LICENCIATURA EN EDUCACIÓN

TRABAJO FINAL DE GRADO

PLAN DE INTERVENCIÓN

Unidad Educativa Maryland

Modelos de Aprendizajes Innovadores

“La ciberseguridad en el ámbito educativo para la Unidad Educativa Maryland de Villa Allende, Córdoba”

Autora: Romero, Cinthya Ayelén

D.N.I.: 36480343

Legajo: VEDU01625

Tutora: Teresita Jalin

Río Tercero, Córdoba, junio de 2023

Agradecimientos

A mi familia, por ser mi sostén, en especial a mi abuelo José y a mi tío Jorge: desde donde estés, esto es por y para vos. Te llevo siempre conmigo.

A mis amigos, mi familia por elección, que supieron entender mis tiempos y mis ausencias.

A mis compañeras de trabajo, que me acompañaron y siguieron paso a paso cada examen y entrega.

A Susi y Caro, por su apoyo incondicional y no soltarme la mano.

A Almendrita, mi compañera incondicional en los días y noches de estudio, siempre pegada a mi.

A mi, por encarar este desafío y llevarlo adelante con esfuerzo y dedicación, incluso cuando sentía que no podía lograrlo.

A Dios, por guiar mis pasos y cuidarme siempre.

Índice

Resumen

El presente plan de intervención se llevará a cabo en la Unidad Educativa Maryland, una institución privada y laica de la localidad de Villa Allende provincia de Córdoba que apuesta a las TIC en todos sus niveles educativos, sin embargo, se detecta en la misma, el problema que da origen a nuestro plan: no existe en la escuela un ambiente ciber seguro, por lo que esta intervención se llevará a cabo con una capacitación docente en ciberseguridad donde los profesores de nivel secundario y el departamento de informática identifiquen los riesgos a los que están expuestos, conozcan los contenidos básicos de la sguridad digital y se promueva un uso responsable de las TIC en la institución. Se realizarán 6 encuentros presenciales donde se propiciará el aprendizaje colaborativo, la resolución8 de casos donde los docentes apliquen estos conocimientos obtenidos, creen acciones de prevención a las amenazas digitales y se elabore conjuntamente un plan de acción que favorezca la ciberseguridad.

Palabras claves: ciberseguridad, uso responsable, tic, plan de acción

Introducción

En el año 2017, el Ministerio de Educación de la Nación lanza el programa “Aprender Conectados” (Resolución Ministerial N.º 1410/2018) que promueve una política integral de innovación educativa cuya misión principal es integrar la comunidad educativa en la cultura digital que impulsa la alfabetización digital centrada en el aprendizaje de competencias y saberes necesarios para una inserción plena en la cultura contemporánea y en la sociedad del futuro.

En educación podemos utilizar las TIC en infinidad de situaciones que fomenten y potencien la cultura digital. Hoy, nos es factible digitalizar materiales educativos, crear aulas virtuales, agilizar y expandir las posibilidades de comunicación entre docentes y estudiantes, introducir aplicaciones que enriquezcan el proceso de enseñanza – aprendizaje, entre otros.

La transformación digital en el ámbito educativo no solo ofrece escenarios positivos, introducirnos en el mundo digital nos expone a una infinidad de riesgos como violación de la privacidad, sobre exposición, hackeos y un sinfín de ciber delitos. Esto, en una institución educativa donde además, quienes manipulan las TIC son menores de edad, aumenta los peligros considerablemente.

Esta propuesta fue enmarcada en la línea temática *Modelos de aprendizajes innovadores*, considerando que las nuevas propuestas digitales necesitan respaldarse en un ambiente seguro para nuestra inmersión en el mundo digital.

Pérez, directora de la Revista Bienestar Digital comentó que:

> Es imprescindible capacitar a la ciudadanía con competencias digitales que les permita usar de forma saludable la tecnología y garantizar su propia seguridad en el entorno digital. Conocer la red y la tecnología es la mejor arma para frenar las manipulaciones de pensamiento y abusos cada vez más habituales en este nuevo ámbito. Es una batalla colectiva en defensa de la libertad individual y contra la manipulación de pensamiento, que finalizará cuando consigamos que impere la cultura de ciberseguridad, con un pensamiento crítico y donde las personas tengamos un papel activo sobre la información que consumimos. (Pérez, R 2021 p. 13)

A partir de un minucioso análisis de la Unidad Educativa Maryland se plantea el problema de la ausencia de ciberseguridad en el establecimiento y, en consecuencia, la necesidad de intervención donde se propone la capacitación docente al respecto.

Se pretende con esta intervención capacitar a los docentes de nivel secundario y a la coordinadora del departamento de informática de la Unidad Educativa Maryland en el primer semestre del ciclo lectivo 2023, en el uso responsable de las TIC y la ciberseguridad en instituciones educativas, favoreciendo el desarrollo de habilidades informáticas de manera segura.

En el primer momento se da a conocer al equipo directivo de la Unidad Educativa Maryland la necesidad de intervención y la propuesta de la Lic. Romero para lograrlo, se organiza el espacio y los recursos necesarios para el proceso de capacitación y se realiza el primer encuentro con los docentes, donde se diagnostica el conocimiento previo sobre ciberseguridad y sus intenciones respecto a los encuentros siguientes.

