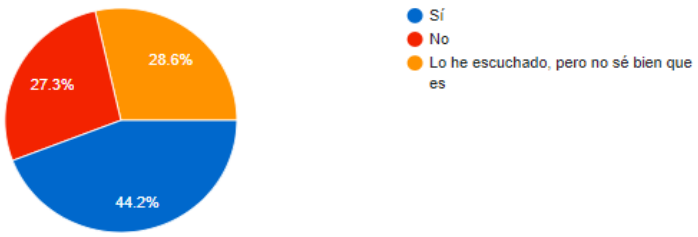


Fuente: elaboración propia, 2024.

El 56 % de los jóvenes no sabe que es un “virus”, “malware” o “código malicioso” y el 62 % desconoce cómo identificar cuando su celular o computadora tiene malware/código malicioso. Adicionalmente, según los datos recopilados, el 70 % se conectan a redes wifi-públicas, exponiendo sus datos y dispositivos a las diferentes amenazas cibernéticas, ya que el 38 % considera que estar conectado a una red wifi pública no representa un riesgo y el 59 % guarda sus contraseñas en una libreta/hoja suelta/cuaderno, en el correo electrónico o en las notas del celular. Por lo que, estos datos brindan una perspectiva de la realidad de muchos de los jóvenes que carecen de conocimiento en temas de seguridad de la información.

Figura 5.

Porcentaje de estudiantes que tiene conocimientos en amenazas cibernéticas.



Fuente: elaboración propia, 2024.

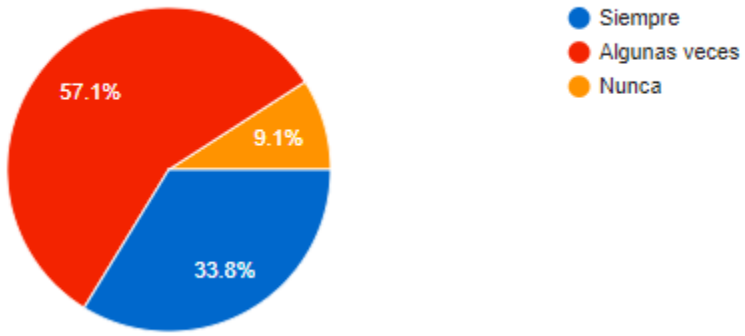
En cuanto a temas de supervisión y formación por parte de sus padres o docentes, el 66 % menciona que sus profesores no le brindan información sobre los riesgos o prevenciones que deben

tomar en cuenta, cuando usan las redes sociales o plataformas digitales y el 49 % menciona que sus padres no le brindan información sobre este mismo tema.

Lo anterior, refuerza la carencia en temas de educación y de seguridad en línea y como muchos de los jóvenes costarricenses se encuentran desprotegidos por la falta de formación por parte de sus mentores, ya sea en casa o en la institución.

Figura 6

Formación que reciben los jóvenes por parte de los profesore acerca de los riesgos en línea.



Fuente: elaboración propia, 2024.

Como parte de la propuesta se elaborará una Política de Ciberseguridad para el Liceo de Pavas, con el fin de proteger los activos y recursos educativos, ya que en estos se almacenan y procesan una gran cantidad de datos confidenciales, como registros de estudiantes, información sensible en temas disciplinarios o emocionales, información financiera, entre otros. Estos datos suelen ser el objetivo de ciberdelincuentes, piratas informáticos o personas internas maliciosas que buscan robarlos, manipularlos o destruirlos con diversos fines, como extorsión, espionaje o sabotaje.

Para esto se realizó una entrevista a la encargada de la institución y se le preguntó, si existía algún control para el acceso de personas no autorizadas a las instalaciones, ella mencionó que solo se solicita la cédula y dependiendo del colaborador de seguridad no se cuestiona a quien desee ingresar, lo cual puede traducirse en un impacto en los activos y la información del liceo.

Por otro lado, se le preguntó, la manera de almacenamiento y procesamiento de los datos de los estudiantes y sus familias por parte del personal docente y administrativo y el encargado mencionó que todo se lleva de manera manual, con expedientes físicos y a nivel interno nada se lleva de manera digital. La información financiera se lleva de igual manera, por medio de libros de y un contador público, por lo que, no hay un control riguroso de las finanzas internas, incluso actualmente existe un proceso legal de investigación, ya que la junta de administración anterior realizó malos manejos del dinero y se les solicitó la renuncia.

También se le consultó acerca de la persona que se encarga del mantenimiento de los equipos y la red, la respuesta fue que se realizan contrataciones a terceros y que estos a su vez, no cuentan con ningún tipo de restricción y tienen acceso total a los equipos que pertenecen al centro educativo, en cuanto a la red, por lo que, existe una pública para los estudiantes e invitados y una privada para el personal docente y administrativo; además, en cuanto a controles de las contraseñas de red, no se cuenta con ningún nivel de complejidad y la encargada de accesos es la directora.

La institución cuenta con equipos de cómputo solo para el personal administrativo y las aulas de informática, por lo que, los docentes que deseen hacer uso de algún medio digital deben ser proporcionados por ellos mismos; en el caso de los equipos del área administrativa del liceo, la encargada menciona que cuentan con contraseñas de acceso muy básicas, las cuales tienen apuntadas en una libreta y en cuanto a los laboratorios cumplen el mismo patrón, por ejemplo: “Estudiante123”.

Los programas o sistemas de información utilizados en la institución son el paquete de office para temas varios y la plataforma “Saber”, la cual es proporcionada por el MEP para el control global de notas y algunos indicadores de evaluación. Las computadoras institucionales no cuentan con ningún tipo de respaldo, ya sea físico o en la nube, por lo que, si un equipo se daña, se pierde toda la información almacenada, además solo se cuenta con el antivirus que tiene integrado Windows y no se realizan actualizaciones periódicas, por lo tanto, no contienen mecanismos de seguridad adicionales.

Se le consultó acerca de los equipos del laboratorio y de los controles que se ejecutan para el acceso a contenido inadecuado por parte de los estudiantes o hasta incluso de los profesores y se menciona que no existen restricciones en ese sentido y no se ejecutan medidas para filtrar el contenido, por lo tanto, se tiene acceso ilimitado, lo cual se traduce en una serie de riesgos y amenazas para los jóvenes.

En cuanto al uso del correo en el personal docentes y administrativo, se hace uso de la cuenta institucional del MEP, pero menciona que muchos de los docentes utilizan sus cuentas personales para enviar comunicados, lo cual implica en caso de ser vulnerado, convertirse en un riesgo a la privacidad y al manejo de los datos personales de los estudiantes.

Por último, se le realizó la consulta del manejo y control de las redes sociales de la institución y la encargada menciona que solo hay tres personas con accesos y permisos para publicar información en el muro, las cuales son la jefe técnica del Departamento de orientación, la subdirectora y un auxiliar.

CAPÍTULO V. PROPUESTA

Como se detalló en capítulos anteriores, para realizar el desarrollo de la propuesta se analizaron los programas educativos de países líderes en este tema como los son Israel, Reino Unido y Estados Unidos. Israel es un referente mundial en ciberseguridad y sus programas de formación en primaria y secundaria no son la excepción, puesto que promueven planes de alfabetización digital desde edades tempranas e incluso en los últimos años de secundaria brindan la posibilidad de formar parte de programas de enseñanza en materias tecnológicas de alto nivel, con el fin de abordar la creciente demanda de expertos en ciberseguridad.

El gobierno de los Estados Unidos a través de sus programas de formación en ciberseguridad en edades tempranas impulsa el desarrollo de las habilidades técnicas necesarias para identificar y mitigar amenazas cibernéticas, así como el pensamiento crítico en este tema. Uno de los propósitos principales es promover entre los estudiantes de primaria y secundaria, la identificación de oportunidades profesionales en el campo de la ciberseguridad.

Por su parte, el Reino Unido, por medio de sus programas de educación en ciberseguridad, principalmente en jóvenes de secundaria, se enfocan en la enseñanza en temas fundamentales como: la detección de amenazas, la privacidad en línea y la protección de datos personales, con el fin de prepararlos para ser ciudadanos digitales responsables.

En Costa Rica, en este año 2024 se comenzó a implementar el Programa Nacional de Formación Tecnológica del MEP, con el propósito principal de alfabetizar a los jóvenes de los centros educativos públicos en temas digitales, abordando de una manera muy diluida los diferentes conceptos de ciberseguridad; además este tema ha dejado muchas dudas, ya que la adopción de dicho programa no ha sido una tarea fácil, debido a que el programa abarca muchos temas de estudio distribuidos en las 4 áreas definidas y lamentablemente, se asigna un área por institución.

La propuesta nace como una respuesta a la necesidad que tiene la población del Liceo de Pavas en temas de formación en ciberseguridad, los cuales pertenecen a una zona socioeconómica vulnerable y que en su mayoría, están expuestos a una serie de amenazas y riesgos. Según el Departamento de orientación, el 80 % de los conflictos de la población estudiantil del colegio son producto del mal uso de la tecnología o de las redes sociales, por lo que, estos medios son detonantes de violencia y agresión física o verbal.

La jefa del Departamento de orientación, Susan Sánchez menciona que: “el mal uso que le dan los estudiantes del colegio a la tecnología ha colaborado para que se den casos de envíos de imágenes o videos con una connotación sexual y sin ningún tipo de precaución en temas de

privacidad, que luego son usados por los mismos estudiantes para exponer a otros y para ser difundidos, también toman fotos sin permiso para hacer *sticker,* con el fin de cometer *bullying*" y señala que esto se agrava, ya que en la etapa de la adolescencia no existe una consciencia desarrollada y sumado al desconocimiento del tema, los lleva a cometer acciones imprudentes.

Ante este panorama, el proyecto se enfoca en generar los insumos para incentivar la formación en fundamentos en ciberseguridad, con el fin de educarlos para que sean ciudadanos informados, integrando a todos los actores del proceso educativo como lo son: estudiantes, profesores, personal administrativo y a los padres de familia. También se realizará la elaboración de una política de seguridad de la información, con el fin de proteger los activos y recursos educativos de la institución.

Guía de Ciberseguridad para Estudiantes del Liceo de Pavas

Se elaboró una guía de contenido en conceptos y fundamentos en materia de ciberseguridad para los estudiantes de décimo y undécimo año del Liceo de Pavas. Esta será impartida por medio del programa diseñado que lleva por nombre "Ciber Embajadores" en el cual, los estudiantes de décimo y undécimo que sean formados en materia de ciberseguridad serán los encargados de transmitir los conocimientos adquiridos a la comunidad estudiantil de sétimo, octavo y noveno año, fomentando el aprendizaje activo y al mismo tiempo, educando a los más jóvenes en materia de ciberseguridad para prepararlos en el transitar por el mundo digital.

Los estudiantes de décimo y undécimo deben cumplir con un requisito del Ministerio de Educación Pública, el cual consiste en hacer 30 horas de servicio comunal; como parte de las opciones que se les brindará será participar del programa de "Ciber Embajadores", que con el apoyo del personal de orientación y los profesores de tecnología se dará seguimiento y guía para la ejecución de este.

El propósito es que los estudiantes puedan dedicar 10 horas al estudio de las guías apoyados con un tutor y las 20 horas restantes sean usadas para que ellos impartan sus conocimientos a los estudiantes de séptimo, octavo y noveno. El contenido visual de la guía se muestra en el Apéndice E, a continuación, se detallará la estructura de esta:

Capítulo 1. Fundamentos de Ciberseguridad

- Concepto de "ciudadanía digital": ser un usuario responsable y respetuoso en línea.
- ¿Qué es la ciberseguridad y por qué es importante?
- Amenazas más comunes: *phishing*, *malware* y robo de identidad.

Capítulo 2. Riesgos en Línea

- Principales riesgos a los que se enfrentan los jóvenes en línea: *ciberbullying, grooming, sexting, fake news y publicación de información privada.*
- Mecanismos utilizados para engañar a los jóvenes.
- ¿Cómo evitar ser víctima de engaños?

Capítulo 3. Protección de Datos Personales

- Creación de contraseñas seguras.
- ¿Cómo manejar la privacidad en redes sociales?
- ¿Cómo proteger tus dispositivos personales?
- Consejos para una navegación segura.

Capítulo 4. Protección Legal en el Mundo Digital

- Introducción a las leyes sobre delitos informáticos y protección de datos.
- Consecuencias legales de participar en prácticas ilícitas en línea.

Capítulo 5. Habilidades para la Vida

- Beneficios de estudiar ciberseguridad.
- ¿Qué son las habilidades blandas y sus beneficios?
- ¿Cómo desarrollar la comunicación interpersonal, la resolución de problemas y el autocontrol?

Capítulo 6. Desafíos de Ciberseguridad

- Ejercicios y simulaciones de escenarios en los cuales, poner en práctica lo aprendido.

Guía de Ciberseguridad para Padres de Familia del Liceo de Pavas

Se desarrolló una guía de formación básica para los padres de familia del Liceo de Pavas, con el fin de educarlos para que sean ciudadanos informados y puedan orientar y supervisar a sus hijos, aplicando controles parentales, así como que sean capaces de brindar conocimiento de las diversas amenazas en línea en las que están expuestos los jóvenes en la actualidad.

Los encargados de implementar e impartir los conocimientos serán los profesores de tecnología, apoyados por el equipo de orientación, que enviarán las guías a los padres de familia y reforzarán conocimientos en las reuniones trimestrales que realizan con ellos. El contenido visual de la guía se muestra en el Apéndice F, a continuación, se detallará la estructura de esta:

Capítulo 1. Entendiendo el Mundo Digital

- ¿Qué es internet y cómo funciona?
- ¿Cómo usan internet mis hijos y su importancia?
- ¿Qué es la ciberseguridad y la importancia en la vida de los jóvenes?
- Principales amenazas en línea: phishing, malware y robo de identidad.
- Principales riesgos a las que se enfrentan los jóvenes: *ciberacoso, sexting, grooming, publicación de información privada y fake news.*
- Plataformas y dispositivos utilizados por los jóvenes para navegar.

Capítulo 2. Educando a Nuestros Jóvenes para un Futuro Seguro

- Aprendamos acerca de contraseñas seguras.
- ¿Cómo proteger los dispositivos personales de nuestros hijos?
- Manejo de la privacidad en las redes sociales.
- Importancia del uso de controles parentales.

Capítulo 3. Protegiendo a Nuestros Jóvenes de los Riesgos en Línea

- ¿Qué hacer si sus hijos sufren violencia en línea?
- Leyes que protegen a los jóvenes en el entorno digital.
- Consejos para educar jóvenes responsables en el entorno digital.

Guía de Ciberseguridad para Profesores y Personal Administrativo de Liceo de Pavas

Se elaboró una guía de formación en conceptos fundamentales en ciberseguridad para los docentes y personal administrativo del Liceo de Pavas, con el fin de dotarlos de herramientas que les permita tener un papel formativo en los estudiantes, ya que es determinante que los profesores conozcan de los riesgos a los que se expone la juventud en el mundo digital y puedan detectar, evitar y abordar posibles casos de ciberacoso, estafas, robo de identidad, fraude en línea, desinformación, así como leyes y normas.

Los encargados de impartir estas guías serán los profesores de tecnología y el personal de orientación, los cuales la institución eligió para este fin, ya que están facultados con las capacidades necesarias para incentivar a sus compañeros en la formación en temas de ciberseguridad, adicionalmente se hará uso de las reuniones mensuales de docentes para la ejecución de esta tarea.

El contenido visual de la guía se muestra en el Apéndice G, a continuación, se detallará la estructura de esta:

Capítulo 1. La Ciberseguridad y la Educación

- La ciberseguridad y su importancia en el rol de docente.
- Formas de interactuar por los adolescentes en el mundo digital.
- Respeto, ética y responsabilidad en línea.

Capítulo 2. Riesgos y Amenazas en el Entorno Digital

- Principales amenazas en línea: phishing, malware, robo de identidad.

- Riesgos a las que se enfrentan los jóvenes: *ciberacoso, sexting, grooming, publicación de información privada, fake news.*

Capítulo 3. Protección de Dispositivos y Datos Personales

- Crear y gestionar contraseñas seguras.
- ¿Cómo proteger sus dispositivos personales?
- Manejo de la privacidad en las redes sociales.
- Leyes que protegen a los jóvenes en el entorno digital

Capítulo 4. Fomentando el Interés en Carreras en Ciberseguridad

- Papel que juegan los docentes en fomentar el interés por las carreras tecnológicas.

Política de Seguridad de la Información para el Liceo de Pavas

Se desarrolló una Política de Seguridad de la Información para el Liceo de Pavas con el fin de proteger los activos y recursos educativos, esta institución almacena y procesa una gran cantidad de datos confidenciales, como registros de estudiantes, información sensible en temas disciplinarios o emocionales, información financiera, entre otros. Estos datos suelen ser el objetivo de ciberdelincuentes, piratas informáticos o personas internas que buscan robarlos, manipularlos o destruirlos con diversos fines maliciosos, como extorsión, espionaje, sabotaje.

Para estructurar la política se tomará como referencia la norma ISO/IEC 27002:2022, la cual proporciona un conjunto de mejores prácticas y controles en temas de seguridad de la información y ciberseguridad, adicionalmente se usó como referencia la Política en Tecnologías de la Información (2020), del Ministerio de Educación Pública, la cual busca garantizar la protección, la confidencialidad, la integridad y la disponibilidad de la información. El contenido visual de la política se muestra en el Apéndice H, a continuación, se mencionarán los lineamientos que contiene la Política de Seguridad de la Información para el Liceo de Pavas:

Lineamiento para la gestión y control de accesos físicos

El lineamiento para la gestión y control de accesos físicos busca establecer procedimientos que regulen el acceso a la institución educativa. Con el fin de proteger los activos de información, y garantizar que solo el personal autorizado pueda ingresar a las instalaciones, con el objetivo de minimizar amenazas a la seguridad de la información y los recursos educativos. Para establecer los procedimientos que regulen este aspecto se usó como referencia, el manual: *Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información,* de la norma ISO/IEC 27002:2022, y se adaptó a las necesidades y recursos de la institución educativa.

Para estructurar este lineamiento se utilizó la sección de controles físicos, específicamente en los apartados: *Entrada física, Aseguramiento de oficinas, salas e instalaciones y Supervisión de la seguridad física*, en los cuales se detallan todos los aspectos necesarios para garantizar la seguridad física de las instalaciones y los activos de información, con el fin de restringir y controlar el acceso a ciertas áreas a través de sistemas de autenticación, tarjetas de acceso, y medidas de seguridad física como el uso de cerraduras electrónicas y cámaras de vigilancia, asegurando que solo el personal autorizado pueda ingresar.

Lineamiento de protección de información sensible

El lineamiento para la protección de información sensible procura establecer normas para la recolección, almacenamiento y manejo adecuado de los datos personales de los estudiantes y sus familias, así como de los docentes y administrativos. Con el fin de garantizar la seguridad y confidencialidad de la información. Para establecer los procedimientos que regulen este aspecto se usó como referencia, el manual: *Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información,* de la norma ISO/IEC 27002:2022, y se adaptó a las necesidades y recursos de la institución educativa.

Para desarrollar este lineamiento se utilizó la sección de controles organizacionales, en el apartado: *Clasificación de la información*, en este se describen como implementar procedimientos para clasificar la información en categorías según su nivel de sensibilidad y riesgo, lo que facilita la aplicación de controles específicos a cada tipo de dato, adicionalmente, definir políticas que detallen cómo debe protegerse cada categoría de información, incluyendo requisitos para su almacenamiento, procesamiento y transmisión segura.

Lineamiento para la gestión de redes seguras

El lineamiento para la gestión de redes seguras tiene como objetivo garantizar que las redes informáticas de la institución educativa funcionen de manera confiable y segura. Se busca prevenir el acceso no autorizado, proteger los recursos tecnológicos y la información sensible, además de asegurar la disponibilidad de la red para los usuarios autorizados. Para establecer los procedimientos que regulen este aspecto se usó como referencia, el manual: *Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información,* de la norma ISO/IEC 27002:2022, y se adaptó a las necesidades y recursos de la institución educativa.

El desarrollo de este lineamiento se fundamentó en la sección de controles tecnológicos, en concreto los apartados: *Seguridad en redes, Seguridad de los servicios de red y Segregación de redes*, en los cuales se mencionan los procedimientos para ejecutar los controles correspondientes, con el fin de asegurar la autenticación y el monitoreo de acceso a la red, así como segmentación de redes y políticas de acceso restringido, lo que reduce el riesgo de ataques internos y externos.

Lineamiento para la gestión de los equipos y antivirus

El lineamiento para el mantenimiento de los equipos y antivirus tiene la finalidad de garantizar que todos los equipos informáticos funcionen de manera óptima. Ejecutando mecanismos para el mantenimiento preventivo del hardware y el software, con el fin de evitar fallas en los equipos, y protegerlos contra amenazas o riesgos cibernéticas Para establecer los procedimientos que regulen este aspecto se usó como referencia, el manual: *Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información,* de la norma ISO/IEC 27002:2022, y se adaptó a las necesidades y recursos de la institución educativa.

Para construir este lineamiento se utilizó la sección de controles tecnológicos, en los apartados: *Protección contra malware, Instalación de software en sistemas operativos*, en estos se detallan recomendaciones para la implementación de soluciones de seguridad, como software antivirus y sistemas de detección de amenazas, para identificar, prevenir y mitigar el malware. Además, se sugieren políticas de actualización y análisis periódicos para detectar software malicioso.

Lineamiento para la gestión de contraseñas seguras

El lineamiento para la gestión de contraseñas seguras pretende establecer reglas y recomendaciones que ayudan a fortalecer la seguridad de las contraseñas; además, busca garantizar la actualización periódica y el almacenamiento seguro de contraseñas. Para establecer los procedimientos que regulen este aspecto se usó como referencia, el manual: *Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información,* de la norma ISO/IEC 27002:2022, y se adaptó a las necesidades y recursos de la institución educativa.

El desarrollo de este lineamiento se basó en la sección de controles tecnológicos, en el apartado: *Restricción de acceso a la información*, este detalla pautas a seguir en temas de autenticación y autorización y el uso de políticas estrictas que determinen quién puede acceder a qué información, así como la implementación de métodos seguros de autenticación, como contraseñas robustas, autenticación multifactor y procedimientos de gestión de credenciales para evitar accesos no autorizados.