En el segundo momento se realizan cinco encuentros presenciales con el cuerpo docente, donde se los capacita en conocimientos básicos sobre la ciberseguridad y se promueve a través de diversas propuestas el uso responsable de las TIC.

Finalmente, en el tercer momento de la capacitación, se realiza una retroalimentación de lo trabajado en el último encuentro presencial, se certifica la participación de los integrantes y se realiza también una devolución de resultados de la evaluación procesual con todos los instrumentos evaluativos utilizados en el desarrollo de la capacitación al equipo directivo de la institución.

Presentación de la línea temática escogida

Las escuelas no pueden ser ajenas al proceso revolucionario digital que atravesamos, más bien, somos los educadores quienes debemos formarnos y transformar nuestras prácticas en pos de una educación del siglo XXI.

> Para las escuelas y los sistemas educativos en particular, las nuevas tecnologías ofrecen amplias oportunidades de reorganización, tanto de sus funciones de transmisión de conocimiento como de sus procesos de gestión interna. Más aún, algunos piensan que no podrán dejar de aprovecharlas. (Brunner 2000 p. 15).

Las nuevas necesidades de la sociedad demandan a las instituciones educativas, una formación integral, donde los estudiantes sean capaces no solo de buscar información, sino de procesarla, analizarla críticamente y elaborar sus propias conclusiones. Esto supone además un alto riesgo de exposición de todos los actores inmersos en la cultura digital, un espacio de ciberseguridad en los establecimientos educativos resulta de primera necesidad frente a este riesgo.

El cambio educativo es inminente, como también lo es ajustar las medidas de seguridad para afrontar el cambio con responsabilidad y desde una oportunidad de mejora y no como una transformación radical.

> La presencia de las nuevas tecnologías en las aulas ya no tiene vuelta atrás. Si hasta hace unos años las autoridades y los docentes podían pensar que los medios digitales debían restringirse a algunas horas por semana o a algunos campos de conocimiento, hoy es difícil, no imposible, ponerle límites a su participación en los procesos de enseñanza y aprendizaje. Experiencias como

> los modelos 1 a 1 (una computadora por alumno), las pizarras electrónicas, los laboratorios de informática móviles, o incluso la convivencia cotidiana con celulares y otros artefactos digitales, muestran que las nuevas tecnologías llegaron para quedarse (Dussel, 2011 p. 9).

Una innovación educativa implica entonces, un cambio significativo en el proceso de enseñanza-aprendizaje, tanto en los materiales y métodos, como en los contenidos implicados en la enseñanza. La diferencia percibida debe estar relacionada con la calidad de novedad del elemento mejorado y la importancia que la innovación propuesta aportará una mejora considerable a la institución educativa y a los grupos de interés externos.

La innovación educativa es fundamental para que el aprendizaje se adapte a las necesidades de los alumnos en cada momento y evolucione. Es por ello, que este plan de intervención busca a partir de las condiciones edilicias, recursos y posibilidades de la Unidad Educativa Maryland, promover el uso responsable y cuidado de las TIC en las aulas con un aprendizaje de calidad que esté a la altura de las demandas actuales.

Los docentes deben ser capacitados para aportar a su práctica un enfoque tecnológico. Tal como exponen Koehler y Mishra, (2009); “La escuela debe constituir un entorno enriquecido de aprendizaje donde los docentes puedan entramar y resignificar el conocimiento pedagógico que ya poseen, con nuevo conocimiento tecnológico” (p.2). Es por ello, que la formación del equipo docente en la Unidad Educativa Maryland será nuestro puntapié inicial para lograr un desempeño acorde a nuestros objetivos.

Síntesis de la organización

La institución escogida es La Unidad Educativa Maryland. La información recabada corresponde a datos extraídos de la Universidad Siglo 21 y la página web de la institución.

La Unidad Educativa Maryland es una institución privada y laica ubicada en la calle Güemes al 702 en la localidad de Villa Allende, departamento de Colón, provincia de Córdoba, Argentina. El terreno donde se encuentra, consta de 8170 metros cuadrados de superficie de los cuales 1278 metros cuadrados son de superficie cubierta, el mismo pertenecía a la Municipalidad de Villa Allende y fue cedido a través de un contrato de comodato.

Sus instalaciones se pueden apreciar en un recorrido virtual a través de Round Me (https://roundme.com/tour/344685/view/1156074/) como así también, visitando su página web (www.maryland.edu.ar). Sus vías de contacto son por mail a administración@maryland.edu.ar o a sus teléfonos (03543) 432239/433629/4335656.

La Unidad Educativa Maryland debe su nombre a las expectativas de su fundadora quien tenía la formación en lengua inglesa, debido a su fuerte vínculo con el estado de Maryland, Estados Unidos.

Sus inicios se remontan al año 1994 cuando Marga de Maurel, Nancy Goico y Marta Carry comenzaron con las gestiones pertinentes para fundar una escuela, redactando el documento correspondiente. El mismo fue presentado por primera vez en la Dirección General de Enseñanza Privada (DIPE) en 1992. Allí comenzaron las gestiones y requerimientos solicitados por DIPE y el Ministerio de Educación de Córdoba. Lograron abrir sus puertas en 1994 (Universidad Siglo 21, 2019a).

En septiembre de ese mismo año, el grupo societario, que ahora contaba con Dolly Arias; organizó las primeras reuniones destinadas a presentar el proyecto a la sociedad de Villa Allende y a convocar a las personas que luego se harían cargo de la puesta en marcha de ese proyecto, que finalmente comienza a funcionar en marzo de 1995 con una matrícula de 50 alumnos. A medida que los estudiantes iban egresando se iban abriendo nuevas divisiones y así en 1998 funcionaba el nivel inicial y el nivel primario completos, con dos secciones por cada división y una matrícula de 245 alumnos. En 1999 comenzó el nivel medio, solo con ciclo básico que, por razones económicas, edilicias y de baja matrícula, cerró sus puertas al año siguiente hasta 2008, donde la institución vuelve a ofrecer el ciclo básico en su propio edificio. En este nuevo intento, el nivel fue creciendo hasta completar los seis años. (Universidad Siglo XXI, 2021b)

El nivel inicial cuenta con sala de 4 y 5 años, el nivel primario es de primero a sexto grado con dos secciones cada uno y el nivel secundario de primero a sexto año con una orientación en ciencias sociales y humanidades.

Además, la escuela cuenta con una formación opcional en lengua inglesa (F.O.L.I) que se dicta de manera opcional en contra turno desde el nivel inicial al nivel secundario. El programa F.O.L.I cuenta con 3 trayectos, el primero abarca desde la sala de 4 años a 2º grado, el segundo de 3º grado a 6º grado y el tercer trayecto por último abarca los años correspondientes al nivel medio.

La institución, además, promueve los exámenes internacionales respaldados por la Universidad de Cambridge como lo son el Young learners, KET, PET, First y CAE (Unidad Ed. Maryland s.f.d https://maryland.edu.ar/foli/).

La unidad educativa Maryland cuenta también con un departamento de informática donde tienen por objetivo que, a través de la utilización de la computadora como una herramienta, se formen personas que tengan la capacidad de buscar información, seleccionarla, analizarla y evaluarla con juicio crítico de manera que la misma les permita tomar decisiones trascendentes. (Universidad Siglo 21, 2019c). Para ello cuentan con una sala de computación de 20 computadoras conectadas en red, internet con banda ancha y un cañón para el Nivel Inicial y el Nivel Primario. Al finalizar este tramo, los estudiantes acceden a un exámen y con él a un certificado aprobado por el Consejo de Ciencias Informáticas de la provincia de Córdoba como "Operador de PC" (Universidad Siglo 21, 2019d). En el Nivel Medio cada aula posee una pantalla táctil y hay en la institución 35 notebooks conectadas a la red de internet para trabajar en las aulas, donde lo hacen aplicando la tecnología y los conocimientos aprendidos en proyectos interdisciplinarios con otros espacios. (Universidad Siglo 21, 2021e)

La población que asiste a la escuela está conformada por estudiantes de clase media – alta, 80% oriundos de la localidad y el 20% restante pertenecen a localidades vecinas tales como Unquillo, Mendiolaza y La Calera. En la actualidad tiene una matrícula de 620 estudiantes entre los tres niveles educativos que la completan.

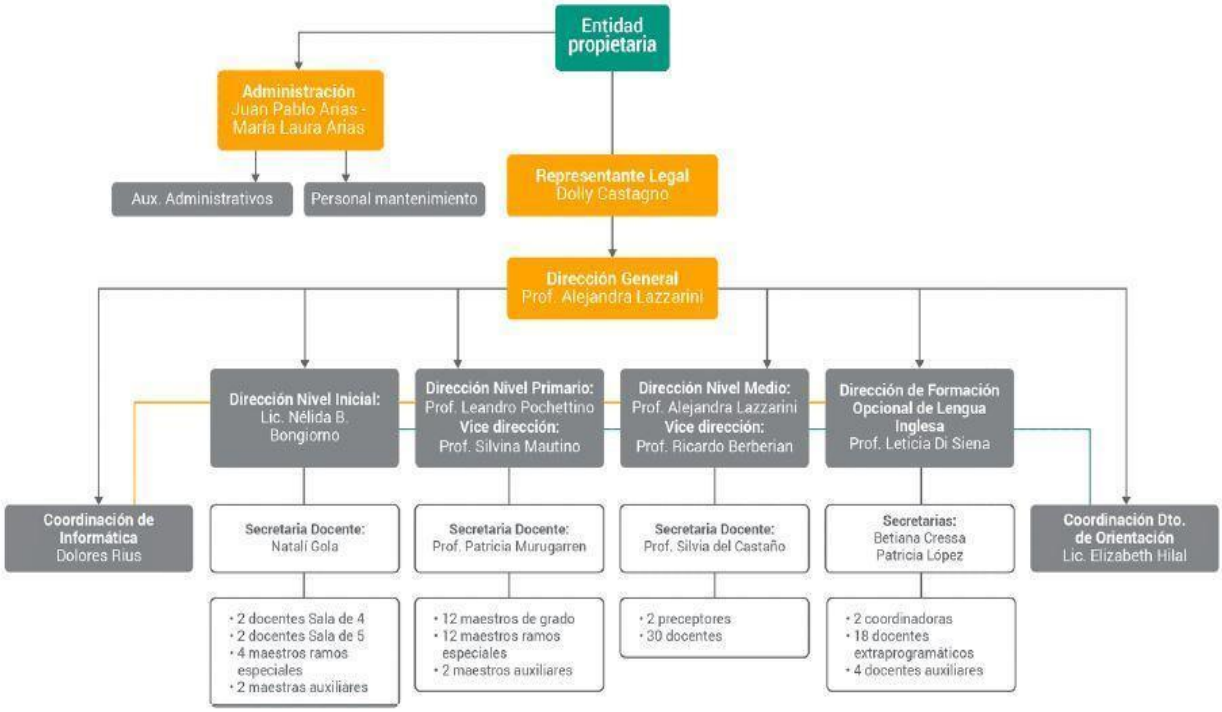
La *misión* de la Unidad Educativa Maryland es centrarse en una formación integral de sus estudiantes, a partir de prácticas coherentes y construidas en torno al trabajo colaborativo, con una fuerte apuesta a la Orientación en Comunicación y en la Lengua Inglesa, en la zona de Villa Allende, Córdoba. (Universidad Siglo 21, 2021f).