Lineamiento de respaldo de datos

El lineamiento para la protección de información sensible tiene como objetivo establecer mecanismos para proteger la información y garantizar su disponibilidad en caso de pérdida, daño o corrupción. Para establecer los procedimientos que regulen este aspecto se usó como referencia, el manual: *Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información,* de la norma ISO/IEC 27002:2022, y se adaptó a las necesidades y recursos de la institución educativa.

Para estructurar este lineamiento se utilizó la sección de controles tecnológicos, en el apartado: *Copia de seguridad de la información*, en el cual se menciona la implementación de políticas claras que establezcan la frecuencia, el alcance y los tipos de datos que deben respaldarse regularmente, así como mantener los registros de las copias de seguridad y monitorizar los procesos para asegurar su cumplimiento y detectar cualquier anomalía.

Lineamiento de gestión de terceros

El lineamiento para la gestión de terceros procura establecer normas que regulen las relaciones con terceros o proveedores, implementando mecanismos para identificar, evaluar y mitigar los riesgos y amenazas en los recursos educativos y tecnológicos del liceo, realizando acuerdos de confidencialidad con los proveedores que tengan accesos a los activos del centro educativo. Para establecer los procedimientos que regulen este aspecto se usó como referencia, el manual: *Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información,* de la norma ISO/IEC 27002:2022, y se adaptó a las necesidades y recursos de la institución educativa.

La construcción de este lineamiento se basó en la sección de controles organizacionales, específicamente en los apartados: *Seguridad de la información en las relaciones con los proveedores y Abordar la seguridad de la información en los acuerdos con proveedores*, se estos se detalla acerca del establecimiento de acuerdos que incluyan cláusulas de seguridad de la información, en donde se definan aspectos referentes a la protección de datos, acceso restringido y confidencialidad de la información. También se recomienda el uso mecanismos para monitorear y revisar el cumplimiento de los acuerdos de seguridad por parte de los proveedores, adaptando los controles según los cambios en el riesgo.

Lineamiento para el uso de controles de filtrado web

El lineamiento para el uso de controles de filtrado web busca establecer normas que permitan a los educadores supervisar y orientar el uso de los recursos tecnológicos del centro educativo por parte de los estudiantes, con el fin de restringir el acceso a material inapropiado. Para establecer los procedimientos que regulen este aspecto se usó como referencia, el manual *Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información,* de la norma ISO/IEC 27002:2022, y se adaptó a las necesidades y recursos de la institución educativa.

Para construir este lineamiento se utilizó la sección de controles tecnológicos, específicamente en el apartado: *Filtrado web*, en el cual se realizan recomendaciones de establecimiento de políticas con el objetivo de limitar el acceso a páginas web que puedan representar riesgos de seguridad o contenido inapropiado.

Lineamiento para la gestión de las redes sociales

El lineamiento para la gestión de las redes sociales tiene como objetivo establecer normas que regulen el uso de las plataformas digitales, con el fin garantizar el uso responsable del contenido que publican en las redes sociales. Además, se pretende resguardar la reputación del centro educativo y controlar la información personal de estudiantes y docentes que se publique.

Si bien es cierto en la norma ISO/IEC 27002:2022, no hay un apartado que detalle específicamente algo sobre las redes sociales, se tomaron como referencia los apartados mencionados anteriormente en cada uno de los lineamientos y se desarrolló una serie de recomendaciones que se apegan al uso y tratamiento de la información, así como la gestión y control de accesos y autenticación, y la asignación de responsables.

CAPÍTULO VI. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Se analizaron los esfuerzos realizados a nivel internacional, específicamente en Israel, Estados Unidos y Reino Unido y se refleja un enfoque integral en términos de educación en ciberseguridad para los jóvenes, adaptados según el enfoque educativo de cada país. En Israel, la educación en ciberseguridad se orienta hacia la formación de ciudadanos con habilidades defensivas que sirvan a la nación, mientras que el Reino Unido se enfoca en construir una fuerza laboral preparada para enfrentar los desafíos de la ciberseguridad del futuro. Por su parte, Estados Unidos está adoptando un enfoque desde los niveles básicos de la educación, incentivando la participación activa de estudiantes, educadores y comunidades en la concientización y el desarrollo de competencias cibernéticas.

Este análisis demuestra la importancia de la colaboración entre gobierno, instituciones educativas y la comunidad para cultivar una cultura de ciberseguridad sólida, que permita a las nuevas generaciones proteger y mejorar su entorno digital. Estos modelos internacionales sirven como ejemplo para el emular sus enfoques y esfuerzos, con el fin fortalecer las habilidades en ciberseguridad de los jóvenes costarricenses.

Este año, el Ministerio de Educación Pública puso en práctica el Programa de Formación Tecnológica en el Sistema Educativo Costarricense, el cual consiste en dotar a los jóvenes de colegios públicos de conocimientos tecnológicos en diferentes aspectos, pues si bien la malla curricular contiene aspectos relevantes, en el Liceo de Pavas se presentan algunas fallas en su ejecución y no se cuentan con los recursos tecnológicos para ponerlo en marcha de una manera óptima. Adicionalmente, los temas en ciberseguridad se abordan de una manera transversal y se diluyen, disminuyendo el protagonismo que realmente debería tener en la formación de los jóvenes.

La presente investigación revela una preocupante carencia de conocimientos básicos y prácticas seguras en ciberseguridad entre los jóvenes del Liceo de Pavas. A pesar de que la mayoría de los adolescentes dedica más de una hora diaria a redes sociales y se consideran nativos digitales, desconocen términos como “virus” o “malware”, adicional a esto carecen del conocimiento para identificar cuando han sido atacados por una amenaza cibernética; esto se agrava por la falta de supervisión y educación, pues no se abordan estos temas en los hogares y ni en las aulas.

Por otro lado, los jóvenes aceptan o siguen a desconocidos en sus perfiles de Redes Sociales, por lo que, abren la puerta a situaciones potencialmente peligrosas, ya que muchos de ellos han recibido contenido explícito por medio de fotos, videos o audios, sin su consentimiento. Aunado a lo anterior, una cantidad importante de los estudiantes mencionan haber sido víctimas de ciberacoso. Es por esto, por lo que, existe una apremiante necesidad de educación y capacitación en ciberseguridad, ya que los estudiantes señalan que sus padres y profesores no les brindan información sobre los riesgos o prevenciones que deben tomar cuando hacen uso de redes sociales o plataformas digitales.

Por otro lado, los resultados reflejan una preocupante falta de preparación en temas de ciberseguridad tanto en docentes como en padres de familia, quienes juegan un papel fundamental en la orientación de los jóvenes en cuanto al uso seguro de la tecnología. Esta realidad destaca una desconexión entre las generaciones, donde los adultos carecen de las competencias digitales para educar, orientar y proteger a los adolescentes en el entorno digital.

Existe una notable disparidad generacional en la preferencia del uso de redes sociales, lo que plantea serias implicaciones en la educación sobre ciberseguridad. Esta diferencia señala un cambio en las dinámicas de comunicación, por lo que, resulta fundamental fortalecer la preparación de padres y docentes en temas de ciberseguridad y fomentar un diálogo abierto con los jóvenes, con el fin de reducir los riesgos digitales y promover un entorno más seguro y responsable para los estudiantes del Liceo de Pavas.

Hay también una alarmante falta de límites y orientación en el uso de la tecnología por parte de los jóvenes, esto porque menos de la mitad de los padres establece restricciones sobre el tiempo y la manera en que sus hijos utilizan las redes sociales, lo que sugiere una falta de conciencia sobre los riesgos asociados con la exposición prolongada y descontrolada a estas plataformas. Así mismo, los profesores no les brindan una guía significativa en este sentido. Esta carencia de límites en el hogar y la falta de educación formal sobre ciberseguridad no solo deja a los jóvenes vulnerables ante todas las amenazas que pueden darse en el mundo digital, sino que también promueve un ambiente donde el autocontrol es escaso.

Ante este panorama, la propuesta de formación tiene como objetivo, proporcionar a los padres y docentes herramientas y conocimientos específicos sobre las aplicaciones que utilizan los estudiantes fomentando una comunicación más efectiva y un ambiente de confianza. Esto permitirá a los adultos involucrarse activamente en la educación digital de los jóvenes, ayudándoles a

navegar por el ciberespacio de manera más segura y consciente. Por lo tanto, una comunidad educativa informada y capacitada no solo protegerá a sus miembros de los riesgos cibernéticos, sino que también impulsará un entorno en el que los jóvenes puedan desarrollar habilidades para el futuro.

Por otro lado, al ser una propuesta integral, se realizó un análisis del estado de la institución educativa en términos de seguridad de la información, se determinó que el liceo no cuenta con aspectos mínimos en temas de seguridad de la información, carece de la ejecución de buenas prácticas, lo cual lo convierte en un blanco fácil y los hace vulnerables, poniendo en riesgo sus activos tecnológicos y digitales. Además, la falta de políticas de control de accesos físicos y tecnológicos, así como la ausencia de gestión en los equipos y antivirus, se convierten en una puerta abierta, comprometiendo los datos sensibles de la institución.

La implementación de un programa de formación en ciberseguridad para la población del Liceo de Pavas representa una solución vital para abordar las debilidades identificadas en el manejo de la tecnología, dada la falta de preparación y conocimiento sobre los riesgos digitales entre docentes, padres y estudiantes. Por lo que, a través de la educación y la concientización, se podrá promover un uso más responsable y seguro de las tecnologías, garantizando una mejor protección para los jóvenes.

Finalmente, es un esfuerzo conjunto, pues tanto la institución educativa como: los docentes, alumnos y padres de familia, deben trabajar triangularmente para construir un futuro digital seguro. Por lo tanto, al tomar acciones proactivas, no solo se protege la información importante, sino que también se educa y empodera a las futuras generaciones.

Recomendaciones

Los padres de familia son la primera línea de defensa para la protección de los adolescentes en el ciberespacio, pues en el hogar se cultivan los valores, deberes y modales con los que saldrán los jóvenes al mundo, por esto su papel como guías, cuidadores y protectores es protagonista.

Ante esta realidad es vital promover una cultura de límites claros sobre el uso de dispositivos y redes sociales en casa y acá es donde las guías toman protagonismo, debido a que estas, han sido creadas y pensadas para que su vocabulario sea de fácil entendimiento para dicha

población, buscando facilitar su propagación y uso como herramienta principal para formar a los padres en estos temas.

Adicionalmente, se propone utilizar las reuniones de entregas de notas, así como la escuela para padres, para fomentar discusiones abiertas sobre el uso de la tecnología y los límites en el hogar, pues esto podría ser parte de un diagnóstico institucional de necesidades y permitiría la sensibilización acerca de los temas de ciberseguridad, así como también una actualización constante a los padres y/o cuidadores.

Por lo que, resulta de vital importancia la capacitación pronta de los docentes, pues vienen a formar una segunda línea de defensa no solo al ser quienes apoyan la educación y brindan asesoría e información a los estudiantes, sino que también vienen a ser escudos protectores que robustecen la política de ciberseguridad de la institución. De ahí, la importancia de su involucramiento y capacitación constante para mantenerse actualizados antes las amenazas cibernéticas que se desarrollan rápidamente y que ponen en riesgo la integridad de los jóvenes, de la institución e incluso, de ellos mismos.

Dicha capacitación debe realizarse por parte de los profesores de tecnología, hacia sus pares, lo docentes de otras asignaturas, así como también al personal administrativo. Los profesores deben establecer un cronograma de capacitaciones y utilizar los consejos de docentes y otros espacios que la administración disponga en esta línea, con el fin de compartir el contenido de manera efectiva con sus colegas. Las actualizaciones de las guías estarán a cargo de los profesores de tecnología, quienes, junto con el apoyo del personal administrativo, realizarán las evaluaciones anuales e incorporarán el contenido que determinen necesario.

Tal y como se mencionó anteriormente, las guías fueron redactadas con vocabulario de fácil entendimiento con el fin de lograr una amplia adopción y familiarización entre los docentes; además ser un facilitador para la transmisión y aprendizaje de la información por medio de los espacios dispuestos por la institución para las capacitaciones.

En cuanto a los estudiantes, ellos vienen a ser las semillas que se esparcirán en tierra fértil, buscando por medio de la presente propuesta, no solo que su formación en ciberseguridad germine, sino también que sean los propagadores del conocimiento a sus pares y para enseñarles desde edades tempranas a ser ciudadanos digitales responsables que se incorporen al mundo con la ventaja del conocimiento.

Por lo tanto, es relevante el involucramiento de los docentes en su formación, por medio del conocimiento adquirido, gracias a las guías propuestas, el cual viene a tomar un papel protagónico. La transmisión de la información y el acompañamiento o asesoría puede ejecutarse a través de clases interactivas y dinámicas; se pueden utilizar las lecciones guía o las sesiones de orientación para fomentar la discusión sobre la importancia de la seguridad digital, así como las recomendaciones deben seguir para evitar ser víctimas de los ciberdelincuentes.

Además, se alienta a los docentes a involucrar a estudiantes de décimo año y undécimo a que participen del servicio comunal, para que se conviertan en facilitadores y compartan lo aprendido con otros compañeros, creando de esa manera un ambiente de aprendizaje colaborativo.

También, sería importante fomentar un ambiente colaborador donde los tres actores: padres, docentes y estudiantes puedan discutir abiertamente sobre sus experiencias en el uso de la tecnología y cuánto les han venido a aportar las guías a su conocimiento. En este aspecto, se pueden establecer grupos de apoyo o foros, donde se comparta información, se resuelvan dudas y se promueva una comunicación efectiva sobre el uso seguro de las redes, para ello pueden invitarse aquellos casos de estudiantes que se vean envueltos en situaciones conflictivas que tengan que ver con las redes o internet.

La institución podría utilizar su página de Facebook oficial, la cual tiene más 8 mil seguidores, para difundir el material o bien, hacer invitaciones para que la comunidad educativa participe de charlas acerca de esta temática.

Las guías de ciberseguridad deben ser documentos vivos, que se actualicen regularmente para incorporar nuevas amenazas y cambios en las plataformas digitales. Por lo que, se sugiere realizar revisiones anuales que involucren a estudiantes, padres y docentes en el proceso, asegurándose de que se mantenga como documentación relevante y útil. Al implementar estas recomendaciones, el Liceo de Pavas podrá fortalecer su comunidad educativa, asegurando que docentes, padres y madres de familia y estudiantes estén preparados para enfrentar los desafíos en temas de ciberseguridad, promoviendo un entorno digital seguro y responsable.

Se recomienda establecer controles de efectividad del uso y estructura de las guías, con el fin de evaluarlas. Para esto, el personal administrativo deberá realizar un informe anual, que proporcione la cantidad de estudiantes que participaron del programa “Ciber Embajadores”, así como de los estudiantes de sétimo, octavo y noveno, que se vieron beneficiados con recibir el conocimiento impartido por los adolescentes que formaron parte del programa.

Adicionalmente, se sugiere validar por medio de pruebas de conocimiento y encuestas la efectividad del contenido de las mismas, con el objetivo de medir el mecanismo de aprendizaje y el impacto en la comunidad educativa contemplando al personal docente, estudiantes y sus familias.

En cuanto a la institución, como ente, se le sugiere formar un comité responsable de monitorear, evaluar y mejorar continuamente la política de seguridad de la información, identificando y respondiendo a nuevas amenazas, actualizando protocolos y encargándose de capacitar al personal, con el fin de mantener siempre la guardia y cerrar cualquier brecha que pueda significar un franco débil para un ataque a los recursos y activos institucionales.

REFERENCIAS

Bermúdez, M. (2023). Contraloría alerta: 68 % de instituciones públicas son vulnerables en ciberseguridad, pese a que ciberataque de 2022 provocó gastos por más de ₡15 mil millones. *Semanario Universidad*. https://semanariouniversidad.com/pais/contraloria-alerta-68-de-instituciones-publicas-son-vulnerables-en-ciberseguridad-pese-a-que-ciberataque-de-2022-provoco-gastos-por-mas-de-%E2%82%A115-mil-millones/

Bustillos Ortega, O. y Rojas Segura, J. (2023). *Ciberseguridad y desarrollo de habilidades digitales: propuesta de alfabetización digital en edades tempranas.* https://doi.org/10.26439/interfases2023.n018.6626

Castro, M. (2021). *¿Como ejercer una ciudadanía digital responsable?* Tribunal Supremo de Elecciones.

Checkpoint. (2024). *Tipos de amenazas de ciberseguridad.* https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Ciberseguridad se dispara: sector creció 350% en la demanda de talento a nivel mundial. (2024). *La República.* https://www.larepublica.net/noticia/ciberseguridad-se-dispara-sector-crecio-350-en-la-demanda-de-talento-a-nivel-mundial

Cisco. (2023). *Top 10 Cybersecurity Tips*. https://umbrella.cisco.com/blog/cisco-umbrella-top-10-cybersecurity-tips

Cisco. (2024). *¿Qué es la ciberseguridad?* https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Cyber.org. (2020). *The National Integrated Cyber Education Research Center.* https://cyber.org/news/nicerc-unveils-rebrand-cyberorg

Decreto 37052. (2012). *Creación Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR.* http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=72316&nValor3=88167&strTipM=TC

Estrategia Nacional de Ciberseguridad de Estados Unidos. (2023). https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/

Estrategia Nacional de Ciberseguridad de Reino Unido. (2022). https://assets.publishing.service.gov.uk/media/63245ce7d3bf7f1bff8894f2/National_Cyber_Strategy_-_Spanish_Translation_-_Electronic_Version.pdf

FasterCapital. (2024). *Ciberseguridad educativa Proteger a los emprendedores del mañana una guía para la ciberseguridad en la educación.* https://fastercapital.com/es/contenido/Ciberseguridad-educativa--Proteger-a-los-emprendedores-del-manana--una-guia-para-la-ciberseguridad-en-la-educacion.html

Fortinet. (2023). *Informe global sobre el panorama de amenazas de 2H de 2023.* https://www.fortinet.com/lat/resources/analyst-reports/threat-report-2h-2023

GOB. (2024). *Guía de ciberseguridad.* https://www.gob.mx/cms/uploads/attachment/file/896412/Gu_a_de_Ciberseguridad_en_apoyo_a_la_educaci_n.pdf

González, V. y Prendes, M. (2018). *Ciberacosadores: un estudio cuantitativo con estudiantes de secundaria*. https://recyt.fecyt.es/index.php/pixel/article/view/63099/38510

GOV, Reino Unido. (2017). *Cyber Schools Programme.* https://www.gov.uk/guidance/cyber-schools-programme

GOV, Reino Unido. (2022). *Cyber Schools Explorers.* https://www.gov.uk/guidance/cyber-explorers

GOV, Reino Unido. (2023). *Tens of thousands of students receive free training to build cyber skills.* https://www.gov.uk/government/news/tens-of-thousands-of-students-receive-free-training-to-build-cyber-skills

Gross, J. (2023). *Así es como Finlandia enseña a los chicos a detectar la desinformación.* https://www.nytimes.com/es/2023/01/13/espanol/finlandia-clases-desinformacion.html

HealthyChildren.org. (2022). *"Sexteo": cómo hablar con sus hijos del riego de enviar mensajes con contenido sexual.* https://www.healthychildren.org/Spanish/family-life/Media/Paginas/the-new-problem-of-sexting.aspx

Henley, J. (2020). *How Finland starts its fight against fake news in primary schools.* https://www.theguardian.com/world/2020/jan/28/fact-from-fiction-finlands-new-lessons-in-combating-fake-news

Hernández-Sampieri, R. y Mendoza, C. (2020). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.*

Hernández-Sampieri, R, Méndez, Mendoza, Cuevas (2017). *Fundamentos de investigación.*

INCIBE. (2024). *Ciberseguridad para familias.* https://www.incibe.es/menores/familias/ciberseguridad

INCIBE. (2024). *Configura correctamente tu dispositivo y asegura tu información.* https://www.incibe.es/ciudadania/tags/configuraci%C3%B3n%20segura

INCIBE. (2024). *Grooming.* https://www.incibe.es/menores/tematicas/grooming

INCIBE. (2024). *Las redes sociales como herramienta para ciberdelincuentes*. https://www.incibe.es/ed2026/talento-hacker/blog/las-redes-sociales-como-herramienta-para-ciberdelincuentes

INCIBE. (2024). *Privacidad.* https://www.incibe.es/menores/tematicas/privacidad

INCIBE. (2024). *Sexting.* https://www.incibe.es/menores/tematicas/sexting

Infobae. (2024). *La escasez de estudiantes en carreras STEM podría frenar el avance científico y tecnológico en el mundo.* https://www.infobae.com/educacion/2024/06/06/la-importancia-de-fomentar-el-interes-para-que-los-jovenes-estudien-ciencia-tecnologia-ingenieria-o-matematicas/

ISO/IEC 27002. (2022). *Information security, cybersecurity and privacy protection - Information security controls.* https://www.iso.org/es/contents/data/standard/07/56/75652.html

ITU. (2023). *POP: La Iniciativa de Protección Infantil en línea, lanzada por la Unión Internacional de Telecomunicaciones*. https://www.itu.int/en/ITUD/Cybersecurity/Pages/COP/COP.aspx

Kaspersky. (2024). *¿Qué es la ciberseguridad?* https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kaspersky. (2024). *Cómo identificar noticias falsas*. https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-identify-fake-news

Kaspersky. (2024). *Las 15 mejores reglas de seguridad y qué no hacer en línea.*

Ley 10238. Ley de protección de la imagen, la voz y los datos personales de las personas menores de edad. (2022). Asamblea Legislativa de Costa Rica. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=97506&nValor3=131719&strTipM=TC

Ley 7739. Código de la Niñez y la Adolescencia. (1998). Asamblea Legislativa de Costa Rica. http://www.pgrweb.go.cr/scij/busqueda/normativa/normas/nrm_texto_completo.aspx?param2=1&nValor1=1&nValor2=43077&lResultado=4&strSelect=sel