Tiene como *visión* una formación humanista que reconoce en el centro de la dimensión vital del hombre su libertad y el sentido social de esa construcción, aspirando

a un desarrollo integral del alumno/a. (Unidad Educativa Maryland s.f.d. https://maryland.edu.ar/institucional/)

La opción por una educación en valores y el reconocimiento de la escuela como una institución social, configurada históricamente y con una clara función formativa-pedagógica a la que le asiste un alto contenido ético, un compromiso ligado a la dignidad de las personas y la construcción de una sociedad cada vez más justa y democrática. (Unidad Educativa Maryland s.f.d https://maryland.edu.ar/institucional/)

La estructura de la escuela está representada en el siguiente organigrama:



Fuente: Universidad S. XXI

Delimitación de la necesidad de intervención

La Unidad Educativa Maryland cuenta con un departamento de informática que abarca los tres niveles educativos: nivel inicial, nivel primario y nivel medio.

Como recurso edilicio posee una sala de informática integrada por 20 computadoras conectadas en red, internet banda ancha en todas las pc, un cañón y aire acondicionado. Dicha sala, es utilizada por el nivel inicial y el nivel primario mientras que, para el nivel medio, la escuela cuenta con 35 notebooks conectadas en la red de la escuela e Internet para trabajar en las aulas. (Universidad Siglo 21, 2019g).

La institución utiliza las TIC como una herramienta de búsqueda de información y de apoyo al aprendizaje en el nivel primario, otorgando al finalizar sexto grado un diploma de "Operador de Pc" avalado por el Consejo de Ciencias de Informáticas de la provincia de Córdoba. (Unidad Educativa Maryland, s. f. e. https://bit.ly/2GmAZMZ). En el nivel secundario mientras tanto, las TIC son utilizadas de manera transversal en los distintos espacios curriculares, articulando la actividad con el departamento de informática.

En la Unidad Educativa Maryland el proceso innovador de las TIC se utiliza como instrumento de mejora en la situación de enseñanza – aprendizaje, donde los estudiantes se encuentran desde el nivel inicial al nivel medio atravesados por el mundo digital.

Las TIC forman parte de la cultura tecnológica donde estamos inmersos, pero, además, la ciberseguridad se muestra como un elemento de especial importancia para todos los usuarios, principalmente en la escuela donde quienes manipulan las TIC son menores de edad.

La seguridad, confidencialidad, integridad, disponibilidad de información y la protección de los usuarios son aspectos que no podemos pasar por alto.

Los estudiantes de la Unidad Educativa Maryland en su perfil, se espera que puedan procesar información, explorar, e investigar en el ámbito social y natural, enfrentándose al conocimiento con una actitud creativa y crítica. (Unidad Educativa Maryland, s. f. h, https://goo.gl/jZh5eq), parece pertinente sumar a esta actitud crítica de los estudiantes, una conciencia sobre el uso responsable de la tecnología, siendo ellos nativos digitales, es nuestra responsabilidad como formadores ofrecerles herramientas para desenvolverse en el mundo digital con seguridad y compromiso.

La institución cuenta con un programa de capacitación docente; “La propuesta gira en torno a revisar el sentido del oficio de maestro lo que requiere de un trabajo exploratorio, no mecánico, un verdadero trabajo artesanal, personal y reflexivo capaz de colocar en el lugar de “aprendices” a los maestros.” (Universidad Siglo XXI, 2021h).

El programa de capacitación docente en cuestión consta de 8 encuentros de 2 horas de duración cada uno de agosto a noviembre, sin embargo, no se realiza en el mismo ninguna propuesta relacionada a la seguridad digital.

La necesidad surge, entonces, al ver que la institución, en sus tres niveles educativos, inicial, primario y medio, utiliza las TIC e incluso posee un departamento de informática coordinado por la Sra. Dolores Ruis y así mismo, no evidencian ninguna capacitación al personal respecto a la ciberseguridad escolar ni tampoco presenta la institución un plan de contingencia en caso de un ciber riesgo, algo de suma necesidad teniendo en cuenta que la escuela tiene una base de datos con información personal y detallada de sus estudiantes, todos ellos menores de edad y que además, los estudiantes al tener acceso a

internet, están expuestos a innumerables riesgos como lo son, el grooming, el ciber acoso, ciber estafas y otros ciberataques.