Ley 8934. Ley de Protección de la Niñez y la Adolescencia frente al contenido nocivo de Internet y otros medios electrónicos. (2011). Asamblea Legislativa de Costa Rica. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=71024&nValor3=0

Ley 8968. Ley de Protección de la persona frente al tratamiento de sus datos personales. (2011). Asamblea Legislativa de Costa Rica. http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC

Ley 9452. Convenio sobre la Ciberdelincuencia. (2017). Budapest. https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=84360&nValor3=108815&strTipM=TC

McAfee. (2024). *Ciberacoso: causas, riesgos y cómo evitarlo.* https://www.mcafee.com/learn/es/ciberacoso/

Meta. (2024). *¿Qué hacer cuando tu hijo(a) adolescente sufre de acoso online?* https://familycenter.meta.com/latam/education/resources/how-can-parents-prevent-cyberbullying/

MICITT. (2023-2027). *Estrategia Nacional de Ciberseguridad de Costa Rica*. Ministerio de Ciencia, Tecnología y Telecomunicaciones. https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf

Microsoft. (2023). *Informe de Seguridad Online de Microsoft*. https://news.microsoft.com/es-es/2023/02/07/el-74-de-los-adolescentes-encuestados-en-el-informe-de-seguridad-online-de-microsoft-afirma-haber-experimentado-algun-riesgo-en-internet/

Microsoft. (2024). *¿Qué es la ciberseguridad?* ¿https://www.microsoft.com/es-es/security/business/security-101/what-is-cybersecurity

Microsoft. (2024). *¿Qué es la protección con contraseña?* https://www.microsoft.com/es-cl/security/business/security-101/what-is-password-protection

Miglino, J. (2021). *Estadísticas Mundiales de Bullying 2021.* https://bullyingsinfronteras.blogspot.com/2018/10/estadisticas-mundiales-de-bullying_29.html

Ministerio de Educación Pública. (2020). *Política en tecnologías de la información.* https://juegosdeportivosestudiantiles.mep.go.cr/wp-content/uploads/2023/09/Politica-en-Tecnologias-de-la-Informacion-MEP.pdf

Ministerio de Educación Pública. (2023). *Consejo Superior de Educación aprueba nuevo Programa Nacional de Formación Tecnológica.* https://www.mep.go.cr/noticias/consejo-superior-educacion-aprueba-nuevo-programa-nacional-formacion-tecnologica

Ministerio de Educación Pública. (2023). Factores detonantes de acoso escolar entre estudiantes de colegios públicos académicos. https://www.mep.go.cr/sites/default/files/2024-02/informefinal-acosoescolar2023.pdf

Ministerio de Educación Pública. (2023). *Programa de Formación Tecnológica en el Sistema Educativo Costarricense.* https://www.mep.go.cr/sites/default/files/2024-03/malla-curricular-PNFT.pdf

NACIONAL CIBERSECURITY ALLIANCE. (2022). *Control Parental*. https://staysafeonline.org/es/online-safety-privacy-basics/parental-controls/

NACIONAL CIBERSECURITY ALLIANCE. (2022). *Formando ciudadanos digitales.* https://staysafeonline.org/es/online-safety-privacy-basics/raising-digital-citizens/

NACIONAL CIBERSECURITY ALLIANCE. (2022). *Hablar con niños y adolescentes sobre seguridad y privacidad*. https://staysafeonline.org/es/online-safety-privacy-basics/talking-to-kids-teens/

NACIONAL CIBERSECURITY ALLIANCE. (2022). *Padres y educadores: Qué hacer con el ciberacoso.* https://staysafeonline.org/es/online-safety-privacy-basics/cyberbullying-parents/

NACIONAL CIBERSECURITY ALLIANCE. (2024). *Mes de la concientización sobre la ciberseguridad.* https://www.cisa.gov/sites/default/files/2024-10/Cybersecurity-Awareness-Month-2024-Toolkit-Guide_ES.pdf

OAS. (2020). Educación en Ciberseguridad-Planificación del futuro mediante el desarrollo de la fuerza laboral. https://www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf

OCDE, (2024). *Igualdad de género en Costa Rica : Hacia una mejor distribución del trabajo remunerado y no remunerado*. (2024). https://www.oecd-ilibrary.org/content/country/cr

OMS. (2022). *Informe sobre la prevención de la violencia en internet contra la infancia.* Organización Mundial de la Salud https://iris.who.int/bitstream/handle/10665/364706/9789240062061-eng.pdf?sequence=1

Plan Nacional de Ciberseguridad de Israel. (2021). https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf

Rashi Foundation. (s.f.). *Magshimim*. https://rashi.org.il/en/programs/magshimim/

Rashi Foundation. (s.f.). *Mamriot.* https://rashi.org.il/en/programs/mamriot/

Rashi Foundation. (s.f.). *StarTech.* https://rashi.org.il/en/programs/startech/

U.S. Government Accountability Office (GAO). (2022). https://www.gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done

UNESCO. (2023). *Conferencia "Por un Internet Confiable".* https://www.youtube.com/watch?v=1gST4BPCweE&list=PLWuYED1WVJIN2lb0GGhj65GNHGtxeEvA-&index=23

UNICEF. (2019). *Iniciativa Kindly.* https://www.unicef.org/innovation/kindly

UNICEF. (2021). *Impacto de la tecnología en la adolescencia. Relaciones, riesgos y oportunidades*. https://www.unicef.es/sites/unicef.es/files/comunicacion/Res_Ejec_Impacto_de_la_tecnologia_en_la_adolescencia.pdf

UNICEF. (2021). *Observación general núm. 25, relativa a los derechos de los niños en relación con el entorno digital, generada por el Comité de las Naciones Unidas para los Derechos del Niño.* https://www.un.org/es/global-issues/child-and-youth-safety-online

UNICEF. (2022). *Ciberacoso: qué es y cómo detenerlo*. https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

UNICEF. (2022). *Las 12 habilidades transferibles del Marco Conceptual y Programático.*

UNICEF. (2024). *Alianza Mundial WePROTECT*. https://www.weprotect.org/

UNICEF. (2024). *La seguridad de la infancia y la juventud en la red*. https://www.un.org/es/global-issues/child-and-youth-safety-online

Universidad de Costa Rica. (2023). *Miles de niños y adolescentes en Costa Rica están expuestos a contenido sexual y a contacto con personas desconocidas por medio de internet*. https://www.ucr.ac.cr/noticias/2023/11/23/miles-de-ninos-y-adolescentes-en-costa-rica-

estan-expuestos-a-contenido-sexual-y-a-contacto-con-personas-desconocidas-por-medio-de-internet.html

University of Chicago. (2024). *How Diverse Communities of Young People Think About the Multifaceted Relationship Between Social Media and Mental Health.* https://www.commonsensemedia.org/sites/default/files/research/report/2024-double-edged-sword-hopelab-report_final-release-for-web-v2.pdf

We are social & Meltwater. (2024). *Informe Digital Global, abril 2024*. https://wearesocial.com/es/blog/2024/04/informe-digital-global-abril-2024/

APÉNDICE A. ENCUESTA PARA ESTUDIANTES

En el marco de una investigación sobre el Programa de Formación en Ciberseguridad para la Población del Liceo de Pavas, le invitamos a completar este cuestionario. Su participación es de gran importancia para comprender cómo el tema en estudio influye en la actividad de la organización.

Este cuestionario es confidencial. Sus respuestas solo se utilizarán con fines de investigación y no serán compartidas con ninguna otra persona o institución.

Completar el cuestionario tomará aproximadamente 10 minutos.

1. **Género**

( ) Femenino ( ) Masculino ( ) Prefiero no responder

2. **Edad**

( ) 12-14 años ( ) 15-17 años ( ) 18 años o más

3. **Nivel que cursa**

( ) Sétimo ( ) Octavo ( ) Noveno ( ) Décimo ( ) Undécimo

4. **¿Utiliza con frecuencia las Redes Sociales?**

( ) Sí ( ) No

5. **¿Cuáles Redes Sociales utiliza?**

( ) Facebook ( ) Instagram ( ) WhatsApp ( ) TikTok ( ) Be real( ) Twich ( ) Snapchat ( ) Twitter ( ) Ninguna

6. **¿El acceso a sus datos personales en sus redes sociales es privado o público?**

( ) Privados ( ) Públicos ( ) Algunos privados y otros públicos

7. **¿Cuánto tiempo destina al día para navegar en Redes Sociales?**

( ) 1 hora o menos ( ) 1-2 horas ( ) más de 2 horas

8. ¿Con qué frecuencia acepta o lo siguen personas que no conoce personalmente?

( ) Siempre ( ) Con mucha frecuencia ( ) Pocas veces ( ) Nunca acepto desconocidos

9. ¿Alguna vez ha enviado mensajes, fotos o videos con contenido sexual? También conocido como "sexting" (Recuerde que sus respuestas son anónimas y confidenciales)

( ) Sí ( ) No ( ) Prefiero no responder

10. ¿Cuál fue su motivación para compartir este tipo de contenido?

( ) Está de moda ( ) Me dejé llevar por el momento ( )
Presión de mi pareja/amistad/desconocido ( ) Tener intimidad con mi pareja ( ) Ninguna

11. ¿Ha recibido contenido explícito fotos, videos o audios, sin su consentimiento?

Sí ( ) No ( )

12. El Ciberacoso es usar las redes sociales para molestar, acosar, amenazar, humillar o difundir chismes o información personal de otra persona. ¿Alguna vez ha sido víctima de ciberacoso?

( ) Sí ( ) No

13. En caso de que su respuesta sea afirmativa: ¿qué acciones tomó?

( ) No contestar ( ) Bloquear a la persona/ cuenta ( ) Informé a mis padres o adulto de confianza / profesor ( ) No le conté a nadie ( ) Denuncié/Reporté ( ) Ninguna

14. ¿Sabe usted que es un "virus", "malware" o "código malicioso"?

( ) Sí ( ) No ( ) Nunca lo había escuchado ( ) Lo escuchado, pero no sé bien que es

15. ¿Sabe cómo identificar cuando su celular o computadora tiene malware/código malicioso?

( ) Sí ( ) No ( ) No estoy seguro

16. ¿Descarga aplicaciones, películas, videojuegos u otros por páginas "pirata" donde es gratis?

( ) Sí ( ) No

17. ¿Con qué frecuencia se conecta a redes de wifi públicas?

( ) Siempre ( ) Con mucha frecuencia ( ) Pocas veces ( ) Nunca

18. ¿Siente que estar conectado(a) a una red pública representa un riesgo?

( ) Sí ( ) No

19. ¿Dónde tiene guardadas sus contraseñas?

( ) Notas del celular ( ) En una libreta/hoja suelta/cuaderno ( ) En mi correo electrónico

20. ¿Comparte noticias/artículos con solo haber leído el título?

( ) Siempre ( ) Algunas veces ( ) Nunca

21. ¿Conoce los derechos que como usuario tiene con respecto al uso de datos personales en medios sociales y digitales?

( ) Sí ( ) No

22. ¿Sus profesores le brindan información sobre los riesgos o prevenciones que debe tomar cuando hace uso de Redes Sociales o plataformas digitales?

( ) Siempre ( ) Algunas veces ( ) Nunca

23. ¿Sus padres le brindan información o supervisión sobre los riesgos o prevenciones que debe tomar cuando hace uso de Redes Sociales o plataformas digitales?

( ) Siempre ( ) Algunas veces ( ) Nunca

APÉNDICE B. ENCUESTA PARA PADRES DE FAMILIA

En el marco de una investigación sobre el Programa de Formación en Ciberseguridad para la Población del Liceo de Pavas, le invitamos a completar este cuestionario. Su participación es de gran importancia para comprender cómo el tema en estudio influye en la actividad de la organización.

Este cuestionario es confidencial. Sus respuestas solo se utilizarán con fines de investigación y no serán compartidas con ninguna otra persona o institución.

Completar el cuestionario tomará aproximadamente 10 minutos.

1. **Género**

( ) Femenino ( ) Masculino ( ) Prefiero no responder

2. **Edad**

( ) 20-30 años ( ) 31-40 años ( ) 40-50 años ( ) 51 o más

3. **Nivel de escolaridad**

( ) Primaria incompleta ( ) Primaria completa ( ) Secundaria incompleta ( ) Secundaria completa ( ) Universidad incompleta ( ) Universidad completa

4. **¿Utiliza con frecuencia las Redes Sociales?**

( ) Sí ( ) No

5. **¿Cuáles Redes Sociales utiliza?**

( ) Facebook ( ) Instagram ( ) WhatsApp ( ) TikTok ( ) Be real( ) Twich ( ) Snapchat ( ) Twitter ( ) Ninguna

6. **¿Cuánto tiempo destinan al día sus hijos navegando en Redes Sociales?**

( ) 1 hora o menos ( ) 1-2 horas ( ) más de 2 horas

7. **¿Establece límites de tiempo en sus hijos para el uso de Redes Sociales?**

( ) Siempre ( ) Algunas Veces ( ) Nunca

8. **¿Con que frecuencia tiene conversaciones con sus hijos acerca de sus actividades en Redes Sociales e internet?**

( ) Siempre ( ) Algunas Veces ( ) Nunca

9. **¿Sus hijos reciben orientación en el colegio sobre los peligros a los que están expuestos al navegar en internet o Redes Sociales?**

( ) Sí ( ) No ( ) No lo sé

10. **¿Sus hijos le han manifestado que han sido víctimas de acoso en internet o Redes Sociales?**

( ) Sí ( ) No

11. **En caso de que su respuesta sea afirmativa: ¿qué ha hecho al respecto?**

( ) No hice nada ( ) Fui a hablar al colegio ( ) Hice una denuncia formal ( ) Me contacté con el agresor(a) ( ) Ninguna de las anteriores

12. **¿Usted ha recibido información sobre los peligros de compartir información personal a terceros o por medio de redes sociales?**

( ) Sí ( ) No

13. **¿Sabe usted que es un "virus", "malware" o "código malicioso"?**

( ) Sí ( ) No ( ) Lo he escuchado, pero no sé bien que es

14. **¿Sabe cómo identificar cuando su celular o computadora tiene malware/código malicioso?**

( ) Sí ( ) No ( ) No estoy seguro(a)

15. **¿Con qué frecuencia se conecta a redes de wifi públicas?**

( ) Siempre ( ) Con mucha frecuencia ( ) Pocas veces ( ) Nunca

16. **¿Considera que estar conectado(a) a una red pública representa un riesgo?**

( ) Sí ( ) No ( )

17. ¿Dónde tiene guardadas sus contraseñas?

( ) Notas del celular ( ) En una libreta/hoja suelta/cuaderno ( ) En mi correo electrónico
( ) Otro

18. ¿Comparte noticias/artículos con solo haber leído el título?

( ) Siempre ( ) Algunas Veces ( ) Nunca

19. Cuándo lee una noticia/artículo: ¿usted verifica la fuente?

( ) Siempre ( ) Algunas Veces ( ) Nunca

20. ¿Conoce los derechos que como usuario tiene con respecto al uso de datos personales en medios sociales y digitales?

( ) Sí ( ) No ( ) No estoy seguro

APÉNDICE C. ENCUESTA PARA DOCENTES

En el marco de una investigación sobre el Programa de Formación en Ciberseguridad para la Población del Liceo de Pavas, le invitamos a completar este cuestionario. Su participación es de gran importancia para comprender cómo el tema en estudio influye en la actividad de la organización.

Este cuestionario es confidencial. Sus respuestas solo se utilizarán con fines de investigación y no serán compartidas con ninguna otra persona o institución.

Completar el cuestionario tomará aproximadamente 10 minutos.

1. **Género**

( ) Femenino ( ) Masculino ( ) Prefiero no responder

2. **Edad**

( ) 20-30 años ( ) 31-40 años ( ) 40-50 años ( ) 51 o más

3. **¿Utiliza con frecuencia las Redes Sociales?**

( ) Sí ( ) No

4. **¿Cuáles Redes Sociales utiliza?**

( ) Facebook ( ) Instagram ( ) WhatsApp ( ) TikTok ( ) Be real( ) Twich ( ) Snapchat ( ) Twitter ( ) Otro

5. **¿Cuánto tiempo destina al día navegando en Redes Sociales?**

( ) 1hora o menos ( ) 1-2 horas ( ) más de 2 horas

6. **¿Está familiarizado con el concepto "Ciberseguridad"?**

( ) Sí ( ) No ( ) Nunca lo he escuchado( ) Lo he escuchado, pero no sé bien que es

7. **¿Con que frecuencia tiene conversaciones con sus estudiantes acerca de sus actividades en Redes Sociales e internet?**

( ) Siempre ( ) Algunas Veces ( ) Nunca

8. ¿Sus estudiantes le han manifestado que han sido víctimas de acoso en internet o Redes Sociales?

( ) Sí ( ) No

9. En caso de que su respuesta sea afirmativa: ¿qué ha hecho al respecto?

( ) No hice nada ( ) Conversamos con los padres de familia ( ) Hice una denuncia formal
( ) Me contacté con el agresor(a) ( ) Ninguna de las anteriores

10. ¿Sabe usted que es un "virus", "malware" o "código malicioso"?

( ) Sí ( ) No ( ) Nunca lo había escuchado ( ) Lo escuchado, pero no se bien que es

11. ¿Sabe cómo identificar cuando su celular o computadora tiene malware/código malicioso?

( ) Sí ( ) No ( ) No estoy seguro

12. ¿Con qué frecuencia se conecta a redes de wifi públicas?

( ) Siempre ( ) Con mucha frecuencia ( ) Pocas veces ( ) Nunca

13. ¿Siente que estar conectado(a) a una red pública representa un riesgo?

( ) Sí ( ) No ( ) No estoy seguro

14. ¿Dónde tiene guardadas sus contraseñas?

( ) Notas del celular ( ) En una libreta/hoja suelta/cuaderno ( ) En mi correo electrónico

15. ¿Comparte noticias/artículos con solo haber leído el título?

( ) Siempre ( ) Algunas Veces ( ) Nunca

16. Cuando lee una noticia/artículo: ¿se fija en la fuente?

( ) Siempre ( ) Algunas Veces ( ) Nunca

17. ¿Conoce los derechos que como usuario tiene con respecto al uso de datos personales en medios sociales y digitales?

( ) Sí ( ) No ( ) No estoy seguro

APÉNDICE D. GUÍA DE ENTREVISTA SEMIESTRUCTURADA

Organización: Centro educativo Liceo de Pavas.
Nombre del Entrevistado: Hannia Garro Rodríguez.
Cargo: Encargada de la institución.

Preguntas

1. ¿Qué medida se utiliza para controlar el acceso de personas no autorizadas a las instalaciones?
2. ¿Cómo se recopilan, almacenan y procesan los datos de los estudiantes y sus familias por parte del personal docente y administrativo?
3. ¿Cómo se recopila, almacena y procesa la información financiera del centro educativo?
4. ¿Realizan respaldos periódicos de la información digital? ¿Medios por los cuales realizan esos respaldos?
5. ¿La red inalámbrica es de acceso público? ¿Quién gestiona el control de accesos y el mantenimiento de la red?
6. ¿Quién es el encargado de realizar el mantenimiento de los equipos informáticos? ¿Cuenta con restricciones de accesos sobre los activos de la institución?
7. ¿Existe políticas o procedimientos de contraseñas en los equipos de cómputo o sistemas?
8. ¿Cuáles sistemas de información son utilizados en el centro educativo?
9. ¿Quién realiza la instalación de software en los equipos de cómputo?
10. ¿Los equipos de cómputo de la institución cuentan con alguna protección como antivirus? ¿Se actualizan de manera periódica?
11. ¿Quién es el encargado de la gestión de redes sociales del centro educativo?
12. ¿Los docentes y personal administrativo utilizan el correo personal para realizar comunicaciones internas o externas?
13. ¿Cuentan los equipos de cómputo con controles de acceso, a la red y a su contenido para estudiantes y personal docente y administrativo, como por ejemplo, controles parentales?

APÉNDICE E. GUÍA DE CIBERSEGURIDAD PARA ESTUDIANTES DEL LICEO DE PAVAS

GUÍA DE CIBERSEGURIDAD

Para Estudiantes

Autor: Luis Andrés Montero Madriz.

2024

2

Guía de ciberseguridad para estudiantes

Esta guía de formación en ciberseguridad tiene como objetivo enseñarte a cómo protegerte de las amenazas digitales y a desarrollar hábitos seguros en el uso de la tecnología, para que puedas interactuar de manera segura y consciente con el entorno digital.

¿Qué aprenderás?

Riesgos y amenazas en el mundo digital: Podrás identificar las principales amenazas y riesgos a los que te enfrentas al navegar en línea.

Proteger tu privacidad: Aprenderás a como mantener tus datos a salvo, por medio de la creación de contraseñas seguras y la seguridad en tus dispositivos.

Crear hábitos seguros: Comprenderás la importancia del uso responsable de tus redes sociales y hábitos de navegación segura.

Protección legal: Conocerás las leyes y normas que te protegen en caso de sufrir daños en el mundo digital.

Desarrollar habilidades sociales: Aprenderás la importancia de las habilidades sociales en tu desarrollo educativo.

La guía se desarrolló a partir de diversas referencias bibliográficas, adaptándose a la población objetivo mediante un lenguaje accesible para fomentar el aprendizaje autónomo. Con un diseño intuitivo y atractivo, se facilita la comprensión y transferencia del conocimiento, haciendo de este recurso una herramienta educativa valiosa en temas de ciberseguridad.

Contenido

Capítulo 1. Fundamentos de Ciberseguridad
- Concepto de "ciudadanía digital": ser un usuario responsable y respetuoso en línea.
- ¿Qué es la ciberseguridad y por qué es importante?
- Amenazas más comunes: phishing, malware y robo de identidad.

Capítulo 2. Riesgos en Línea
- Principales riesgos a los que se enfrentan los jóvenes en línea: ciberbullying, grooming, sexting, fake news y publicación de información privada.
- Mecanismos utilizados para engañar a los jóvenes.
- ¿Cómo evitar ser víctima de engaños?

Capítulo 3. Protección de Datos Personales
- Creación de contraseñas seguras.
- ¿Cómo manejar la privacidad en redes sociales?
- ¿Cómo proteger tus dispositivos personales?
- Consejos para una navegación segura.