El Ministerio de Educación de la provincia de Córdoba lanzó este año 3 programas de fortalecimiento para las escuelas en todos los niveles educativos. El "programa de fortalecimiento en matemática", el "programa provincial de oralidad, lectura y escritura" y el programa de "leer, escribir y pensar en la cultura digital", siendo este último, un gran avance en la implementación de las TIC en las escuelas de toda la provincia, promoviendo el uso y la capacitación sobre las mismas a todos los docentes de los establecimientos educativos y un acompañamiento constante con material teórico y recursos para implementarlo, dentro de éste programa, el Ministerio de Educación tiene un apartado especial llamado "Las Tecnologías digitales y los procesos socioculturales" donde específicamente tiene como objetivo analizar los riesgos y medidas de seguridad básicas en el uso de dispositivos computacionales conectados a Internet, demostrando así, la importancia de mantener seguras a las instituciones educativas quienes, conectadas a la red, están expuestas a innumerables riesgos.

Tal como señala la Secretaría de Educación, Ministerio de Educación, Gobierno de la Provincia de Córdoba; "La incorporación de las TIC en las escuelas para habitar las sociedades presentes y futuras debe contemplar -en los procesos de enseñanza y aprendizaje - la responsabilidad asumida por la escuela" (p.2). Desarrollaremos entonces en los estudiantes de la Unidad Educativa Maryland el espíritu crítico ante su actuación en internet, a la hora de compartir información y archivos de forma segura siendo internet un espacio virtual compartido, respeto e interacción social, guiando al personal docente de la institución para implementar la ciberseguridad en sus prácticas digitales.

Siendo las TIC un recurso invaluable que promueven y garantizan a los estudiantes de la Unidad Educativa Maryland los derechos en una alfabetización digital que los prepara para la vida en la sociedad y el mundo del trabajo, asegurar su seguridad en el mundo digital y siendo ellos mismos responsables de su uso será nuestro principal objetivo.

Objetivos

Objetivo general

✓ Capacitar a los docentes de nivel secundario y a la coordinadora del departamento de informática de la Unidad Educativa Maryland en el primer semestre del ciclo lectivo 2023, en el uso responsable de las TIC y la ciberseguridad en instituciones educativas, favoreciendo el desarrollo de habilidades informáticas de manera segura.

Objetivos específicos

✓ Desarrollar un dispositivo de formación docente sobre las bases conceptuales de seguridad informática que les permita incorporar hábitos seguros en la web.

✓ Elaborar de manera colaborativa un plan de acción producto final de la capacitación docente que propicie el uso responsable de las TIC.

✓ Evaluar, en el segundo semestre, la puesta en práctica del plan de acción implementado por los docentes y la coordinadora de informática.

Justificación

En base a lo analizado en la Unidad Educativa Maryland, es de vital importancia que los docentes de la institución sean capacitados sobre ciberseguridad escolar para que el uso de las TIC sea de manera responsable y segura. Los entornos educativos representan un espacio ideal para los hackers maliciosos, ya que ingresando al sistema de la institución pueden acceder a información personal de los estudiantes y docentes, bases de datos contables, información de proveedores y datos de investigación, secuestrando y eliminado datos de los sistemas de los usuarios, pudiendo así inhabilitar el acceso, pidiendo posteriormente un rescate para recuperar esa información, usarla para algún otro delito o bien eliminando definitivamente.

La capacitación de este plan de intervención en la Unidad Educativa Maryland, posibilitará a los docentes de nivel medio reflexionar sobre los riesgos potenciales en el uso de las TIC como así también les posibilitará identificar los riesgos a los que está expuesta la seguridad de la información en la escuela para así conocer y aplicar las medidas de protección a la hora de acceder y compartir información personal en la web.

Esta mejora pretende además, que en el transcurso del año, estos conocimientos adquiridos por los docentes de nivel medio, a través del departamento de informática se traslade a todos los docentes de la institución educativa, para reforzar las medidas de seguridad y ofrecer a los estudiantes herramientas para que ellos mismos puedan comprender, analizar y detectar riesgos en la web y así hacer un uso responsable de las mismas, tanto en la escuela como en su vida fuera de ella, garantizándoles un futuro seguro donde la información sea una herramienta que les facilite la vida y no un arma que se use en su contra.

Este plan de intervención será posible en la Unidad Educativa Maryland, ya que al ser una Institución de gestión privada, donde asiste la clase media y alta de la localidad de Villa Allende y las localidades vecinas, cuenta con el capital económico necesario para invertir en este plan, como así también los recursos tecnológicos y edilicios para su realización.

La escuela Maryland tiene un departamento especial de informática, con una coordinadora a cargo y un profesor de informática que trabaja transversalmente con el cuerpo docente de la institución para integrar las TIC a las propuestas curriculares. Además, el departamento de Informática tiene como principal objetivo:

Nuestro objetivo es que a través de la utilización de la computadora como una herramienta, formemos personas que tengan la capacidad de buscar información, seleccionarla, analizarla y evaluarla con juicio crítico, constituyendo un medio ideal para que los niños logren aprendizajes significativos, adquieran habilidades, y desarrollen actitudes que los ayuden a desenvolverse en cualquier ámbito como personas independientes, de manera que les permita tomar decisiones trascendentes. . (Unidad Educativa Maryland, s. f. e. https://bit.ly/2GmAZMZ).