Capítulo 4. Protección Legal en el Mundo Digital
- Introducción a las leyes sobre delitos informáticos y protección de datos.
- Consecuencias legales de participar en prácticas ilícitas en línea.

Capítulo 5. Habilidades para la Vida
- Beneficios de estudiar ciberseguridad.
- ¿Qué son las habilidades blandas y sus beneficios?
- ¿Cómo desarrollar la comunicación interpersonal, la resolución de problemas y el autocontrol?

Capítulo 6. Desafíos de Ciberseguridad
- Ejercicios y simulaciones de escenarios en los cuales, poner en práctica lo aprendido.

CAPÍTULO 1:

FUNDAMENTOS DE CIBERSEGURIDAD

Comprender los fundamentos en ciberseguridad es esencial para proteger tu información y la de quienes te rodean.

En este capítulo aprenderás:

- Cómo ser un ciudadano digital responsable y respetuoso en línea.
- ¿Qué es la ciberseguridad y por qué es importante?
- Amenazas más comunes: phishing, malware, robo de identidad.

CAPÍTULO 1:

FUNDAMENTOS DE CIBERSEGURIDAD

Ciudadanía digital

Ser un usuario responsable y respetuoso en línea.

La ciudadanía digital consiste en el uso responsable, ético y seguro de la tecnología y el internet.

Algunas responsabilidades que tienes como ciudadano digital son las siguientes:

Debes respetar a los demás en línea, el respeto y la empatía son fundamentales para una sana convivencia en línea.

No acoses, ofendas o compartas información que pueda dañar a alguien más.

Tienes que proteger tu privacidad, evita compartir información personal sensible como direcciones, contraseñas o detalles íntimos.

Evita la piratería, el plagio y las acciones que dañen a otras personas.

Cuando utilices contenido de otras personas, como imágenes o textos, siempre da crédito a quien la creó.

Ser ciudadanos digitales responsables contribuye a un entorno en línea más seguro.

¿Conoces el significado de ciberseguridad?

La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial; extorsionar a los usuarios o interrumpir la continuidad del negocio.

CAPÍTULO 1: FUNDAMENTOS DE CIBERSEGURIDAD

¿Por qué debes conocer de ciberseguridad?

- Te permite identificar y evitar fraudes en línea, como estafas.
- Te permite tomar decisiones informadas y protegerte a ti y a los demás.
- Te proporciona habilidades muy demandadas en el mercado laboral.
- Te ayuda a usar las redes sociales de manera responsable y segura, protegiendo tu reputación en línea y evitando el ciberacoso.
- Te ayuda a proteger tu información personal, como contraseñas y fotos.

TÉCNICAS QUE UTILIZAN LOS ciberdelicuentes

AMENAZAS MÁS COMUNES:

- Phishing
- Malware
- Robo de identidad

PHISHING • INGENIERÍA SOCIAL • MALWARE

CAPÍTULO 1:
FUNDAMENTOS DE CIBERSEGURIDAD

PHISHING

Consiste en el uso de correos electrónicos para engañar a las personas con el fin de que hagan clic en enlaces o archivos adjuntos maliciosos.

Trucos

1. Correos o mensajes falsos de empresas conocidas, pidiéndote que actualices tus datos.
2. Urgencia o amenazas, dicen que tu cuenta será bloqueada o que hay un problema urgente que necesitas resolver de inmediato.
3. Ofertas , premios, descuentos o regalos increíbles, si haces clic en un enlace o proporcionas tus datos.
4. Solicitudes de información personal, como contraseñas, números de tarjeta de crédito o tu dirección.
5. Enlaces que no coinciden con la dirección, parecen legítimos pero llevan a direcciones web diferentes.

Recomendaciones

1. No abras archivos adjuntos o enlaces que provienen de cuentas de correo electrónico de desconocidos.
2. No respondas a solicitudes de información personal o familiar por correo electrónico, mensajes de texto o llamadas telefónicas.
3. No introduzcas ninguna de tus contraseñas después de hacer clic en un enlace sospechoso.
4. Si recibes correos o mensajes de personas desconocidas, que te parezcan sospechosos, procura eliminarlos de tus bandejas de mensajes.

CAPÍTULO 1: FUNDAMENTOS DE CIBERSEGURIDAD

INGENIERÍA SOCIAL

Es el uso de técnicas psicológicas y de manipulación para engañar a alguien a que haga lo que quiere, aprovechándose de la confianza o desconocimiento.

Trucos

1. Ofrecen algo que parece atractivo o valioso, como un archivo, un programa gratuito o incluso una memoria USB que promete contenido interesante, este método se conoce como baiting.
2. Llaman por teléfono haciéndose pasar por alguien de confianza, y te convencen para que reveles tu información personal o realices una transferencia de dinero, este método se llama vishing.
3. Ofrecen algo a cambio de información o acceso, como un supuesto premio, un descuento o un servicio gratuito, para que aceptes, sin darte cuenta de que estás siendo engañado, este método se llama quid pro quo.

Recomendaciones

1. No des información personal sin confirmar la identidad de la persona que lo solicita.
2. No hagas clic en enlaces ni descargues archivos de fuentes desconocidas.
3. Antes de compartir información o seguir una instrucción, verifica si es una solicitud legítima.

¡A veces, la curiosidad puede jugar en nuestra contra!

Puede resultar en el robo de datos personales.

CAPÍTULO 1: FUNDAMENTOS DE CIBERSEGURIDAD

MALWARE

Es un software malicioso que se puede utilizar para lograr muchos objetivos diferentes, diseñado para causar daño a tus dispositivos o robar información.

Trucos

1. Enlaces falsos en correos o mensajes.
2. Archivos adjuntos en correos electrónicos o mensajes de texto.
3. Descargas de software o aplicaciones no oficiales.
4. Actualizaciones falsas o falsas alertas de seguridad.
5. Juegos o contenido multimedia falsos.
6. Mensajes emergentes engañosos, alertas de tu navegador o sistema, pidiéndote que descargues un archivo para solucionar un problema.

Recomendaciones

1. Mantén tu software actualizado.
2. Usa un antivirus confiable.
3. Sé cauteloso con las descargas.
4. Verifica la autenticidad y legitimidad de un mensaje o enlace.
5. Usa las opciones de seguridad y privacidad en tu navegador para bloquear sitios web maliciosos y anuncios engañosos.

El malware puede robar contraseñas y otra información sensible.

CAPÍTULO 2:

RIESGOS EN LÍNEA

Vivir conectados es parte de nuestra realidad, pero también lo son los riesgos en línea. Conocerlos y aprender a protegernos es la clave para disfrutar de internet de manera segura.

En este capítulo aprenderás:

- Acerca de los principales riesgos a los que te enfrentas en línea: ciberbullying, grooming, sexting, fake news, publicación de información privada.
- Mecanismos que utilizan para engañarte.
- ¿Cómo evitar ser víctima de engaños?

CAPÍTULO 2:

RIESGOS EN LÍNEA

Los riesgos reales en el mundo digital.

CIBERBULLYING

Consiste en una forma de hostigamiento, agresión o acoso que se realiza por medios digitales, puede darse en en aplicaciones, videojuegos, redes sociales, blogs y algunas otras plataformas.

Trucos

1. Creación de perfiles falsos.
2. Difusión de rumores o información falsa.
3. Excluyen a la víctima, dejándola fuera de conversaciones o eventos, y haciendo comentarios hirientes sobre su exclusión.
4. Publican información personal de la víctima, como dirección, número de teléfono, o incluso información privada, para que otros la acosen o intimiden.
5. Se hacen pasar por la víctima en línea, enviando mensajes o publicando contenido ofensivo para dañar su reputación.

Recomendaciones

1. Denunciar al acosador.
2. Bloquea y reporta.
3. Habla con alguien de confianza.
4. Denuncia legalmente.
5. Guarda pruebas, como tomar capturas de pantalla o guarda los mensajes, fotos o videos puede ser útil al pedir ayuda o denunciar el acoso.

Impacta a nivel emocional, puede causar depresión, estrés, ansiedad, baja autoestima y hasta el suicidio.

CAPÍTULO 2: RIESGOS EN LÍNEA

GROOMING

Estrategias de contacto que realiza un adulto para intentar ganarse la confianza de un niño, niña o adolescente a través de internet, con el objetivo de explotarlo o acosarlo sexualmente.

Trucos

1. Fingir ser alguien de su edad.
2. Regalar cumplidos y atención especial.
3. Compartir intereses o gustos comunes.
4. Mostrar empatía y apoyo ante tus problemas o situaciones.
5. Enviar regalos o dinero.
6. Crear una relación secreta.
7. Introducir conversaciones inapropiadas, temas sexuales, de manera sutil.

Recomendaciones

1. No aceptes solicitudes de amistad de desconocidos.
2. Desconfía de quien te pide mantener secretos.
3. No compartas información personal ni fotos privadas.
4. Habla con un adulto de confianza si alguien te hace sentir incómodo.
5. Revisa la configuración de privacidad en todas tus redes sociales.

Sabías que el grooming puede causar riesgos de abuso sexual y traumas psicológicos.

CAPÍTULO 2:
RIESGOS EN LÍNEA

SEXTING

Se define como el intercambio de imágenes o videos con contenido sexual, a través de teléfonos y/o Internet (mensajes, correos electrónicos, redes sociales).

Trucos

1. Intentan ganar tu confianza, se muestran como amigos.
2. Te hacen sentir especial y te llenan de cumplidos.
3. Te piden fotos o videos íntimos, a veces con insistencia.
4. Aseguran que el contenido será secreto.
5. Te hacen sentir culpable o te presionan con frases como **"si me amas, lo harías"**.

Recomendaciones

1. No envíes fotos o vídeos íntimos.
2. No cedas a la presión o chantaje.
3. No confíe en promesas de privacidad.
4. Bloquea a personas sospechosas.
5. Revisa y ajusta tus configuraciones de seguridad.
6. Infórmate sobre los riesgos y las leyes relacionadas.

Sabías que el sexting puede afectar gravemente tu autoestima e imagen.

CAPÍTULO 2:
RIESGOS EN LÍNEA

PUBLICACIÓN DE INFORMACIÓN PRIVADA

La publicación de información privada en línea implica compartir datos personales como nombres, direcciones, números de teléfono y fotos en redes sociales o plataformas digitales.

Trucos

1. La información privada puede ser utilizada por delincuentes para hacerse pasar por otra persona.
2. Compartir detalles personales puede atraer a acosadores en línea.
3. Publicar información inapropiada puede afectar la imagen personal y profesional en el futuro.
4. La necesidad de aceptación puede llevarte a compartir más de lo recomendable.

Recomendaciones

1. Utiliza herramientas de configuración de privacidad en redes sociales para limitar quién puede ver tu información.
2. Reflexiona sobre cómo la información puede ser usada por otros antes de compartirla.
3. Habla con un adulto de confianza si se siente incómodo o si la información ha sido comprometida.

La información publicada puede permanecer en internet indefinidamente, incluso después de ser eliminada.

CAPÍTULO 2:
RIESGOS EN LÍNEA

FAKE NEWS

Son noticias o información falsa que se difunden con la intención de engañarte. Estas noticias pueden parecer reales, pero su propósito es desinformar o manipular tus opiniones.

Trucos

1. Se utilizan títulos exagerados que buscan provocarte una fuerte reacción emocional, sin comprobar el contenido.
2. Se citan fuentes que no existen o se alteran citas reales para hacer que la noticia parezca más creíble. Ejemplo: según un estudio de la Universidad X..." (cuando no hay tal estudio).
3. Se utilizan perfiles automatizados o falsos en redes sociales para difundir información rápidamente, creándote la ilusión de que una noticia es popular. Ejemplo: muchos retweets de cuentas sin actividad real.
4. Se utilizan imágenes editadas o sacadas de contexto para respaldar una afirmación falsa.

Conocer sobre las fake news te ayuda a formar un pensamiento crítico y protegerte de la desinformación.

Recomendaciones

1. Asegúrate de que la noticia provenga de un medio confiable y reconocido.
2. Investiga si el sitio tiene buena reputación.
3. No te quedes solo con el titular. Revise todo el artículo para entender el contexto y la información completa.
4. Verifica que la noticia sea reciente. A veces, se comparten noticias viejas como si fueran nuevas.
5. Asegúrate de que el autor sea un periodista reconocido o tenga experiencia en el tema. Busca su nombre en otras publicaciones.
6. Si una noticia solo aparece en un lugar, es sospechoso. Comprueba si otros medios informan sobre lo mismo.
7. Si no hay pruebas o datos claros, desconfía.

CAPÍTULO 3:

PROTECCIÓN DE DATOS

En el mundo digital, tus datos personales son muy valiosos. Entender cómo protegerlos es esencial para mantener tu privacidad y seguridad en línea.

En este capítulo aprenderás:

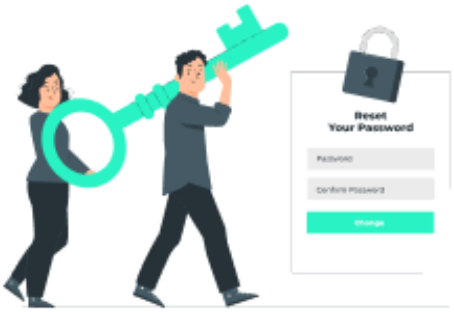
- Acerca de creación de contraseñas seguras.
- ¿Cómo manejar la privacidad en redes sociales?
- ¿Cómo proteger tus dispositivos personales?
- Consejos para una navegación segura.

CAPÍTULO 3:

PROTECCIÓN DE DATOS

¿Cómo mantener tus datos a salvo?

La ciberseguridad desempeña un papel crucial en la protección de la infraestructura digital y la información sensible en un mundo cada vez más dependiente de la tecnología.



RECUERDA:

- La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales.
- Los ciberataques apuntan a acceder, modificar o destruir la información confidencial; extorsionar a los usuarios o dañar los sistemas o plataformas digitales.

1. Creación de contraseñas seguras

Las contraseñas son para proteger tu información personal. Una contraseña débil puede ser fácilmente hackeada, poniendo en riesgo tus cuentas.

Consejos para crear contraseñas seguras

Longitud: Usa al menos 12 caracteres para que sea más difícil de adivinar.

Diversidad: Combina letras (mayúsculas y minúsculas), números y símbolos. Por ejemplo: "C0ntr@seña!2024".

Evita lo obvio: No uses fechas de nacimiento, nombres de mascotas o palabras comunes.

Usa frases: Considera crear una frase que sea fácil de recordar pero difícil de adivinar. Ejemplo: "MiGatoEs@moRado2024".

Cambia regularmente: Es recomendable cambiar tus contraseñas cada 3-6 meses para mayor seguridad.

CAPÍTULO 3: PROTECCIÓN DE DATOS

2. Configuración de privacidad en redes sociales

La configuración de privacidad ayuda a proteger tu información personal de desconocidos y te permite controlar quién puede ver lo que compartes.

RECUERDA:

La privacidad permite que:

- Evita que te expongas a riesgos innecesarios, como el robo de identidad o el uso indebido de tu información.
- Evita el ciberacoso.
- Protege tu reputación digital.
- Previene el robo de identidad.

Consejos para configurar la privacidad

Revisa la configuración: Asegúrate de que tus perfiles estén configurados como "privados" para que sólo tus amigos puedan ver tus publicaciones.

Controla quién puede enviar solicitudes de amistad: Limita esto a sólo amigos conocidos para evitar interacciones no deseadas.

Piensa antes de publicar: Pregúntate si estarías cómodo con que cualquier persona vea la información que vas a compartir.

Revisa las etiquetas: Configura tu cuenta para que debas aprobar cualquier publicación en la que te etiqueten antes de que se haga visible.

CAPÍTULO 3: PROTECCIÓN DE DATOS

3. Consejos para proteger dispositivos personales

Tus dispositivos (teléfonos, tabletas, computadoras) almacenan información personal, como fotos, mensajes y datos financieros. Protegerlos evita que caigan en manos equivocadas.

Consejos para proteger tus dispositivo

Usa bloqueo de pantalla: Activa un código, patrón o reconocimiento facial para acceder a tu dispositivo.

Actualiza regularmente: Mantén tu sistema operativo y aplicaciones actualizadas para protegerte de vulnerabilidades.

Instala software de seguridad: Utiliza aplicaciones de seguridad que ofrezcan protección contra virus y malware.

Ten cuidado con las conexiones Wi-Fi: Evita conectarte a redes públicas o no seguras. Si necesitas hacerlo, considera usar una VPN (Red Privada Virtual).

Haz copias de seguridad: Regularmente, guarda copias de tu información importante en la nube o en un disco externo.

RECUERDA:

- Proteger tus dispositivos es tan importante como proteger tu privacidad y seguridad en línea.
- Los dispositivos móviles contienen mucha información personal y son la puerta de entrada a nuestra vida digital.
- Tomar medidas para protegerlos evita riesgos como el robo de datos, malware o incluso el acceso no autorizado a tus redes sociales.

"Un dispositivo bien protegido es una vida digital más segura."

CAPÍTULO 3: PROTECCIÓN DE DATOS

¿Quieres tener una navegación más segura?

Sigue estos pasos

1. No des tus datos personales a desconocidos.
2. Evita conectarte a las redes públicas de wifi.
3. Ten cuidado con los archivos que llegan por sorpresa.
4. Mantén tus claves en secreto.
5. Escápate del Spam, no des clic en los enlaces o anuncios.
6. Cubre tu webcam cuando no la estés usando.
7. Nunca tengas una cita a solas con alguien que conociste en internet.
8. No des clic a links con ofertas de sitios que no conoces.

9. Navega en sitios web seguros y adecuados para tu edad.
10. Cuida tu privacidad en las redes sociales.
11. Usa la configuración de privacidad de tu compu, tablet o celular.
12. Ten cuidado donde descargas música, videos o juegos.
13. Revisa que tu computadora tenga un antivirus actualizado.
14. Tu contraseña debe ser segura y difícil de adivinar.

CAPÍTULO 4:

PROTECCIÓN LEGAL EN EL MUNDO DIGITAL

En el mundo digital, es importante conocer nuestros derechos y las leyes que protegen nuestra información, esto nos permite ser ciudadanos digitales responsables y seguros.

En este capítulo aprenderás:

- Acerca de las leyes sobre delitos informáticos y protección de datos.
- Consecuencias legales de participar en prácticas ilícitas en línea.

CAPÍTULO 4:

PROTECCIÓN LEGAL EN EL MUNDO DIGITAL

¿Sabes que existen unas leyes que te protegen?

LEY 9048 de delitos informáticos

¿Sabías que si alguien hackea tu cuenta de redes sociales o intenta entrar en tu computadora sin permiso, está violando la **Ley 9048**?

Si alguien accede a tu información sin tu autorización. Por ejemplo, si intentan robarte contraseñas o leer tus mensajes privados, están cometiendo un delito.

Consecuencia: ¡Podrían enfrentar multas o incluso ir a la cárcel hasta por 10 años!

LEY 8968 de protección de la persona frente al tratamiento de sus datos personales

¿Sabías que nadie puede compartir tus fotos, videos o información personal sin tu permiso?

Si una empresa o una persona recopila tu información sin tu consentimiento, puedes pedir que la borren o que dejen de usarla.

Consecuencia: Si no respetan tu decisión, pueden ser multados y enfrentar problemas legales.

LEY 10238 de protección de la imagen, la voz y los datos personales de las personas menores de edad

¿Sabías que nadie puede publicar o usar tus fotos, videos o cualquier información que te identifique sin el consentimiento explícito de tus padres o tutores legales?

Esta ley está diseñada para proteger la tu privacidad y seguridad, específicamente tu imagen, voz y datos personales.

Consecuencia: La ley establece multas a quienes violen esta normativa.

CAPÍTULO 4: PROTECCIÓN LEGAL EN EL MUNDO DIGITAL

LEY 8454 de certificados, firmas digitales y documentos electrónicos

¿Sabías que cuando usas una firma digital en un documento, tiene la misma validez que tu firma a mano?

Esta ley permite que hagas trámites seguros en línea, como firmar contratos o autorizar documentos importantes, sin necesidad de estar presente físicamente.

Consecuencia: Si alguien usa tu firma digital sin tu autorización, puede ser considerado fraude.

LEY 8934 protección de la niñez y la adolescencia en internet

¿Sabías que La **Ley 8934** te protege a los niños del acceso a contenidos dañinos como: violencia, pornografía o contenido que promueve el odio?

Los proveedores de Internet: Si no bloquean contenido inapropiado, pueden recibir multas o ser suspendidos.

Instituciones educativas: Si no educan sobre el uso seguro de Internet, también pueden enfrentar sanciones.

Personas que comparten contenido inapropiado: Compartir contenido violento o pornográfico con menores puede resultar en cárcel.

Estas leyes están diseñadas para protegerte en el mundo digital. Saber sobre ciberseguridad te ayuda a proteger tu privacidad y evitar riesgos en internet. Esto te permite defenderte y buscar ayuda si alguna vez te sientes en peligro.

CAPÍTULO 5:

HABILIDADES PARA LA VIDA

Las habilidades sociales no solo nos ayudan a enfrentar los retos del día a día, sino que también nos preparan para construir un futuro lleno de oportunidades.

En este capítulo aprenderás:

- Sobre los beneficios de estudiar ciberseguridad.
- ¿Qué son las habilidades blandas y su importancia?
- ¿Cómo desarrollar la comunicación interpersonal, la resolución de problemas y el autocontrol?

CAPÍTULO 5:

HABILIDADES PARA LA VIDA

Beneficios de estudiar ciberseguridad

1 La ciberseguridad es una de las áreas con mayor crecimiento en el mercado laboral, las empresas buscan constantemente profesionales capacitados para proteger sus sistemas y datos de ciberataques.

2 Esta carrera no solo ofrece un trabajo seguro, sino también posibilidades de crecimiento y especialización.

3 Estudiar ciberseguridad te permite adquirir habilidades para entender y mitigar los riesgos en línea, preparándote para enfrentar los desafíos digitales actuales.

4 Los profesionales en ciberseguridad juegan un papel vital en la protección de datos personales y la seguridad en línea.

5 Estudiar ciberseguridad te ofrece una carrera con mucha proyección y la oportunidad de marcar diferencia en el mundo digital.

6 Los profesionales que estudian esta carrera obtienen buen pago por sus servicios.

CAPÍTULO 5:
HABILIDADES PARA LA VIDA

¿Cómo transmitir tu conocimiento?

¿Sabes qué son las habilidades blandas?

Son cruciales para tu desempeño en el colegio y en diferentes áreas de la vida.

Desarrollar estas habilidades permiten adaptarse al mundo moderno.

BENEFICIOS

- Ayudan a gestionar mejor los conflictos.
- Tener buenas relaciones interpersonales.
- Comunicarte asertivamente.
- Aprender a trabajar en equipo.
- Desarrollar valores como la ética profesional.

CAPÍTULO 5: HABILIDADES PARA LA VIDA

También puedes aprender de:

1. Comunicación interpersonal

Es cuando dos o más personas hablan o interactúan directamente, compartiendo ideas, sentimientos o información cara a cara o a través de mensajes. Es una conversación que ayuda a entendernos y conectar con los demás.

Es una habilidad que debes desarrollar para tener relaciones sanas y felices a lo largo de tu vida.

"ESCUCHAR A LOS DEMÁS ES EL PRIMER PASO PARA CONSTRUIR CONEXIONES FUERTES; CUANDO PRESTAMOS ATENCIÓN, ABRIMOS LA PUERTA A LA COMPRENSIÓN Y AL RESPETO MUTUO."

¿Cómo desarrollarla?

- Demuéstrales que los estás escuchando: "Te entiendo".
- Tratando de comprender al otro.
- Sé abierto y honesto.
- Practicando la escucha activa: Escuchar atentamente.
- En una conversación, no te concentres en cómo responder, sino en escuchar y comprender.
- Trata de respetar su opinión sin juzgarlos.
- Respetando a los demás.
- Usa palabras que demuestren amabilidad.

CAPÍTULO 5:
HABILIDADES PARA LA VIDA

2. Solución de problemas

Es la capacidad de encontrar soluciones a los retos o dificultades que se presentan. Es como ser un detective que busca respuestas para arreglar situaciones complicadas y lograr que las cosas funcionen bien.

Es una habilidad que debes desarrollar para tener relaciones sanas y felices a lo largo de tu vida.

"LOS JÓVENES QUE APRENDEN HABILIDADES PARA RESOLVER PROBLEMAS Y CONFLICTOS SE SIENTEN BIEN CONSIGO MISMOS. TIENEN LA CAPACIDAD DE TOMAR MEJORES DECISIONES."

¿Cómo desarrollarla?

Identifica el problema, el primer paso es determinar exactamente cuál es el conflicto.

¿Por qué esto es tan importante para mí?. ¿Por qué necesito esto?. ¿Qué podría pasar si?. ¿Por qué me está molestando?

Haz una lluvia de ideas sobre posibles soluciones , haz una lista de todas las formas que crees que pueden resolver el problema.

Evalúa las soluciones, mira los pros y los contras de todas las posibles soluciones.

Pon la solución en acción. Una vez que hayas encontrado una posible solución, ponla en práctica para ver si realmente funciona.

CAPÍTULO 5: HABILIDADES PARA LA VIDA

3. Autocontrol

Es la capacidad de mantener la calma y controlar las emociones y acciones, incluso cuando estás enojado o bajo presión. Es como tener un freno interno que ayuda a tomar buenas decisiones en lugar de reaccionar impulsivamente.

Es una habilidad esencial no solo para el mundo laboral sino para la vida en general.

"EL AUTOCONTROL ES TU SUPER PODER EN EL MUNDO DIGITAL. CADA VEZ QUE TE TOMAS UN SEGUNDO PARA PENSAR ANTES DE ACTUAR, ESTÁS USANDO ESE PODER. ¡RECUERDA, TÚ TIENES EL CONTROL!"

¿Cómo desarrollarla?

Compartir tus emociones con alguien de confianza puede ayudarte a manejarlas mejor y encontrar soluciones.

Tener expectativas y metas claras.

Reconoce tus emociones, Aprende a identificar lo que sientes. Si puedes nombrar tu emoción, será más fácil controlarla.

Respira Profundo al sentir que te vas a enojar o perder el control, toma unas respiraciones profundas antes de reaccionar.

Piensa en las consecuencias. Antes de actuar, piensa s. ¿Cómo afectará tu reacción a ti y a los demás?

Busca una distracción al sentir que vas a perder el control, haz algo que te guste, como escuchar música o salir a caminar.

Habla de lo que sientes con alguien de confianza puede ayudarte a manejarlas mejor y encontrar soluciones.

Cuenta hasta 10 lentamente. Antes de decir o hacer algo enojado en tu mente.

Practica todos los días, el autocontrol mejora con la práctica.

CAPÍTULO 6:

DESAFÍOS DE CIBERSEGURIDAD

Practica y Aprende

1. ¿Cuáles de los siguientes son buenos hábitos de ciberseguridad? (Elige dos)

a) Usar la misma contraseña para todas las cuentas.
b) No compartir información personal en redes sociales.
c) Hacer clic en enlaces de correos desconocidos.
d) Configurar la privacidad de tus redes sociales.

2. Situación: Juan recibe un mensaje de un desconocido que le pide su número de teléfono y le ofrece un premio a cambio de responder preguntas personales.

¿Qué debe hacer Juan?
a) Ignorar el mensaje y bloquear al remitente.
b) Responder al mensaje para obtener el premio.
c) Dar su número sólo si el remitente parece de confianza.
d) Comentar con sus amigos lo que pasó y seguir adelante.

3. Situación: María subió una foto a redes sociales sin darse cuenta de que contenía su dirección en segundo plano. Un desconocido le escribe diciendo que sabe dónde vive.

¿Qué debe hacer María?
a) Eliminar la foto de inmediato y ajustar su configuración de privacidad.
b) Responder al desconocido pidiendo que no le moleste.
c) Subir más fotos para que su dirección quede menos visible.
d) No hacer nada porque seguramente no es serio.

CAPÍTULO 6: DESAFÍOS DE CIBERSEGURIDAD

4. Situación: Raúl recibe una llamada de alguien que dice ser del soporte técnico de su proveedor de internet, pidiéndole que descargue un programa en su computadora para solucionar un problema de seguridad. El tono de la persona suena urgente.

¿Qué debe hacer Raúl?
a) Descargar el programa porque confía en que están ayudándolo.
b) Colgar la llamada y llamar directamente a su proveedor para verificar la situación.
c) Descargar el programa pero tener cuidado al usarlo.
d) Preguntar más detalles sobre el problema antes de decidir.

5. Situación: Laura y su novio han estado intercambiando mensajes y fotos privadas. Él le pide que le envíe una foto comprometedora asegurándole que no la compartirá con nadie más.

¿Qué debe hacer Laura?
a) Debe compartirla, igual es para su novio.
b) Preguntarles a sus amigos si debe compartirla.
c) Compartir imágenes y videos, ya que no cree que pase nada.
d) No debe compartirla, ya que luego de enviarla perderá el control de lo que pueda pasar con la imagen.

6. Situación: Valeria comienza a recibir mensajes en sus redes sociales donde otros compañeros de clase se burlan de su apariencia y le hacen comentarios hirientes. Ella no sabe cómo lidiar con los insultos.

¿Qué debe hacer Valeria?
a) Responder a los comentarios defendiendo su apariencia.
b) Ignorar los mensajes y no hablar con nadie del tema.
c) Guardar las pruebas, bloquear a los agresores y hablar con un adulto de confianza.
d) Cambiar su apariencia para evitar más burlas.

CAPÍTULO 6: DESAFÍOS DE CIBERSEGURIDAD

7. Situación: Pablo conoce a alguien en un juego en línea que dice tener su misma edad y gustos. Después de unos días, esa persona le pide su número de teléfono para seguir hablando por otro medio.

¿Qué debe hacer Pablo?
a) Darle su número porque parecen tener muchas cosas en común.
b) Pedirle que le agregue en redes sociales para conocerlo mejor.
c) No compartir ninguna información personal y contar a un adulto lo que está pasando.

8. Situación: Los estudiantes y padres del liceo de Pavas reciben un mensaje viral en Facebook que dice: "Se suspenden clases por brote de diarrea." El mensaje parece legítimo, pero no tiene fuentes confiables.

¿Qué deben hacer sus padres?
a) No enviarlos a clases para evitar que sus hijos enfermen.
b) Compartir la noticia con otros padres para evitar que vayan a clases.
c) Verificar la fuente antes de creer o compartir la noticia.

Respuestas
1- b y d
2- a
3- a
4- b
5- d
6- c
7- c
8- c

RECUERDA

La ciberseguridad no es solo para expertos; es la mezcla perfecta de habilidades técnicas y destrezas sociales.

Aprender a solucionar problemas y tener autocontrol son habilidades que te hacen invencible, dentro y fuera del mundo digital.

Imagínate como un embajador digital, combinando liderazgo, empatía y tus habilidades tecnológicas para guiar a otros y hacer del internet un lugar más seguro.

Saber de ciberseguridad te protege y a la vez estás creando una onda expansiva de responsabilidad digital.

Esta guía te equipa para ser un líder en el mundo digital, donde tu conocimiento técnico y tus habilidades personales se unen para enfrentar cualquier desafío en línea.

Referencias

- Checkpoint, (2024). Tipos de amenazas de ciberseguridad. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security
- GOB, (2024). Guía de ciberseguirdad. https://www.gob.mx/cms/uploads/attachment/file/896412/Gu_a_de_Ciberseguridad_en_apoyo_a_la_educaci_n.pdf
- HealthyChildren.org, (2022). "Sexteo": cómo hablar con sus hijos del riego de enviar mensajes con contenido sexual. https://www.healthychildren.org/Spanish/family-life/Media/Paginas/the-new-problem-of-sexting.aspx
- https://latam.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online
- INCIBE, (2024). Ciberseguridad para familias. https://www.incibe.es/menores/familias/ciberseguridad
- INCIBE, (2024). Configura correctamente tu dispositivo y asegura tu información. https://www.incibe.es/ciudadania/tags/configuraci%C3%B3n%20segura
- INCIBE, (2024). Grooming. https://www.incibe.es/menores/tematicas/grooming
- INCIBE, (2024). Las redes sociales como herramienta para ciberdelincuentes. https://www.incibe.es/ed2026/talento-hacker/blog/las-redes-sociales-como-herramienta-para-ciberdelincuentes
- INCIBE, (2024). Privacidad. https://www.incibe.es/menores/tematicas/privacidad
- INCIBE, (2024). Sexting. https://www.incibe.es/menores/tematicas/sexting
- Kaspersky, (2024). Cómo identificar noticias falsas. https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-identify-fake-news
- Kaspersky, (2024). Las 15 mejores reglas de seguridad y qué no hacer en línea.
- Ley 10238. Ley de protección de la imagen, la voz y los datos personales de las personas menores de edad. Asamblea Legislativa de Costa Rica (2022). http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=97506&nValor3=131719&strTipM=TC
- Ley 7739. Código de la Niñez y la Adolescencia, Asamblea Legislativa de Costa Rica (1998). http://www.pgrweb.go.cr/scij/busqueda/normativa/normas/nr m_texto_completo.aspx?param2=1&nValor1=1&nValor2=43077&lResultado=4&strSelect=sel
- Ley 8934. Ley de Protección de la Niñez y la Adolescencia frente al contenido nocivo de Internet y otros medios electrónicos. Asamblea Legislativa de Costa Rica (2011). http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=71024&nValor3=0

Referencias

- Ley 8968. Ley de Protección de la persona frente al tratamiento de sus datos personales. Asamblea Legislativa de Costa Rica (2011). http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC
- Meta, (2024). Qué hacer cuando tu hijo(a) adolescente sufre de acoso online. https://familycenter.meta.com/latam/education/resources/how-can-parents-prevent-cyberbullying/
- Microsoft, (2024). ¿Qué es la ciberseguridad?. ¿https://www.microsoft.com/es-es/security/business/security-101/what-is-cybersecurity
- Microsoft, (2024). ¿Qué es la protección con contraseña?. https://www.microsoft.com/es-cl/security/business/security-101/what-is-password-protection
- NACIONAL CIBERSECURITY ALLIANCE (2022), Hablar con niños y adolescentes sobre seguridad y privacidad. https://staysafeonline.org/es/online-safety-privacy-basics/talking-to-kids-teens/
- NACIONAL CIBERSECURITY ALLIANCE (2024), Mes de la concientización sobre la ciberseguridad. https://www.cisa.gov/sites/default/files/2024-10/Cybersecurity-Awareness-Month-2024-Toolkit-Guide_ES.pdf
- NACIONAL CIBERSECURITY ALLIANCE, (2022). Control Parental. https://staysafeonline.org/es/online-safety-privacy-basics/parental-controls/
- NACIONAL CIBERSECURITY ALLIANCE, (2022). Formando ciudadanos digitales. https://staysafeonline.org/es/online-safety-privacy-basics/raising-digital-citizens/
- NACIONAL CIBERSECURITY ALLIANCE, (2022). Padres y educadores: Qué hacer con el ciberacoso. https://staysafeonline.org/es/online-safety-privacy-basics/cyberbullying-parents/
- TSE, (2021). Como ejercer una ciudadanía digital responsable. https%3A%2F%2Fwww.tse.go.cr%2Fpdf%2Fpublicaciones%2FC%25C3%25B3mo-ejercer-una-ciudadan%25C3%25ADa-digital-responsable.pdf
- UNICEF, (2022). Ciberacoso: qué es y cómo detenerlo. https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo#:~:text=Si%20te%20preocupa%20tu%20seguridad,de%20cuidadores%20capacitados%20y%20experimentados.
- UNICEF, (2022). Las 12 habilidades transferibles del Marco Conceptual y Programático. https%3A%2F%2Fwww.unicef.org%2Flac%2Fmedia%2F30756%2Ffile%2FLas%252012%2520habilidades%2520transferibles.pdf

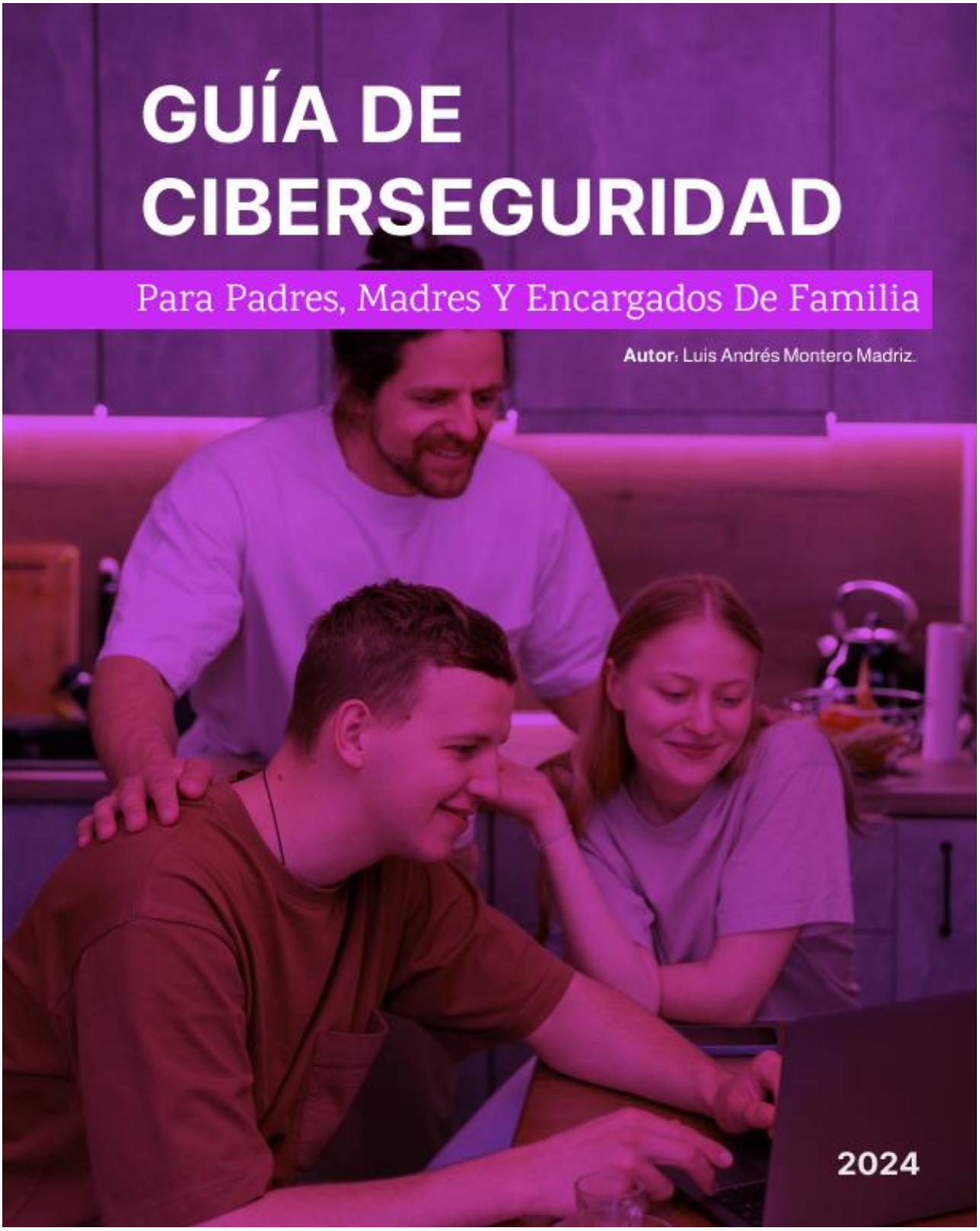
GUÍA DE CIBERSEGURIDAD

Para Estudiantes

Autor: Luis Andrés Montero Madriz.

2024

APÉNDICE F. GUÍA DE CIBERSEGURIDAD PARA PADRES DE FAMILIA Y ENCARGADOS DEL LICEO DE PAVAS



2

Guía de ciberseguridad para Padres, Madres y Encargados de Familia

La ciberseguridad es una responsabilidad compartida entre padres e hijos, y conocer las mejores prácticas es fundamental para protegerlos de las diferentes amenazas y los riegos en línea.

Esta guía de formación en ciberseguridad está diseñada para proporcionar a los padres las herramientas necesarias para educar y proteger a sus hijos en un entorno digital seguro y responsable.

La guía se desarrolló a partir de diversas referencias bibliográficas, adaptándose a la población objetivo mediante un lenguaje accesible para fomentar el aprendizaje autónomo. Con un diseño intuitivo y atractivo, se facilita la comprensión y transferencia del conocimiento, haciendo de este recurso una herramienta educativa valiosa en temas de ciberseguridad.

Contenido

Capítulo 1. Entendiendo el Mundo Digital

- ¿Qué es internet y cómo funciona?
- ¿Cómo usan internet mis hijos y su importancia?
- ¿Qué es la ciberseguridad y la importancia en la vida de los jóvenes?
- Principales amenazas en línea: phishing, malware y robo de identidad.
- Principales riesgos a las que se enfrentan los jóvenes: ciberacoso, sexting, grooming, publicación de información privada y fake news.
- Plataformas y dispositivos utilizados por los jóvenes para navegar.

Capítulo 2. Educando a Nuestros Jóvenes para un Futuro Seguro

- Aprendamos acerca de contraseñas seguras.
- ¿Cómo proteger los dispositivos personales de nuestros hijos?
- Manejo de la privacidad en las redes sociales.
- Importancia del uso de controles parentales.

Capítulo 3. Protegiendo a Nuestros Jóvenes de los Riesgos en Línea

- ¿Qué hacer si sus hijos sufren violencia en línea?
- Leyes que protegen a los jóvenes en el entorno digital.
- Consejos para educar jóvenes responsables en el entorno digital.

CAPÍTULO 1:
ENTENDIENDO EL MUNDO DIGITAL

Entender el mundo digital es fundamental para educar a sus hijos, se vuelve fundamental convertirse en guías para ellos, en el uso seguro y responsable de la tecnología, transformando los riesgos y amenazas en oportunidades de aprendizaje.

En este capítulo aprenderá:

- ¿Qué es internet y cómo funciona?
- ¿Cómo usan internet mis hijos y su importancia?
- ¿Qué es la ciberseguridad y la importancia en la vida de los jóvenes?
- **Principales amenazas en línea:** phishing, malware, robo de identidad.
- **Principales riegos a las que se enfrentan los jóvenes:** ciberacoso, sexting, grooming, publicación de información privada, fake news.
- Plataformas y dispositivos utilizados por los jóvenes para navegar.

CAPÍTULO 1:

ENTENDIENDO EL MUNDO DIGITAL

¿Qué es Internet y cómo funciona?

El internet es una red gigante que conecta a las personas, empresas, datos por medio de las computadoras y celulares en todo el mundo. ¡Es como una gran plaza donde todos pueden hablar y compartir información!.
Es importante como padres entender qué es y cómo lo usan sus hijos.

¿Qué es la ciberseguridad y la importancia en la vida de los jóvenes?

La ciberseguridad es el conjunto de prácticas y herramientas diseñadas para proteger los sistemas, redes y datos de los ataques o accesos no autorizados en el mundo digital.
A medida que los jóvenes pasan más tiempo en línea, se vuelve crucial enseñarles a proteger su privacidad, evitar fraudes y comportarse de manera responsable.

¿Cómo usan Internet mis hijos y su importancia?

Internet es un lugar donde nuestros hijos estudian, juegan, ven videos, leen, conocen personas, se comunican con sus amigos, entre otros. Es importante para ellos porque les permite aprender cosas nuevas y mantenerse conectados con el mundo.

CAPÍTULO 1: ENTENDIENDO EL MUNDO DIGITAL

Principales amenazas en línea: phishing, malware, robo de identidad.

MALWARE:

Es un tipo de programa diseñado para causar daño a sus dispositivos como computadoras, tablets y teléfonos celulares. Puede provocar desde la pérdida de datos hasta que tomen el control total de sus dispositivos.

Es esencial que eduquen a sus hijos sobre el riesgo del malware y cómo prevenirlo, como evitar hacer clic en enlaces sospechosos y mantener actualizados los programas de seguridad en sus dispositivos.