Esta intervención, sumaría a su propuesta académica, la seguridad necesaria para todos los actores sociales que dan uso a las TIC, lo hagan de manera responsable y se eviten inconvenientes dándoles al plantel docente y a los estudiantes las herramientas necesarias para lograrlo.

Marco teórico

En el año 1988 Gusan Morris provocó el colapso de internet, dando la primera alerta de que los sistemas digitales estaban en riesgo. En ese entonces contar con seguridad informática era un privilegio de las grandes corporaciones ya que costaba recursos, dinero, tiempo y esfuerzo.

En el 2010 un virus informático que exponía vulnerabilidades en el sistema operativo de Windows comenzó a circular en las computadoras de millones de usuarios en todo el mundo, surgiendo la necesidad de cuidar la información de los ciudadanos y su propia identidad aparece en el mundo la *ciberseguridad*.

La Dirección nacional de ciberseguridad, define este concepto como la seguridad de las tecnologías de la información, rama de la informática que procura detectar vulnerabilidades que ponen en juego la integridad, disponibilidad y confidencialidad de los sistemas informáticos. (Dirección Nacional de ciberseguridad, 2021)

Los estudiantes de la Unidad Educativa Maryland trabajan desde el jardín de infantes con las TIC, ya sea en juegos, búsqueda de información o elaboración de proyectos interdisciplinarios, siendo las nuevas tecnologías una herramienta utilizada por todos los actores escolares. Hoy casi la totalidad de los niños ingresa a la escuela con cierto grado de dominio en el uso de las TIC, cambiando el papel de las escuelas espectacularmente (Giant, 2016. P 21)

Esta posibilidad de acceso a las TIC significa también el riesgo al que están expuestos los sujetos, sobre todo, la integridad de los estudiantes, al respecto, Unicef emitió un informe donde expresa que a pesar de que los niños están muy presentes en internet –1 de cada 3 usuarios en todo el mundo es un niño– *son muy escasas las medidas que se*

toman para protegerlos de los peligros del mundo digital y para aumentar su acceso a un contenido seguro en línea. (Unicef, 2017), por eso mismo, la necesidad de cuidarlos es imperiosa.

> Es importante tener educación en ciberseguridad desde el jardín con algunos juegos, en la primaria con algo más tangible, en la secundaria y también en la facultad, sin importar la carrera que estudien. Los niños y jóvenes están cada vez más inmersos en el mundo digital y hay un montón de peligros atrás de eso. (Emiliano Piscitelli, 2022)

Podemos, entonces, concientizar a los usuarios para que adquieran conocimiento sobre cuáles son las amenazas a las que están expuestos para y así puedan contar con más recursos a la hora de proteger su información en línea y evitar los ciber ataques. A lo que respecta, Otrera sostiene que podemos enseñarles a ser responsables y prudentes en el uso de las computadoras y darles la oportunidad de que ejerciten su responsabilidad personal (David Otrera, 2016)

La relativa facilidad con la que se puede hacer un mal uso de las herramientas digitales suscita la pregunta *¿Quién les enseñará a utilizar estas herramientas de forma segura?* Apareciendo así el rol de los docentes de la Unidad Educativa Maryland como la población a quienes dirigiremos una capacitación que siente sus bases en los conceptos básicos de la ciberseguridad.

El proceso de capacitación docente se estructura en el marco de la red provincial de formación docente a cargo del Ministerio de educación de la provincia de Córdoba. La ley Federal de educación Nº 24195 en su artículo 19 (a y b) y la recomendación del Consejo Federal de Educación plantean que las exigencias del desempeño del nuevo rol

profesional y los problemas que representa la formación actual, requiere nuevos perfiles profesionales docentes. (Ministerio de Educación de la Nación, 2006)

Pensando entonces en la capacitación, este plan de intervención está dirigido a los docentes de nivel secundario de la Unidad Educativa Maryland con el objetivo de mejorar sus prácticas y proteger su integridad y la de sus estudiantes, propiciando a su vez, una formación que les permita actualizar sus conocimientos en la nueva era digital, con sus respectivos riesgos.

A propósito, Lombardi asegura:

> La capacitación docente es una instancia de articulación entre la teoría y la práctica (…) El perfeccionamiento docente es una práctica que – como todas ellas – tiende puentes entre algo preexistente y algo nuevo a lograr. Por ello es un quehacer social que establece diálogos entre distintos actores sociales e intenta establecer lazos transformadores en esos vínculos. (Gabriela Lombardi, 1997 P. 4)

Es necesario entonces, crear ese puente entre la enseñanza digital que ya está incorporada en la institución y la creciente necesidad de establecer en la misma un ambiente digital seguro para todos los actores. El impacto de la capacitación deberá registrarse luego en el contexto institucional específico para potenciar los aprendizajes con el sentido de innovar en prácticas constituidas.