PISHING:

Es un tipo de ciberataque donde los delincuentes intentan engañar a una persona para que revele información personal, como contraseñas o datos bancarios.

Normalmente, lo hacen haciéndose pasar por una entidad legítima, enviando correos electrónicos o mensajes que parecen reales, pero que en realidad son falsos. Es importante que alerten a sus hijos sobre estos riesgos y les enseñen a no compartir información personal en respuesta a correos o enlaces sospechosos.

ROBO DE IDENTIDAD:

Ocurre cuando alguien utiliza la información personal de una persona sin su consentimiento, con el fin de cometer fraude o engaño. Esto puede ser preocupante en el caso de los jóvenes, donde la información puede ser utilizada para abrir cuentas bancarias, solicitar tarjetas de crédito o incluso obtener préstamos.

Es crucial que los padres tomen medidas, como monitorear la información personal de sus hijos y educarlos sobre la importancia de proteger sus datos.

CAPÍTULO 1: ENTENDIENDO EL MUNDO DIGITAL

Principales riesgos a los que se enfrentan los jóvenes: ciberacoso, sexting, grooming, publicación de información privada, fake news.

CIBERACOSO:

El ciberacoso es un tipo de acoso o intimidación que se realiza por medio de tecnologías digitales. Desde dispositivos como teléfonos móviles, computadoras y tablets, y puede manifestarse en diversas plataformas, como redes sociales, aplicaciones de mensajería y foros en línea.

Señales de Ciberacoso

- Envío repetido de mensajes agresivos o amenazantes a los jóvenes a través de redes sociales o aplicaciones de mensajería.
- Se hacen pasar por otra persona en línea para enviar mensajes perjudiciales o crear confusión.
- Publican información personal del joven sin su consentimiento, como direcciones, números de teléfono o fotos privadas, para causar daño o vergüenza.
- Crean perfiles falsos en redes sociales para engañar o manipular a los jóvenes.

Consecuencias del ciberacoso
El ciberacoso puede tener efectos irreversibles en sus hijos, es importante que hable con ellos del tema, preguntarles si han sido víctimas, algunas consecuencias son:

- Si sus hijos son víctimas de esta amenaza pueden experimentar ansiedad, depresión y estrés severo, afectando su bienestar emocional y mental.
- El acoso constante puede llevar a una disminución de la autoconfianza, lo que afecta su desarrollo personal y social.
- El joven puede mostrar tristeza, nerviosismo o desmotivación para asistir al colegio.
- Los jóvenes que sufren de ciberacoso a menudo se sienten marginadas y pueden evitar situaciones sociales.
- En casos extremos, el ciberacoso puede llevar a los jóvenes a auto lastimarse o tener pensamientos suicidas.
- Los efectos del ciberacoso pueden incluir trastornos del sueño, afectando aún más la salud general de las víctimas.

CAPÍTULO 1: ENTENDIENDO EL MUNDO DIGITAL

GROMMING:

El grooming es una práctica en la que un adulto utiliza Internet para establecer una relación de confianza con un menor, con el objetivo de manipularlo y, en algunos casos, abusar sexualmente de él. Esta interacción se realiza a través de diversas plataformas digitales, como redes sociales, chats y juegos en línea.

Incluye varias fases, que van desde el acercamiento y la construcción de confianza hasta la desensibilización del menor hacia contenido sexual. A menudo, el agresor puede hacerse pasar por un joven para facilitar la conexión con la víctima y, posteriormente, enviarle material sexual o solicitarle que envíe imágenes comprometedoras.

SEXTING:

El sexting consiste en enviar y recibir contenido sexual o erótico a través de dispositivos tecnológicos, como teléfonos móviles y computadoras. Este contenido puede incluir mensajes de texto, fotos, videos, que muestran desnudos u otras imágenes de naturaleza íntima.

El sexting también conlleva riesgos, como la posibilidad de que el contenido se comparta sin consentimiento, lo que podría resultar en humillación, acoso o problemas legales.

FAKE NEWS:

Son información engañosa o falsa presentada como si fuera verdadera, se difunden por medio de las redes sociales, sitios web y otros medios de comunicación, y pueden tener un impacto significativo en la opinión pública y el comportamiento de los jóvenes.

Es fundamental enseñar a sus hijos a reconocer las fake news, verificando las fuentes de información y buscando hechos antes de compartir o creer en lo que leen.

PUBLICACIÓN DE INFORMACIÓN PRIVADA:

Consiste en compartir datos personales como nombres, direcciones, números de teléfono y fotos en redes sociales o plataformas digitales.

Es fundamental educar a los jóvenes sobre la importancia de mantener su información privada, deben aprender a reconocer qué información no deben compartir y ajustar sus configuraciones de privacidad en las plataformas que utilizan.

CAPÍTULO 1: ENTENDIENDO EL MUNDO DIGITAL

Plataformas y dispositivos utilizados por los jóvenes para navegar.

Redes Sociales

Instagram: Compartir fotos, historias y mensajes directos.

Snapchat: Envío de fotos y videos que desaparecen, con filtros populares.

TikTok: Videos cortos, a menudo de tendencias, música y comedia.

Facebook: Menos común entre los jóvenes, pero algunos lo usan para grupos y comunicación.

Plataformas de Mensajería

WhatsApp: Utilizado para mensajería y llamadas.

Messenger: Relacionado con Facebook, para chatear.

Plataformas de Streaming:

YouTube: Videos, tutoriales, entretenimiento y música.

Netflix, Disney+, Amazon Prime Video: Películas y series.

CAPÍTULO 1:
ENTENDIENDO EL MUNDO DIGITAL

Plataformas y dispositivos utilizados por los jóvenes para navegar.

Dispositivos

Celular: Son los dispositivos más populares entre los jóvenes porque se llevan a todo lado y por la cantidad de funciones que ofrecen. Se pueden usar para acceder a internet, redes sociales, aplicaciones de mensajería, juegos y contenido multimedia.
Riesgos:

- Genera problemas de adicción, ciberacoso u otros.
- Riesgo a la privacidad.
- Falta de control parental puede exponer a contenido inapropiado.

Tabletas: Son dispositivos similares a los teléfonos inteligentes, pero con pantallas más grandes, lo que las hace ideales para juegos, ver videos y realizar tareas escolares.
Riesgos:

- Tiempo de pantalla prolongado, especialmente en juegos y videos.
- Compras dentro de las aplicaciones sin supervisión.
- Falta de supervicion puede dar acceso a contenido inapropiado.

Laptops/Computadoras: Son herramientas multifuncionales que los jóvenes usan tanto para el estudio o el entretenimiento. Son potentes y ofrecen un acceso completo a internet y a una variedad de software.
Riesgos:

- Exposición a todo tipo de ciberacoso en redes sociales.
- Exposición a pishing, virus y malware si no se tiene un buen software de seguridad.
- Distracción de tareas escolares.

Consolas: Las consolas de videojuegos también permiten la navegación de internet, ya que muchas cuentan con navegadores web y acceso a plataformas como YouTube y servicios de streaming.
Riesgos:

- Interacción con desconocidos a través de los juegos.
- Compras online.
- Exposición a todo tipo de páginas o juegos.
- Problemas de adicción.

CAPÍTULO 2:

EDUCANDO A NUESTROS JÓVENES PARA UN FUTURO SEGURO

El bienestar de sus hijos también depende de su seguridad en línea, es necesario guiarlos en la implementación de prácticas seguras en el entorno digital, creando una cultura de seguridad y responsabilidad en el uso de la tecnología.

En este capítulo aprenderá:

- Aprendamos acerca de contraseñas seguras.
- ¿Cómo proteger los dispositivos personales de sus hijos?
- Manejo de la privacidad en las redes sociales.
- Importancia del uso de controles parentales.

CAPÍTULO 2:

EDUCANDO A NUESTROS JÓVENES PARA UN FUTURO SEGURO

Aprendamos acerca de contraseñas seguras

- Enséñele a su hijo que debe crear una contraseña larga, única y fácil de recordar. Debe ser fácil de recordar para ti, pero difícil de adivinar para otros.
- Las contraseñas deben tener como mínimo ocho caracteres.
- Debe incluir mayúsculas, minúsculas, números y símbolos especiales para aumentar la seguridad de la contraseña.
- No utilizar nombres, fechas o datos fáciles de adivinar, lo ideal es usar algo único y sin relación con algo personal.
- No repetir contraseñas en diferentes plataformas, si se le complica recordarlas, usar un administrador de contraseñas.
- Una frase larga puede ser más fácil de recordar y suficientemente segura, especialmente si incluye varios tipos de caracteres.

¿CÓMO PROTEGER DISPOSITIVOS PERSONALES DE NUESTROS HIJOS?

- Asegúrese de que todos los dispositivos tengan un software antivirus confiable instalado y actualizado, esto ayuda a detectar y eliminar malware y otras amenazas en línea.
- Debe realizar actualizaciones regulares del sistema operativo y de las aplicaciones, ya que contiene mejoras de seguridad que protegen contra nuevas amenazas
- Una buena práctica es la ejecución de respaldos de la información, ya sea por medio de la nube o de discos duros externos.
- Verifique las configuraciones de seguridad de cada dispositivo, las configuraciones predeterminadas pueden no ser las más seguras.
- Habilite la autenticación de dos factores en las cuentas, el primer factor es normalmente la contraseña, el segundo puede ser un código enviado a un dispositivo móvil o una aplicación de autenticación.

CAPÍTULO 2:
EDUCANDO A NUESTROS JÓVENES PARA UN FUTURO SEGURO

Manejo de la privacidad en las redes sociales

- Asegúrese de leer y entender las políticas de privacidad de las plataformas que usen sus hijos antes de crear sus perfiles.
- Personalice la configuración de privacidad para limitar la visibilidad de su información.
- Enséñeles a sus hijos a configurar sus cuentas en redes sociales como privadas, permitiendo solo a personas conocidas ver sus publicaciones y actividades.
- Defínale las reglas sobre lo que puede y no puede compartir en línea, fotos, videos, conversaciones, ubicaciones y datos personales.
- Es importante que los padres se mantengan al tanto de las nuevas aplicaciones y tendencias en redes sociales para comprender los riesgos y oportunidades que enfrentan sus hijos.
- Revise y asegúrese de que sus hijos solo acepten solicitudes de amistad de personas que conocen personalmente.
- Pregúnteles regularmente con quién están hablando y qué información están compartiendo, el dialogo abierto con sus hijos es fundamental.

CAPÍTULO 2:
EDUCANDO A NUESTROS JÓVENES PARA UN FUTURO SEGURO

IMPORTANCIA DEL USO DE CONTROLES PARENTALES

Muchos padres no conocen a los sitios o información que acceden sus hijos. En internet existe mucho contenido inapropiado para sus hijos, los controles parentales son herramientas que le ayudan a supervisar y gestionar este contenido.

Esto permite configuras límites de tiempo en el uso de dispositivos y aplicaciones, así puede evitar el uso excesivo de la tecnología por parte de sus hijos.

Es recomendable establecer cuentas de usuario separadas, una para los jóvenes y otra de administrador para los padres, esto ayuda a un mejor control y supervisión.

Existen varias plataformas digitales que ofrecen la opción de configurar controles parentales para ayudar a los padres a supervisar y restringir el contenido accesible a sus hijos, por ejemplo:

- **Servicios de streaming**: La mayoría de las plataformas como Netflix, Hulu y Disney+ tienen controles parentales integrados que permiten restringir el acceso a contenido inapropiado según la clasificación por edades.
- **Televisores inteligentes**: Las Smart TVs vienen con opciones de control parental que permiten a los padres limitar el acceso a ciertos canales o aplicaciones, y ajustar las configuraciones de contenido.
- **Plataformas de juegos**: Consolas como PlayStation y Xbox tienen configuraciones de control parental que permiten a los padres gestionar el tiempo de juego y el contenido al que pueden acceder sus hijos.
- **Dispositivos móviles**: Los sistemas operativos como Android y iOS tienen controles parentales que permiten gestionar el acceso a aplicaciones y contenido web, así como establecer límites de tiempo de uso.

Discute con tus hijos sobre las reglas establecidas y la importancia de los controles parentales. Esto promueve un uso más seguro y responsable de la tecnología.

CAPÍTULO 3:

PROTEGIENDO A NUESTROS JÓVENES DE LOS RIESGOS EN LÍNEA

Sus hijos se encuentran expuestos diariamente a múltiples riesgos en línea, es por esto que se vuelve fundamental tener los conocimientos necesarios para protegerlos, asegurando un entorno más seguro y responsable para su crecimiento.

En este capítulo aprenderá:

- ¿Qué hacer si sus hijos sufren de violencia en línea?
- Leyes que protegen a los jóvenes en el entorno digital.
- Consejos para educar jóvenes responsables en el entorno digital.

CAPÍTULO 3:

PROTEGIENDO A NUESTROS JÓVENES DE LOS RIESGOS EN LÍNEA

¿Qué hacer si sus hijos sufren violencia en línea?

1. Ayude a su hijo a reconocer las diferentes formas de violencia en línea, como el ciberacoso, para que pueda entender y diferenciar lo que está sucediendo.
2. Hable con ellos sobre lo que están experimentando, escuchándolos sin juzgar puede ayudar a que se sientan más cómodos compartiendo sus problemas, escuche sus preocupaciones y valide sus sentimientos.
3. Anime a su hijo a guardar pruebas del acoso, como capturas de pantalla de mensajes o publicaciones ofensivas. Esto puede ser útil al reportar el problema a las autoridades pertinentes.
4. Dependiendo de la plataforma donde ocurre el acoso, instruya a su hijo a usar las funciones de reporte. También considere informar al colegio si el acoso está relacionado al centro educativo.
5. Si el acoso tiene un impacto significativo en la salud emocional de su hijo, no dude en buscar ayuda de un psicólogo o un consejero especializado.
6. Ayude a su hijo a desarrollar estrategias para manejar el acoso, como ignorar a los acosadores o bloquear a las personas que lo hostigan.

CAPÍTULO 3: PROTEGIENDO A NUESTROS JÓVENES DE LOS RIESGOS EN LÍNEA

Leyes que protegen a los jóvenes en el entorno digital

LEY 9048 de delitos informáticos

La ley busca prevenir, sancionar y combatir delitos como el acceso no autorizado a sistemas informáticos, la usurpación de identidad, y la difusión de contenido perjudicial o ilegal.

La ley establece que, si un menor de edad comete un delito informático, sus padres pueden ser considerados responsables, por esto es necesario supervisar y educar a los hijos sobre el uso adecuado de la tecnología y las redes sociales.

Estos delitos tienen penas de prisión de uno a cuatro años, dependiendo de la gravedad del acto y el daño causado a la intimidad de otra persona.

Es esencial que los padres conversen con sus hijos sobre los riesgos del uso irresponsable de internet y cómo prevenir ser víctimas o perpetradores de delitos informáticos.

LEY 8968 de protección de la persona frente al tratamiento de sus datos personales

La ley garantiza el derecho de las personas a la privacidad y la autodeterminación informativa, lo que significa que los padres deben ser conscientes de cómo se manejan los datos personales de sus hijos y asegurar que se respete su privacidad.

Para el tratamiento de datos personales de los jóvenes se requiere el consentimiento de los padres o tutores.

Existen sanciones para quienes utilicen o divulguen datos personales sin consentimiento, esto incluye multas que pueden llegar hasta los treinta salarios base.

Al educarse sobre esta ley, pueden tomar decisiones informadas y ayudar a proteger la privacidad de sus hijos en el entorno digital.

CAPÍTULO 3: PROTEGIENDO A NUESTROS JÓVENES DE LOS RIESGOS EN LÍNEA

LEY 10238 de protección de la imagen, la voz y los datos personales de las personas menores de edad

La ley garantiza la protección de la integridad física y moral de los menores, prohibiendo la divulgación no autorizada de sus datos, imágenes o voz. Esto busca evitar la explotación y proteger su privacidad en medios digitales y tradicionales.

La divulgación de cualquier imagen, voz o dato personal de un menor requiere el consentimiento explícito de los padres o tutores legales. La falta de este consentimiento puede resultar en sanciones para los responsables.

LEY 8934 protección de la niñez y la adolescencia en internet

La ley busca salvaguardar los derechos de los menores frente a la exposición a contenidos perjudiciales que pueden afectar su desarrollo.

Los padres son responsables de supervisar y guiar el uso que le dan sus hijos al Internet, fomentando un uso seguro y responsable.

CAPÍTULO 3: PROTEGIENDO A NUESTROS JÓVENES DE LOS RIESGOS EN LÍNEA

CONSEJOS PARA EDUCAR JÓVENES RESPONSABLES EN EL ENTORNO DIGITAL

- Fomente un ambiente donde tus hijos se sientan cómodos compartiendo sus experiencias en línea y escucha sus preocupaciones sobre el ciberacoso y valida sus sentimientos.
- Defina reglas sobre el uso de dispositivos y redes sociales, esto incluye tiempos de uso y qué plataformas son apropiadas.
- Anime a sus hijos a considerar los sentimientos de los demás y a practicar la empatía en sus interacciones en línea. Hazles entender que detrás de cada pantalla hay una persona real.
- Explíquele a su hijo que cualquier foto, video y comentarios que ellos publiquen en internet podría permanecer para siempre y otras personas podrían compartirlos o usarlos de manera indebida.
- Explíquele a su hijo que las personas pueden crear perfiles falsos y fingir que son alguien que no son. Algunas veces los adultos hacen esto para contactar menores.
- Enséñele a su hijo a tener cuidado sobre lo que revela a las personas que no conoce en la vida real.
- Inste a su hijo a que le cuente de inmediato si alguien que ha conocido en línea pide encontrarse con él o ella.
- Enséñele a tratar a los demás con respeto. Ínstelo a no responder ni hacer comentarios sobre publicaciones hirientes.
- Ayúdele a pensar en cómo enfrentar la atención indeseada, como pedidos de información o fotos personales. Esto podría incluir bloquear a la persona y contarle a usted o a otro adulto de confianza.
- Hable sobre las clases de sitios y aplicaciones que su hijo puede usar y cuándo puede estar conectado con ellos.
- Ayude a su hijo a comprender que los límites en el uso de las redes sociales no tienen como fin castigarlo. Los límites son para ayudarle a mantenerse seguro y a que tenga un equilibrio saludable en su vida.
- Padres muestren interés de las actividades que realizan sus hijos en línea y estén dispuestos a escucharlos.
- Anime a sus hijos a tomar descansos de las pantallas y a ser conscientes de su bienestar emocional al usar la tecnología.

Referencias

- Checkpoint, (2024). Tipos de amenazas de ciberseguridad. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security
- GOB, (2024). Guía de ciberseguirdad. https://www.gob.mx/cms/uploads/attachment/file/896412/Gu_a_de_Ciberseguridad_en_apoyo_a_la_educaci_n.pdf
- HealthyChildren.org, (2022). "Sexteo": cómo hablar con sus hijos del riego de enviar mensajes con contenido sexual. https://www.healthychildren.org/Spanish/family-life/Media/Paginas/the-new-problem-of-sexting.aspx
- https://latam.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online
- INCIBE, (2024). Ciberseguridad para familias. https://www.incibe.es/menores/familias/ciberseguridad
- INCIBE, (2024). Configura correctamente tu dispositivo y asegura tu información. https://www.incibe.es/ciudadania/tags/configuraci%C3%B3n%20segura
- INCIBE, (2024). Grooming. https://www.incibe.es/menores/tematicas/grooming
- INCIBE, (2024). Las redes sociales como herramienta para ciberdelincuentes. https://www.incibe.es/ed2026/talento-hacker/blog/las-redes-sociales-como-herramienta-para-ciberdelincuentes
- INCIBE, (2024). Privacidad. https://www.incibe.es/menores/tematicas/privacidad
- INCIBE, (2024). Sexting. https://www.incibe.es/menores/tematicas/sexting
- Kaspersky, (2024). Cómo identificar noticias falsas. https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-identify-fake-news
- Kaspersky, (2024). Las 15 mejores reglas de seguridad y qué no hacer en línea.
- Ley 10238. Ley de protección de la imagen, la voz y los datos personales de las personas menores de edad. Asamblea Legislativa de Costa Rica (2022). http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=97506&nValor3=131719&strTipM=TC
- Ley 7739. Código de la Niñez y la Adolescencia, Asamblea Legislativa de Costa Rica (1998). http://www.pgrweb.go.cr/scij/busqueda/normativa/normas/nr m_texto_completo.aspx?param2=1&nValor1=1&nValor2=43077&lResultado=4&strSelect=sel
- Ley 8934. Ley de Protección de la Niñez y la Adolescencia frente al contenido nocivo de Internet y otros medios electrónicos. Asamblea Legislativa de Costa Rica (2011). http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=71024&nValor3=0

Referencias

- Ley 8968. Ley de Protección de la persona frente al tratamiento de sus datos personales. Asamblea Legislativa de Costa Rica (2011). http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC
- Meta, (2024). Qué hacer cuando tu hijo(a) adolescente sufre de acoso online. https://familycenter.meta.com/latam/education/resources/how-can-parents-prevent-cyberbullying/
- Microsoft, (2024). ¿Qué es la ciberseguridad?. ¿https://www.microsoft.com/es-es/security/business/security-101/what-is-cybersecurity
- Microsoft, (2024). ¿Qué es la protección con contraseña?. https://www.microsoft.com/es-cl/security/business/security-101/what-is-password-protection
- NACIONAL CIBERSECURITY ALLIANCE (2022), Hablar con niños y adolescentes sobre seguridad y privacidad. https://staysafeonline.org/es/online-safety-privacy-basics/talking-to-kids-teens/
- NACIONAL CIBERSECURITY ALLIANCE (2024), Mes de la concientización sobre la ciberseguridad. https://www.cisa.gov/sites/default/files/2024-10/Cybersecurity-Awareness-Month-2024-Toolkit-Guide_ES.pdf
- NACIONAL CIBERSECURITY ALLIANCE, (2022). Control Parental. https://staysafeonline.org/es/online-safety-privacy-basics/parental-controls/
- NACIONAL CIBERSECURITY ALLIANCE, (2022). Formando ciudadanos digitales. https://staysafeonline.org/es/online-safety-privacy-basics/raising-digital-citizens/
- NACIONAL CIBERSECURITY ALLIANCE, (2022). Padres y educadores: Qué hacer con el ciberacoso. https://staysafeonline.org/es/online-safety-privacy-basics/cyberbullying-parents/
- TSE, (2021). Como ejercer una ciudadanía digital responsable. https%3A%2F%2Fwww.tse.go.cr%2Fpdf%2Fpublicaciones%2FC%25C3%25B3mo-ejercer-una-ciudadan%25C3%25ADa-digital-responsable.pdf
- UNICEF, (2022). Ciberacoso: qué es y cómo detenerlo. https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo#:~:text=Si%20te%20preocupa%20tu%20seguridad,de%20cuidadores%20capacitados%20y%20experimentados.
- UNICEF, (2022). Las 12 habilidades transferibles del Marco Conceptual y Programático. https%3A%2F%2Fwww.unicef.org%2Flac%2Fmedia%2F30756%2Ffile%2FLas%252012%2520habilidades%2520transferibles.pdf

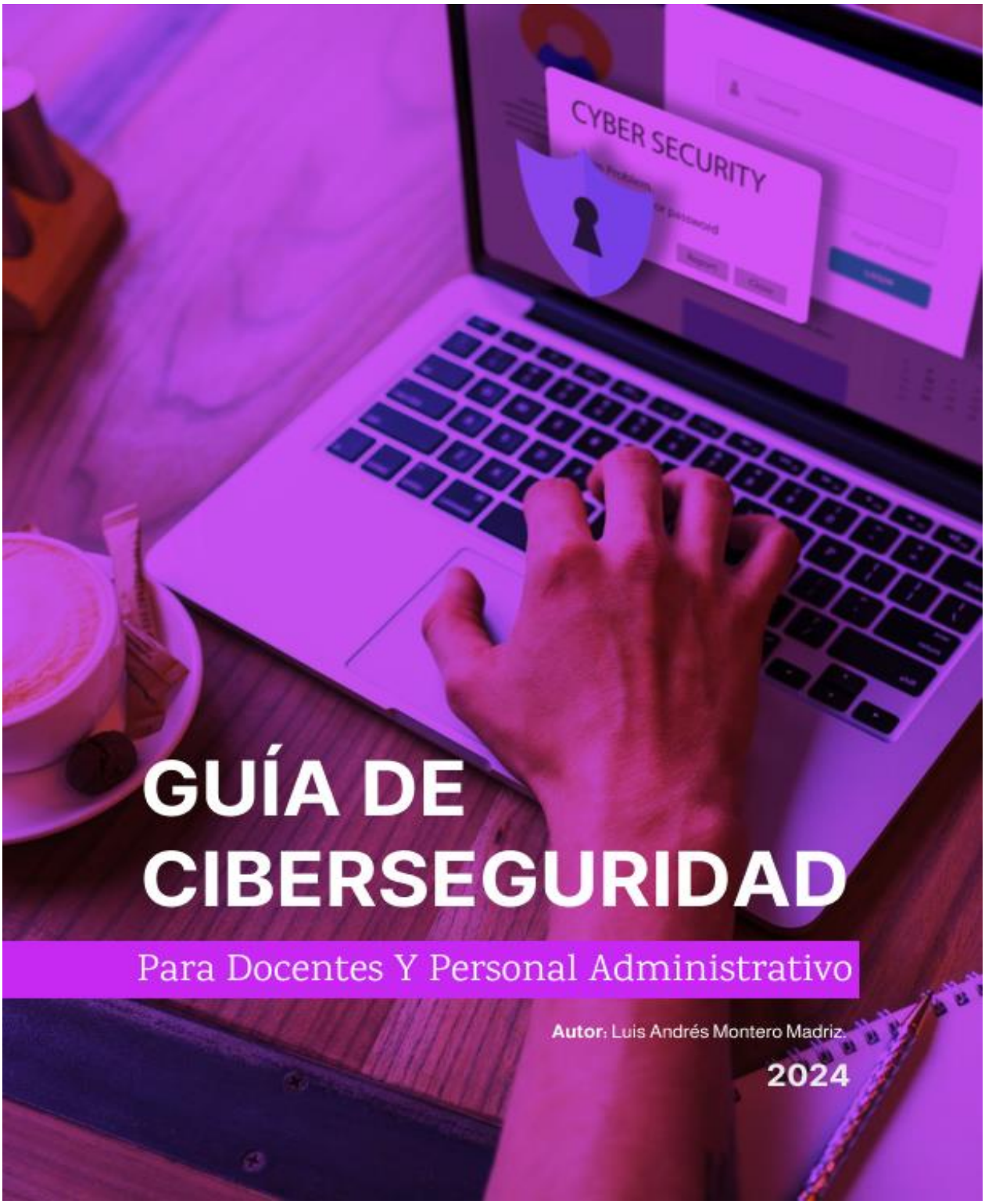
GUÍA DE CIBERSEGURIDAD

Para Padres, Madres Y Encargados De Familia

Autor: Luis Andrés Montero Madriz.

2024

APÉNDICE F. GUÍA DE CIBERSEGURIDAD PARA PROFESORES Y PERSONAL ADMINISTRATIVO DEL LICEO DE PAVAS



Guía de ciberseguridad para Docentes y Personal Administrativo

Esta guía de formación en ciberseguridad tiene como propósito principal suministrar a los docentes y personal administrativo, el conocimiento en fundamentos en ciberseguridad, con el fin de incentivar a los estudiantes a que desarrollen habilidades en la protección y privacidad de sus datos personales, así como a identificar los riesgos y amenazas en línea, promoviendo un aprendizaje responsable y crítico sobre el uso de tecnologías digitales.

La guía se desarrolló a partir de diversas referencias bibliográficas, adaptándose a la población objetivo mediante un lenguaje accesible para fomentar el aprendizaje autónomo. Con un diseño intuitivo y atractivo, se facilita la comprensión y transferencia del conocimiento, haciendo de este recurso una herramienta educativa valiosa en temas de ciberseguridad.

Contenido

Capítulo 1. La Ciberseguridad y la Educación

- La ciberseguridad y su importancia en el rol de docente.
- Formas de interactuar por los adolescentes en el mundo digital.
- Respeto, ética y responsabilidad en línea.

Capítulo 2. Riesgos y Amenazas en el Entorno Digital

- Principales amenazas en línea: phishing, malware, robo de identidad.
- Riesgos a las que se enfrentan los jóvenes: ciberacoso, sexting, grooming, publicación de información privada, fake news.

Capítulo 3. Protección de Dispositivos y Datos Personales

- Crear y gestionar contraseñas seguras.
- ¿Cómo proteger sus dispositivos personales?
- Manejo de la privacidad en las redes sociales.
- Leyes que protegen a los jóvenes en el entorno digital

Capítulo 4. Fomentando el Interés en Carreras en Ciberseguridad

- Papel que juegan los docentes en fomentar el interés por las carreras tecnológicas.

CAPÍTULO 1:

LA CIBERSEGURIDAD Y LA EDUCACIÓN

La ciberseguridad va más allá que solo proteger datos; es empoderar a sus estudiantes para que se conviertan en ciudadanos digitales responsables y críticos en un entorno interconectado.

En este capítulo aprenderá:

- La ciberseguridad y su importancia en el rol de docente.
- Formas de interactuar de los adolescentes en el mundo digital.
- Respeto, ética y responsabilidad en línea.

CAPÍTULO 1:

LA CIBERSEGURIDAD Y LA EDUCACIÓN

¿Qué es la ciberseguridad y por qué es importante en el rol de docente?

La ciberseguridad trata de proteger los sistemas, redes y datos de posibles ataques digitales. Además, enseña acerca del manejo de la información sensible de estudiantes y cómo protegerla.

Los estudiantes deben ser educados sobre prácticas seguras, ya que existen muchos peligros en línea, por esto es importante que los docentes comprendan a que se enfrentan los jóvenes, para educarlos y ayudarlos a prevenir:

- Acoso a través de las redes sociales o mensajería, que puede impactar negativamente la autoestima y bienestar de los adolescentes.
- Los jóvenes pueden acceder a información falsa, violencia o contenidos sexuales sin filtros adecuados.
- El uso excesivo de las plataformas digitales puede provocar aislamiento social, baja concentración y dependencia de internet.
- Los adolescentes pueden ser víctimas de adultos que buscan establecer relaciones con fines sexuales por medio de engaños.

Es importante que los docentes fomenten un uso responsable de la tecnología y promuevan habilidades para que los jóvenes identifiquen y eviten estos riesgos.

CAPÍTULO 1:
LA CIBERSEGURIDAD Y LA EDUCACIÓN

¿Cómo interactúan los adolescentes en el mundo digital?

Los adolescentes interactúan en el mundo digital por medio de las redes sociales, videojuegos, plataformas de mensajería y sitios de entretenimiento.

Estas plataformas les permiten conectarse con amigos, explorar intereses y expresarse libremente, esto trae consigo beneficios, pero al mismo tiempo una responsabilidad como ciudadanos digitales.

FORMAS DE COMUNICACIÓN Y COMPORTAMIENTO EN LÍNEA:

- Interacción instantánea.
- Creación de identidad digital.
- Exposición a tendencias y retos.
- Amistades en línea.
- Influencia de los "influencers".

6

PLATAFORMAS MÁS USADAS POR LOS ESTUDIANTES:

Estas plataformas permiten a los jóvenes comunicarse, expresarse, y crear contenido, pero también pueden exponerlos a riesgos como el ciberacoso o contacto con personas desconocidas.

Redes sociales: Instagram, TikTok, Snapchat, Facebook.
Mensajería: WhatsApp, Telegram, Messenger.
Entretenimiento: YouTube, Twitch.
Videojuegos en línea: Fortnite, Roblox, Minecraft (con componentes sociales y de interacción en línea).

RESPETO, ÉTICA Y RESPONSABILIDAD EN LÍNEA

Los docentes juegan un rol muy importante en la enseñanza del sano y responsable comportamiento que deben tener los jóvenes en el mundo digital.
¿Cómo enseñar a los jóvenes a ser ciudadanos digitales responsables?

- Enseñar a los jóvenes a poner en práctica la empatía a través de la escucha activa y el diálogo sano en línea, comprendiendo los puntos de vista de sus compañeros.
- Instruir a los estudiantes sobre el respeto de las interacciones digitales, y el evitar comentarios ofensivos, manteniendo una comunicación educada.
- Realizar actividades en clase donde los estudiantes se pongan en el lugar del otro, bajo escenarios inapropiados.

CAPÍTULO 2:

RIESGOS Y AMENAZAS EN EL ENTORNO DIGITAL

En un mundo donde la tecnología avanza de manera acelerada, es esencial que como educadores comprendan los riesgos y amenazas en el entorno digital, para poder guiar a sus estudiantes hacia un uso seguro y responsable de las herramientas digitales.

En este capítulo aprenderá:

- **Principales amenazas en línea**: phishing, malware, robo de identidad.
- **Riesgos a las que se enfrentan los jóvenes**: ciberacoso, sexting, grooming, publicación de información privada, fake news.

8

CAPÍTULO 2:

RIESGOS Y AMENAZAS EN EL ENTORNO DIGITAL

Principales amenazas en línea: phishing, malware, robo de identidad.

MALWARE:

Es un tipo de programa diseñado para causar daño a sus dispositivos como computadoras, tablets y teléfonos celulares. Puede provocar desde la pérdida de datos hasta que tomen el control total de sus dispositivos.

Es esencial que eduquen a los estudiantes sobre el riesgo del malware y cómo prevenirlo, como evitar hacer clic en enlaces sospechosos y mantener actualizados los programas de seguridad en sus dispositivos.

ROBO DE IDENTIDAD:

Ocurre cuando alguien utiliza la información personal de una persona sin su consentimiento, con el fin de cometer fraude o engaño. Esto puede ser preocupante en el caso de los jóvenes, donde la información puede ser utilizada para abrir cuentas bancarias, solicitar tarjetas de crédito o incluso obtener préstamos.

PISHING:

Es un tipo de ciberataque donde los delincuentes intentan engañar a una persona para que revele información personal, como contraseñas o datos bancarios. Normalmente, lo hacen haciéndose pasar por una entidad legítima, enviando correos electrónicos o mensajes que parecen reales, pero que en realidad son falsos.

La educación sobre phishing es fundamental para ayudar a los estudiantes a reconocer y evitar este tipo de ataques cibernéticos. Algunas señales de un correo sospechoso son:

- URL incorrectas o extrañas.
- Solicitudes de información personal.
- Errores de ortografía y gramática en el mensaje.

¿Cómo evitar ser víctimas de pishing?

- No dar clic a enlaces sospechosos.
- Verificar la dirección del remitente.
- Utilizar contraseñas fuertes y únicas.

CAPÍTULO 2:
RIESGOS Y AMENAZAS EN EL ENTORNO DIGITAL

Principales riesgos a los que se enfrentan los jóvenes: ciberacoso, sexting, grooming, publicación de información privada, fake news.

CIBERACOSO:

Es un tipo de acoso o intimidación que se realiza por medio de tecnologías digitales. Desde dispositivos como teléfonos móviles, computadoras y tablets, y puede manifestarse en diversas plataformas, como redes sociales, aplicaciones de mensajería y foros en línea.

¿Cómo identificar el ciberacoso en los estudiantes?

- Baja autoestima, ansiedad, depresión o aislamiento social. Se puede notar una disminución en el rendimiento escolar y el interés por actividades cotidianas.
- Publicaciones, mensajes o fotos maliciosas, humillantes o dañinas hacia un estudiante. Esto incluye burlas, amenazas, o la difusión de rumores.
- Deterioro en las relaciones con compañeros, familiares o amigos.

¿Qué hacer sin un estudiante sufre de ciberacoso?

- Promover una cultura de respeto, donde los estudiantes se sientan seguros para reportar el ciberacoso.
- Identificar y abordar el comportamiento, contactando a los padres y ofreciendo apoyo psicológico al estudiante afectado.
- Enseñar a los estudiantes sobre privacidad, respeto en línea y las consecuencias del acoso.
- Revisar las plataformas digitales usadas en el aula para evitar situaciones de acoso.

GROOMING:

Es una práctica en la que un adulto utiliza Internet para establecer una relación de confianza con un menor, con el objetivo de manipularlo y, en algunos casos, abusar sexualmente de él. Esta interacción se realiza a través de diversas plataformas digitales, como redes sociales, chats y juegos en línea.

A menudo, el agresor puede hacerse pasar por un joven para facilitar la conexión con la víctima y, posteriormente, enviarle material sexual o solicitarle que envíe imágenes comprometedoras.

¿Qué hacer sin un estudiante sufre de grooming?

- Guardar mensajes, imágenes o videos relacionados como prueba. Esto es importante para las autoridades cuando se realice la denuncia.
- Es fundamental informar inmediatamente a las autoridades, ya que el grooming es un delito.
- Es importante que los padres estén informados de la situación para que puedan acompañar al menor y tomar medidas de protección adicionales en casa.
- El equipo de orientación del colegio debe brindar apoyo emocional al menor para ayudarlo a gestionar el impacto de la amenaza.

CAPÍTULO 2:
RIESGOS Y AMENAZAS EN EL ENTORNO DIGITAL

SEXTING:

Consiste en enviar y recibir contenido sexual o erótico a través de dispositivos tecnológicos, como teléfonos móviles y computadoras. Este contenido puede incluir mensajes de texto, fotos, videos, que muestran desnudos u otras imágenes de naturaleza íntima.

Riesgos asociados al sexting

- Una vez que se comparte una imagen o video, se pierde el control sobre su difusión.
- Crear, compartir o poseer imágenes de contenido sexual explícito de menores puede tener consecuencias legales graves.
- Los adolescentes pueden sufrir problemas psicológicos como depresión, baja autoestima y estrés al enfrentarse a la exposición de su intimidad.
- El contenido compartido en internet puede influir en las oportunidades futuras de empleo o estudios, afectando su reputación digital.

FAKE NEWS:

Son información engañosa o falsa presentada como si fuera verdadera, se difunden por medio de las redes sociales, sitios web y otros medios de comunicación, y pueden tener un impacto significativo en la opinión pública y el comportamiento de los jóvenes.

- Es fundamental enseñar a los estudiantes a reconocer las fake news, verificando las fuentes de información y buscando hechos antes de compartir o creer en lo que leen.
- Enseñar acerca de herramientas y sitios web de verificación de noticias para confirmar la veracidad.
- Es necesario hacerse preguntas como: ¿Quién las publica? ¿Cuál es la fuente de la información? ¿Existe evidencia que la respalde?

PUBLICACIÓN DE INFORMACIÓN PRIVADA:

Consiste en compartir datos personales como nombres, direcciones, números de teléfono y fotos en redes sociales o plataformas digitales.Es fundamental educar a los jóvenes sobre la importancia de mantener su información privada, deben aprender a reconocer qué información no deben compartir y ajustar sus configuraciones de privacidad en las plataformas que utilizan, algunas consecuencias son:

- La información personal, como direcciones, números de teléfono y datos escolares, puede ser utilizada por personas malintencionadas para el ciberacoso o el robo de identidad.
- Una vez que algo se publica en línea, puede ser difícil eliminarlo. La información puede ser compartida o viralizada sin el consentimiento de quién la subió.
- La publicación de información privada puede llevar a situaciones de acoso y dañar la reputación del estudiante, afectando su autoestima y bienestar.

CAPÍTULO 3:

PROTECCIÓN DE DISPOSITIVOS Y DATOS PERSONALES

La protección de dispositivos y datos personales es una responsabilidad colectiva, educar a sus estudiantes sobre estas prácticas no solo los empodera, sino que también crea una cultura de seguridad y responsabilidad en el uso de la tecnología.

En este capítulo aprenderá:

- Crear y gestionar contraseñas seguras.
- ¿Cómo proteger sus dispositivos personales?
- Manejo de la privacidad en las redes sociales.
- Leyes que protegen a los jóvenes en el entorno digital

CAPÍTULO 3:

PROTECCIÓN DE DISPOSITIVOS Y DATOS PERSONALES

Crear y gestionar contraseñas seguras

Enseñar a los estudiantes sobre contraseñas seguras es fundamental para su seguridad en línea. Algunos consejos que los docentes pueden brindar a los jóvenes son los siguientes:

1. Crear una contraseña larga, única y fácil de recordar. Debe ser fácil de recordar para ti, pero difícil de adivinar para otros.
2. Las contraseñas deben tener como mínimo ocho caracteres.
3. Deben incluir mayúsculas, minúsculas, números y símbolos especiales para aumentar la seguridad de la contraseña.
4. No utilizar nombres, fechas o datos fáciles de adivinar, lo ideal es usar algo único y sin relación con algo personal.
5. No repetir contraseñas en diferentes plataformas, si se le complica recordarlas, usar un administrador de contraseñas.
6. Una frase larga puede ser más fácil de recordar y suficientemente segura, especialmente si incluye varios tipos de caracteres.

CAPÍTULO 3: PROTECCIÓN DE DISPOSITIVOS Y DATOS PERSONALES

¿Cómo proteger sus dispositivos personales?

Enseñar a los estudiantes a proteger sus dispositivos personales es crucial para mantener su información segura. A continuación, algunas recomendaciones:

1. Asegurarse de que todos los dispositivos tengan un software antivirus confiable instalado y actualizado, esto ayuda a detectar y eliminar malware y otras amenazas en línea.
2. Realizar actualizaciones regulares del sistema operativo y de las aplicaciones, ya que esto trae mejoras de seguridad que protegen contra nuevas amenazas.
3. Una buena práctica es la ejecución de respaldos de la información, ya sea por medio de la nube o de discos duros externos.
4. Verificar las configuraciones de seguridad de cada dispositivo, las configuraciones predeterminadas pueden no ser las más seguras.
5. Habilitar la autenticación de dos factores en las cuentas, el primer factor es normalmente la contraseña, el segundo puede ser un código enviado a un dispositivo móvil o una aplicación de autenticación.

CAPÍTULO 3:
PROTECCIÓN DE DISPOSITIVOS Y DATOS PERSONALES

Manejo de la privacidad en las redes sociales

Los estudiantes deben comprender la relevancia de proteger su información personal en línea. Es crucial que no publiquen información sensible como direcciones, números de teléfono o datos familiares.

Aconsejar a los estudiantes que eviten conectarse a redes Wi-Fi públicas para realizar actividades sensibles, como iniciar sesión en redes sociales, ya que estas redes no siempre son seguras.

Es importante que los estudiantes aprendan a identificar contenido inapropiado o peligroso, y cómo evitar compartir información con desconocidos en línea.

Recomendar a los estudiantes en revisar y ajustar las configuraciones de privacidad en sus perfiles de redes sociales para controlar quién puede ver sus publicaciones y datos personales.

Leyes que protegen a los jóvenes en el entorno digital

LEY 9048 de delitos informáticos

La ley busca prevenir, sancionar y combatir delitos como el acceso no autorizado a sistemas informáticos, la usurpación de identidad, y la difusión de contenido perjudicial o ilegal.

Estos delitos tienen penas de prisión de uno a cuatro años, dependiendo de la gravedad del acto y el daño causado a la intimidad de otra persona.

Es esencial que los docentes conversen con los estudiantes sobre los riesgos del uso irresponsable de internet y cómo prevenir ser víctimas o perpetradores de delitos informáticos.

LEY 8968 de protección de la persona frente al tratamiento de sus datos personales

La ley garantiza el derecho de las personas a la privacidad y la autodeterminación informativa.

Existen sanciones para quienes utilicen o divulguen datos personales sin consentimiento, esto incluye multas que pueden llegar hasta los treinta salarios base.

El conocer esta ley permite a los estudiantes tomar decisiones informadas y ayudar a proteger su privacidad en el entorno digital.

CAPÍTULO 3: PROTECCIÓN DE DISPOSITIVOS Y DATOS PERSONALES

LEY 10238 de protección de la imagen, la voz y los datos personales de las personas menores de edad

La ley garantiza la protección de la integridad física y moral de los menores, prohibiendo la divulgación no autorizada de sus datos, imágenes o voz. Esto busca evitar la explotación y proteger su privacidad en medios digitales y tradicionales.