Esta transformación institucional, será monitoreada así en su impacto en el uso de las TIC de la Unidad Educativa Maryland, con lo que Lombardi denomina un “contrato” entre el formador que posee el saber experto, vinculado al contenido diciplinar y los saberes del capacitando (Gabriela Lombardi, 1997 P. 9)

El instrumento de evaluación de los aprendizajes obtenidos del taller docente se orienta a la realización colaborativa de un plan de acción que establezca procedimientos y pautas claras para trabajar con las TIC, tanto para docentes como para estudiantes.

A lo que respecta, el CEO Founder de Drew, compañía internacional de ciberseguridad, sostiene:

> Crear e implementar un plan de ciberseguridad es más importante que lo que muchos suponen, ya que la cantidad de infracciones relacionadas con la seguridad digital va en ascenso, sobre todo, se evidenció un gran aumento durante la pandemia donde los ciberdelitos aumentaron un 82% en 2021 respecto a años anteriores. (Andrés Pérez Español, 2022)

Un plan de ciberseguridad implica seleccionar e implementar acciones prácticas para protegerse de amenazas externas e internas, ayudando a reducir los riesgos.

La compañía especialista en ciberseguridad Drew, recomienda,

> A la hora de elaborar el plan de acción evaluar los riesgos, establecer los objetivos de seguridad y la tecnología existente en la institución, seleccionar un marco de seguridad y capacitar a los actores sociales intervinientes. (Drew, 2022).

Este plan será realizado en el penúltimo encuentro, durante el primer semestre del año y se pondrá en acción durante el segundo semestre, pudiendo así, al finalizar el ciclo escolar, evaluar su efectividad y hacer los ajustes o modificaciones en el caso de ser necesario, para que, durante el próximo año, lo trabajado en ciberseguridad, se traslade de manera transversal a todo el personal de la Unidad Educativa Maryland.

Con este plan de intervención, capacitando y realizando acciones significativas en el proceso de implementación de las TIC en la institución educativa, propiciamos con la seguridad informática un ambiente digital seguro.

Es responsabilidad de los docentes, sensibilizar a los estudiantes sobre el uso responsable de las tecnologías, algo que la mayoría desconoce, a pesar de vincularse permanentemente con ella.

Prensky, (2013) introduce la expresión "nativos digitales" refiriéndose a los estudiantes actuales que crecieron con estas tecnologías y que sus patrones de comportamiento, lenguaje y procesamiento de información es distinto a las generaciones anteriores diferenciándolos de los que denomina "inmigrantes digitales" que son quienes tuvieron que adaptarse a este nuevo entorno digital, incluidos aquí los docentes. Es por esto que estos talleres están dirigidos a estos "inmigrantes digitales" para que se traslade a los "nativos digitales".

Esta intervención, concuerda con los objetivos de la Dirección Nacional de Ciberseguridad de la Nación que establece que la formulación y ejecución de planes de capacitación en materia de ciberseguridad y la promoción de planes, programas y puntos de innovación tecnológica con organismos competentes en la materia es prioridad. (Dirección Nacional de ciberseguridad, 2010)

En este ciclo lectivo, además, el Ministerio de Educación de la provincia de Córdoba implementa desde su organismo de Igualdad y Calidad educativa, un plan denominado *"Leer, escribir y pensar en la Cultura Digital"* donde ofrece una capacitación permanente a los docentes de los distintos niveles educativos, con material y recursos educativos de utilidad para las TIC. Este plan, en su apartado de "Las tecnologías digitales y los procesos socioculturales" tiene como objetivo:

> Que los estudiantes de nivel primario puedan analizar los riesgos y medidas de seguridad básicas en el uso de dispositivos computacionales conectados a Internet y que, los estudiantes de nivel medio, logren conocer e implementar diferentes configuraciones de privacidad con el fin de proteger los datos personales en la web cuando compartimos información en diferentes formatos y a través de diferentes medios. (Igualdad y calidad, 2022).

Convirtiéndose la seguridad digital en las instituciones educativas post pandemia, un aspecto de suma necesidad e importancia, el Ministerio Público Fiscal y el Ministerio de Educación firmaron en septiembre de 2021 un convenio en el marco de cooperación y colaboración para el abordaje de la ciudadanía digital responsable. Se conformó un equipo de trabajo entre la Oficina Especializada en Ciberdelitos, el Instituto de Formación del Ministerio Publico Fiscal, y los Equipos de Acompañamiento (EPAE; Convivencia Escolar, ESI, Educación Digital Córdoba, Desarrollo Curricular) de la Dirección General de Desarrollo Curricular, Capacitación y Acompañamiento Institucional del Ministerio de Educación, con el propósito de dar respuesta a dicho convenio focalizando en la necesidad de construir desde el ámbito escolar una ciudadanía digital responsable que brinde herramientas para el abordaje de situaciones complejas relacionadas al uso de las redes sociales y dispositivos tecnológicos y así dar respuesta a la creciente necesidad. (Igualdad y Calidad educativa, 2021)

Con los derechos vienen las responsabilidades y cuando permitimos y promovemos el uso de los sistemas de información y comunicación, incluso en el aula, a menudo no destacamos que las responsabilidades deben ir de la mano de estos derechos (Giant, 2016), es por esto que este plan de intervención propone una mejoría en la calidad de enseñanza y una propuesta innovadora acorde a las demandas del siglo XXI.