La divulgación de cualquier imagen, voz o dato personal de un menor requiere el consentimiento explícito de los padres o tutores.

LEY 8934 protección de la niñez y la adolescencia en internet

La ley busca proteger a la niñez y la adolescencia frente al contenido nocivo que puede encontrarse en Internet y otros medios electrónicos, que pueden afectar su desarrollo.

Se considera contenido nocivo aquel que pueda dañar la salud mental, física, moral o social de los menores, lo que incluye violencia, pornografía y otras temáticas inapropiadas.

La ley también promueve la educación sobre el uso seguro y responsable de Internet, buscando empoderar a los menores en su navegación en línea.

CAPÍTULO 4:

FOMENTANDO EL INTERÉS EN CARRERAS EN CIBERSEGURIDAD

La ciberseguridad abre las puertas a un futuro profesional interesante y lleno de oportunidades. Inspiren a sus estudiantes fomentando el interés en esta carrera donde sus habilidades puedan marcar la diferencia.

En este capítulo aprenderá:

- Papel que juegan los docentes en fomentar el interés por las carreras tecnológicas.

CAPÍTULO 4:

FOMENTANDO EL INTERÉS EN CARRERAS EN CIBERSEGURIDAD

El papel de los docentes en fomentar el interés por las carreras tecnológicas

Los docentes juegan un papel muy importante en despertar el interés de los estudiantes por el mundo de la tecnología, ya que las oportunidades futuras en este campo son numerosas, ya que las competencias digitales son cada vez más demandadas.

OPORTUNIDADES TECNOLÓGICAS EN COSTA RICA

Carreras como ingeniería en software, ciberseguridad, desarrollo web, e inteligencia artificial están en auge tanto a nivel nacional como global. En nuestro país, la expansión de zonas francas y la presencia de empresas tecnológicas internacionales han generado una alta demanda de profesionales capacitados en estas áreas.

ROL DE LOS ORIENTADORES Y DOCENTES EN EL INTERÉS VOCACIONAL DE CARRERAS TECNOLÓGICAS

Los docentes y el equipo de orientación son fundamentales en fomentar el interés vocacional de los estudiantes en carreras profesionales en ciberseguridad. Tienen como función los siguientes aspectos:

- Proporcionar orientación vocacional que destaque el potencial de carreras tecnológicas, su alto nivel de empleabilidad y la posibilidad de obtener becas o financiamiento para estudiar en estas áreas.
- Proporcionar a los estudiantes recursos educativos en ciberseguridad. Existen iniciativas nacionales e internacionales que proporcionan recursos gratuitos para que los jóvenes exploren y desarrollen habilidades en este campo.
- Invitar a profesionales o empresas del ámbito tecnológico a compartir sus experiencias, por medio de charlas o talleres, con el fin de motivar a los estudiantes a seguir en el camino de la ciberseguridad.
- La enseñanza en aspectos como alfabetización digital y el uso responsable de las plataformas digitales, ayuda a preparar a los estudiantes para las demandas del mundo laboral, aumentando el interés en carreras tecnológicas.

Con estas acciones, los docentes pueden desempeñar un papel crucial en la motivación de los estudiantes hacia las carreras en ciberseguridad, asegurando un futuro más seguro y preparado en el ámbito digital.

Referencias

- Checkpoint, (2024). Tipos de amenazas de ciberseguridad. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security
- GOB, (2024). Guía de ciberseguirdad. https://www.gob.mx/cms/uploads/attachment/file/896412/Gu_a_de_Ciberseguridad_en_apoyo_a_la_educaci_n.pdf
- HealthyChildren.org, (2022). "Sexteo": cómo hablar con sus hijos del riego de enviar mensajes con contenido sexual. https://www.healthychildren.org/Spanish/family-life/Media/Paginas/the-new-problem-of-sexting.aspx
- https://latam.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online
- INCIBE, (2024). Ciberseguridad para familias. https://www.incibe.es/menores/familias/ciberseguridad
- INCIBE, (2024). Configura correctamente tu dispositivo y asegura tu información. https://www.incibe.es/ciudadania/tags/configuraci%C3%B3n%20segura
- INCIBE, (2024). Grooming. https://www.incibe.es/menores/tematicas/grooming
- INCIBE, (2024). Las redes sociales como herramienta para ciberdelincuentes. https://www.incibe.es/ed2026/talento-hacker/blog/las-redes-sociales-como-herramienta-para-ciberdelincuentes
- INCIBE, (2024). Privacidad. https://www.incibe.es/menores/tematicas/privacidad
- INCIBE, (2024). Sexting. https://www.incibe.es/menores/tematicas/sexting
- Kaspersky, (2024). Cómo identificar noticias falsas. https://latam.kaspersky.com/resource-center/preemptive-safety/how-to-identify-fake-news
- Kaspersky, (2024). Las 15 mejores reglas de seguridad y qué no hacer en línea.
- Ley 10238. Ley de protección de la imagen, la voz y los datos personales de las personas menores de edad. Asamblea Legislativa de Costa Rica (2022). http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=97506&nValor3=131719&strTipM=TC
- Ley 7739. Código de la Niñez y la Adolescencia, Asamblea Legislativa de Costa Rica (1998). http://www.pgrweb.go.cr/scij/busqueda/normativa/normas/nr m_texto_completo.aspx?param2=1&nValor1=1&nValor2=43077&lResultado=4&strSelect=sel
- Ley 8934. Ley de Protección de la Niñez y la Adolescencia frente al contenido nocivo de Internet y otros medios electrónicos. Asamblea Legislativa de Costa Rica (2011). http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=71024&nValor3=0

Referencias

- Ley 8968. Ley de Protección de la persona frente al tratamiento de sus datos personales. Asamblea Legislativa de Costa Rica (2011). http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC
- Meta, (2024). Qué hacer cuando tu hijo(a) adolescente sufre de acoso online. https://familycenter.meta.com/latam/education/resources/how-can-parents-prevent-cyberbullying/
- Microsoft, (2024). ¿Qué es la ciberseguridad?. ¿https://www.microsoft.com/es-es/security/business/security-101/what-is-cybersecurity
- Microsoft, (2024). ¿Qué es la protección con contraseña?. https://www.microsoft.com/es-cl/security/business/security-101/what-is-password-protection
- NACIONAL CIBERSECURITY ALLIANCE (2022), Hablar con niños y adolescentes sobre seguridad y privacidad. https://staysafeonline.org/es/online-safety-privacy-basics/talking-to-kids-teens/
- NACIONAL CIBERSECURITY ALLIANCE (2024), Mes de la concientización sobre la ciberseguridad. https://www.cisa.gov/sites/default/files/2024-10/Cybersecurity-Awareness-Month-2024-Toolkit-Guide_ES.pdf
- NACIONAL CIBERSECURITY ALLIANCE, (2022). Control Parental. https://staysafeonline.org/es/online-safety-privacy-basics/parental-controls/
- NACIONAL CIBERSECURITY ALLIANCE, (2022). Formando ciudadanos digitales. https://staysafeonline.org/es/online-safety-privacy-basics/raising-digital-citizens/
- NACIONAL CIBERSECURITY ALLIANCE, (2022). Padres y educadores: Qué hacer con el ciberacoso. https://staysafeonline.org/es/online-safety-privacy-basics/cyberbullying-parents/
- TSE, (2021). Como ejercer una ciudadanía digital responsable. https%3A%2F%2Fwww.tse.go.cr%2Fpdf%2Fpublicaciones%2FC%25C3%25B3mo-ejercer-una-ciudadan%25C3%25ADa-digital-responsable.pdf
- UNICEF, (2022). Ciberacoso: qué es y cómo detenerlo. https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo#:~:text=Si%20te%20preocupa%20tu%20seguridad,de%20cuidadores%20capacitados%20y%20experimentados.
- UNICEF, (2022). Las 12 habilidades transferibles del Marco Conceptual y Programático. https%3A%2F%2Fwww.unicef.org%2Flac%2Fmedia%2F30756%2Ffile%2FLas%252012%2520habilidades%2520transferibles.pdf

GUÍA DE CIBERSEGURIDAD

Para Docentes Y Personal Administrativo

Autor: Luis Andrés Montero Madriz.

2024

APÉNDICE H. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL LICEO DE PAVAS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LICEO DE PAVAS

2024

Contenido

Objetivo 3
Alcance 3
Responsables 3
Introducción 3
Lineamientos 4
Lineamiento para la gestión y control de accesos físicos 5
Lineamiento de protección de información sensible 5
Lineamiento para la gestión de redes seguras 6
Lineamiento para el mantenimiento de los equipos y antivirus 7
Lineamiento para la gestión de contraseñas seguras 8
Lineamiento para el uso de controles de filtrado web 8
Lineamiento de respaldo de datos 9
Lineamiento para la gestión de terceros 10
Lineamiento para la gestión de las redes sociales 10
Revisión y aprobación de la política 12
Referencias 13

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LICEO DE PAVAS

Objetivo

Establecer lineamientos relacionados con la seguridad de la información, con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información y recursos tecnológicos del Liceo de Pavas.

Alcance

La política y sus lineamientos aplica para docentes, personal administrativo, terceros, y visitantes que tengan accesos a los activos de información y recursos tecnológicos del Liceo de Pavas.

Responsables

La directora de la institución es la responsable de aprobar y supervisar la implementación de la política, con el fin de asegurar de que se cumplan los lineamientos de seguridad dentro del liceo. Los docentes del departamento de informática son los encargados de gestionar la política, monitoreando su cumplimiento y tomando medidas preventivas o correctivas en caso de incidentes. Adicionalmente los docentes en general y el personal administrativo son los responsables de seguir los lineamientos establecidos en la política, con el fin de proteger los recursos educativos y los activos de información.

Introducción

Por medio de esta Política de Seguridad de la Información se buscan establecer lineamientos claros sobre la gestión de los activos de información y recursos tecnológicos del Liceo de Pavas. Además, se definen las responsabilidades de los diferentes actores para mantener la seguridad y minimizar los riesgos potenciales.

En este sentido, es una guía esencial para fomentar una cultura de seguridad dentro de la institución educativa, promoviendo buenas prácticas y asegurando que todos los miembros de la entidad trabajen con un enfoque alineado para proteger la información.

Para el desarrollo de esta se tomó como referencia la norma ISO/IEC 27002:2022, la cual proporciona un conjunto de mejores prácticas y controles en temas de seguridad de la información y ciberseguridad, adaptando los controles y recomendaciones, según la necesidad del centro educativo.

Adicionalmente, se usó como referencia la Política en Tecnologías de la Información (2020), del Ministerio de Educación Pública, la cual busca garantizar la protección, la confidencialidad, la integridad y la disponibilidad de la información.

Los lineamientos que se definieron para ejecutar las acciones correspondientes para salvaguardar los activos de información y recursos tecnológicos del Liceo de Pavas son los siguientes:

- Lineamiento para la gestión y control de accesos físicos.
- Lineamiento de protección de información sensible.
- Lineamiento para la gestión de redes seguras.
- Lineamiento para la gestión de los equipos y antivirus.
- Lineamiento para la gestión de contraseñas seguras.
- Lineamiento para el uso de controles de filtrado web.
- Lineamiento de respaldo de datos.
- Lineamiento de gestión de terceros.
- Lineamiento para la gestión de las redes sociales.

Lineamientos

A continuación, se establecen los siguientes lineamientos de seguridad de la información, con el fin de proteger la información sensible frente a accesos no autorizados, modificaciones indebidas o destrucción accidental, además minimizar las vulnerabilidades informáticas y establecer responsables, esto deberá ser cumplido por los docentes, personal administrativo, terceros, visitantes y terceros.

Lineamiento para la gestión y control de accesos físicos

El lineamiento para la gestión y control de accesos físicos busca establecer procedimientos que regulen el acceso a la institución educativa. Con el fin de proteger los activos de información, y garantizar que solo el personal autorizado pueda ingresar a las instalaciones, con el objetivo de minimizar amenazas a la seguridad de la información y los recursos educativos.

Los procedimientos que se deben seguir son los siguientes:

a) Utilizar procedimientos de control de acceso físico, en el cual registren la identidad de las personas que ingresan y su horario, asegurando que solo el personal autorizado tenga acceso a áreas críticas como laboratorios de cómputo y oficinas administrativas.
b) Instalar sistemas de cerraduras electrónicas y cámaras de vigilancia en puntos estratégicos para supervisar las entradas y salidas, garantizando que solo personas autorizadas puedan entrar a las instalaciones del colegio.
c) Limitar el acceso a la institución, asegurando que solo exista acceso por medio de los portones de la entrada principal, así como establecer protocolos para el acceso de visitantes, garantizando su registro y supervisión en todo momento.
d) Realizar auditorías periódicas del sistema de control de acceso para verificar su correcto funcionamiento y detectar posibles vulnerabilidades.

Lineamiento de protección de información sensible

El lineamiento para la protección de información sensible procura establecer normas para la recolección, almacenamiento y manejo adecuado de los datos personales de los estudiantes y sus familias, así como de los docentes y administrativos. Con el fin de garantizar la seguridad y confidencialidad de la información. Con el fin de garantizar la seguridad y confidencialidad de la información.

Los procedimientos que se deben seguir son los siguientes:

a) Identificar los tipos de información sensible que se manejan, como expedientes académicos, datos de salud y situación familiar.

b) Implementar un sistema de gestión de información en el centro educativo que permita digitalizar y almacenar los datos de manera segura.
c) Incorporar soluciones de cifrado de datos para proteger la información.
d) El personal docente y administrativo no puede remitir información sensible de los estudiantes por medios no autorizados.
e) Capacitar al personal docente y administrativo acerca del uso de la información sensible y la importancia de la digitalización.
f) Establecer políticas de auditoría continua para asegurar que los protocolos de seguridad se estén cumpliendo.

Lineamiento para la gestión de redes seguras

El lineamiento para la gestión de redes seguras tiene como objetivo garantizar que las redes informáticas de la institución educativa funcionen de manera confiable y segura. Se busca prevenir el acceso no autorizado, proteger los recursos tecnológicos y la información sensible, además de asegurar la disponibilidad de la red para los usuarios autorizados.

Los procedimientos que se deben seguir son los siguientes:

a) Implementar controles de acceso a la red, permitiendo que solo usuarios autorizados y dispositivos seguros ingresen.
b) Segmentar las redes según corresponda, una para estudiantes, otra para docentes y personal administrativo y una de visitantes, para mejorar la seguridad y acceso no autorizado.
c) Implementar mecanismos de autenticación de dos factores (2FA), aumentando la seguridad en cuanto al acceso de la red, con el fin de verificar la identidad de los usuarios, mejorando así la protección contra accesos no autorizados.
d) Implementar herramientas de monitoreo para detectar y responder rápidamente a posibles amenazas o vulnerabilidad de seguridad.

Lineamiento para el mantenimiento de los equipos y antivirus

El lineamiento para el mantenimiento de los equipos y antivirus tiene la finalidad de garantizar que todos los equipos informáticos funcionen de manera óptima. Ejecutando mecanismos para el mantenimiento preventivo del hardware y el software, con el fin de evitar fallas en los equipos, y protegerlos contra amenazas o riesgos cibernéticas.

Los procedimientos que se deben seguir son los siguientes:

a) Configurar las computadoras de manera que realicen actualizaciones automáticas del sistema operativo. Esto asegura que las correcciones de seguridad y mejoras que se realicen en el sistema operativo, se apliquen cuanto antes.
b) Priorizar la instalación de parches de seguridad y correcciones de bugs, ya que los ciberdelincuentes suelen aprovechar vulnerabilidades no corregidas.
c) Establecer un calendario mensual o trimestral para revisar y aplicar actualizaciones críticas en el software. Actuar de manera preventiva ayuda en el aseguramiento y funcionamiento de los equipos.
d) Antes de cada actualización, realizar respaldos completos del sistema para evitar pérdida de datos en caso de fallos inesperados.
e) Revisar la compatibilidad de hardware antes de aplicar actualizaciones de software. Los equipos obsoletos o descontinuados pueden tener problemas al ejecutar las actualizaciones de versiones del sistema operativo.
f) Instalar un software antivirus confiable en todas las computadoras. Asegurarse de que el antivirus sea compatible con el sistema operativo y que ofrezca protección en tiempo real para prevenir ataques de malware y virus.
g) Configurar el antivirus para que se actualice automáticamente, asegurando que siempre esté al actualizado con las últimas definiciones de virus y amenazas.
h) Programar escaneos completos del sistema de forma semanal o mensual en todas las computadoras. Además, se recomienda realizar escaneos adicionales después de descargar archivos de fuentes externas.

i) No permitir que los usuarios desactiven el antivirus, excepto en casos que de deba hacer de forma definitiva.

Lineamiento para la gestión de contraseñas seguras

El lineamiento para la gestión de contraseñas seguras pretende establecer reglas y recomendaciones que ayudan a fortalecer la seguridad de las contraseñas; además, busca garantizar la actualización periódica y el almacenamiento seguro de contraseñas.

Los procedimientos que se deben seguir son los siguientes:

a) Las contraseñas de los equipos del centro educativo deben tener un mínimo de 8 caracteres, incluir letras mayúsculas, minúsculas, números y caracteres especiales, para garantizar su robustez.
b) Establecer controles que garanticen una periodicidad de cambio en las contraseñas que oscile entre 60 y 90 días, según lo amerite.
c) Limitar el uso y configuración de contraseñas débiles como "1234", "admin" o similares.
d) Utilizar sistemas de gestores de contraseñas con el fin de almacenar y generar contraseñas complejas. Evitando guardar las contraseñas en lugares inseguros o de fácil acceso.
e) Realizar talleres para capacitar a los docentes y personal administrativo sobre la importancia de crear y gestionar contraseñas fuertes.

Lineamiento para el uso de controles de filtrado web

El lineamiento para el uso de controles de filtrado web busca establecer normas que permitan a los educadores supervisar y orientar el uso de los recursos tecnológicos del centro educativo por parte de los estudiantes, con el fin de restringir el acceso a material inapropiado.

Los procedimientos que se deben seguir son los siguientes:

a) Instalar software especializado para filtrar contenido web en los laboratorios de cómputo a los cuales tienen acceso los estudiantes, para bloquear sitios inapropiados, como los que contienen violencia, contenido sexual o actividades ilegales.
b) Habilitar los controles parentales en las computadoras, permitiendo supervisar y restringir el acceso de los estudiantes a aplicaciones y sitios web no educativos.
c) Capacitar al personal docente y administrativo, acerca del uso y configuración de estos controles en los equipos de cómputo de la institución.
d) Asignar encargados que revisen de manera regular los registros de acceso a internet y de ser necesario realicen ajustes a las configuraciones de los controles parentales.

Lineamiento de respaldo de datos

El lineamiento para la protección de información sensible tiene como objetivo establecer mecanismos para proteger la información y garantizar su disponibilidad en caso de pérdida, daño o corrupción.

Los procedimientos que se deben seguir son los siguientes:

a) Identificar los tipos de datos sensibles y críticos que necesitan respaldo, como registros académicos y administrativos.
b) Implementar un sistema de respaldo de datos automático para todas las computadoras del colegio, con copias de seguridad periódicas en la nube.
c) Establecer políticas claras sobre la frecuencia de los respaldos (diarios, semanales) y los tipos de datos que se respaldarán.
d) Realizar capacitaciones para el personal administrativo y docente sobre el uso del sistema de respaldo, asegurando que todos entiendan cómo y por qué se realiza.
e) Establecer un calendario de revisión del sistema de respaldo y actualizar las herramientas utilizadas según sea necesario, asegurando su relevancia y eficacia.

Lineamiento para la gestión de terceros

El lineamiento para la gestión de terceros procura establecer normas que regulen las relaciones con terceros o proveedores, implementando mecanismos para identificar, evaluar y mitigar los riesgos y amenazas en los recursos educativos y tecnológicos del liceo, realizando acuerdos de confidencialidad con los proveedores que tengan accesos a los activos del centro educativo.

Los procedimientos que se deben seguir son los siguientes:

a) Realizar evaluaciones de seguridad y riesgo antes de contratar servicios de terceros, especialmente si tendrán acceso a información sensible de los alumnos.
b) Limitar y controlar el acceso de terceros a la información del colegio mediante autorizaciones específicas y monitorización continua del acceso.
c) Monitorear y revisar regularmente los servicios prestados por terceros para asegurar el cumplimiento de los acuerdos de seguridad y tomar medidas correctivas cuando sea necesario.

Lineamiento para la gestión de las redes sociales

El lineamiento para la gestión de las redes sociales, tiene como objetivo establecer normas que regulen el uso de las plataformas digitales, con el fin garantizar el uso responsable del contenido que publican en las redes sociales. Además, se pretende resguardar la reputación del centro educativo y controlar la información personal de estudiantes y docentes que se publique.

Los procedimientos que se deben seguir son los siguientes:

a) Crear un equipo o designar a una persona responsable de la gestión de todas las cuentas de redes sociales del colegio.
b) Desarrollar lineamientos de uso y manejo de la información en redes sociales, estableciendo procedimientos de publicación, normas de interacción con seguidores y divulgación de información sensible.

c) Implementar controles de acceso para asegurar que solo el equipo designado tenga acceso a las cuentas de redes sociales.

d) Establecer controles con el fin de evaluar el cumplimiento de las normas de publicaciones y las interacciones con la audiencia.

Revisión y aprobación de la política

La revisión y aprobación de la Política de Seguridad de la Información para el Liceo de Pavas está a cargo de la dirección y el equipo técnico asignado para garantizar el cumplimiento de la misma. Además, debe ser revisada y aprobada anualmente, con el fin de evaluar si requiere cambios, en caso de que se detecten vulnerabilidades en los lineamientos establecidos o nuevas amenazas en materia de protección de datos y ciberseguridad, con el objetivo de resguardar los recursos educativos y tecnológicos de la institución.

Referencias

ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection - Information security controls. https://www.iso.org/es/contents/data/standard/07/56/75652.html

Ministerio de Educación Pública, (2020). Política en tecnologías de la información. https://juegosdeportivosestudiantiles.mep.go.cr/wp-content/uploads/2023/09/Politica-en-Tecnologias-de-la-Informacion-MEP.pdf