Síntesis del plan de trabajo

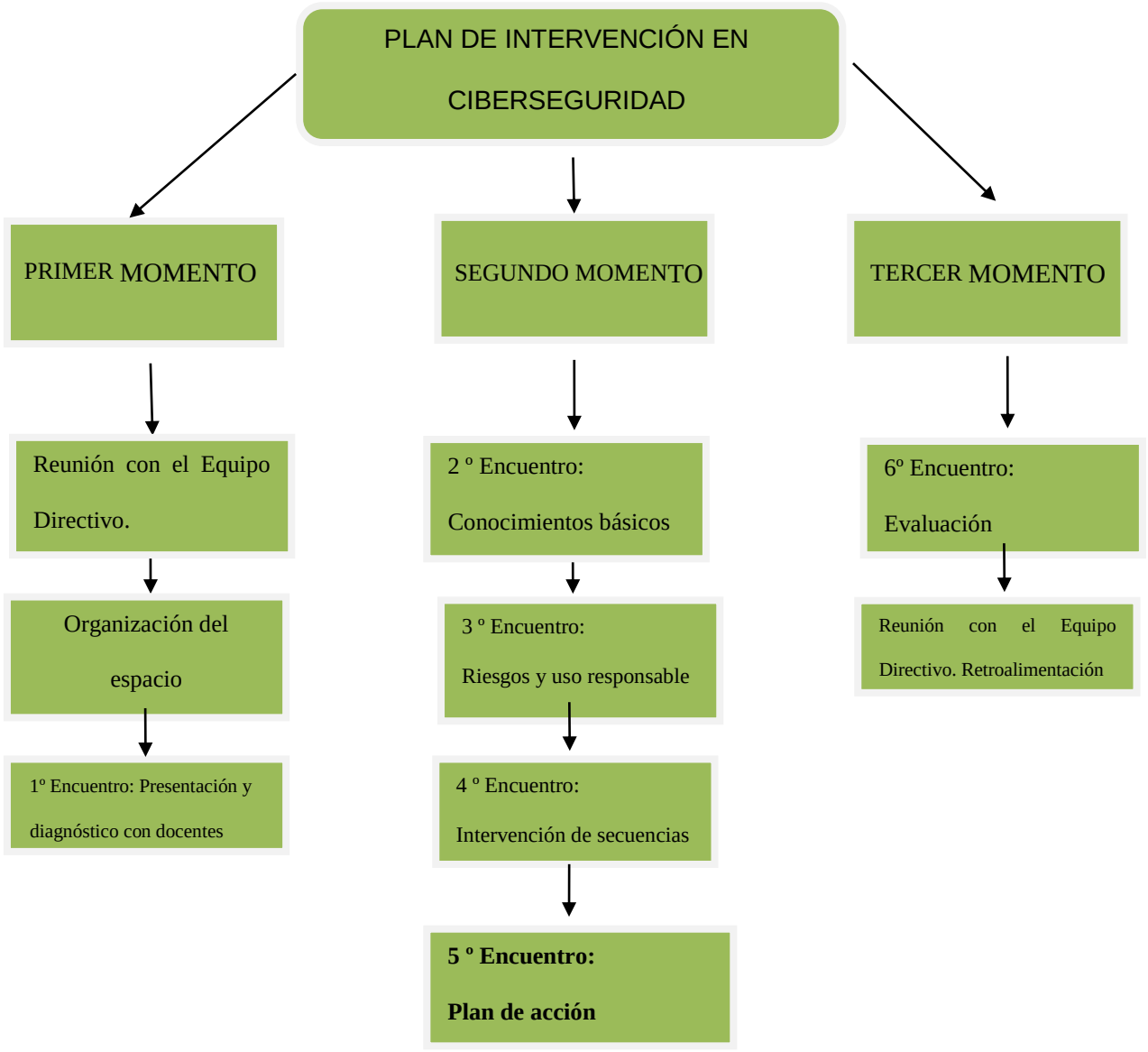


Figura 1

Fuente: elaboración propia, 2022

La intervención propuesta consta de seis encuentros presenciales, cinco de ellos se realizarán de febrero a junio de 2023 y el último en el mes de noviembre, donde tendrá lugar la instancia evaluativa y la entrega de certificados a los participantes. Todos los encuentros serán coordinados por la Licenciada en educación Cinthya Romero.

Estas instancias tendrán formato taller, con 3 horas y media de duración cada uno, considerando 30 minutos para el coffebreak. Están dirigidos al personal docente de nivel secundario y la coordinadora de informática, con la proyección de que lo aprendido se traslade a través del departamento de informática a todos los niveles educativos de la institución.

Se elaborará de manera colaborativo entre los participantes del taller y la Lic. Romero un plan de acción que marque qué hacer en casos donde la ciberseguridad sea vulnerada.

También se propondrá intervenir las secuencias didácticas de los docentes, con el objetivo de evaluar cómo aplican en sus clases el uso responsable de las TIC, esta intervención será trabajada en grupos paralelos duales y luego deliberada entre todos los participantes del taller.

PRIMER MOMENTO

Reunión con el Equipo Directivo *(60')*

Se solicitará una reunión con el Equipo Directivo de la Unidad Educativo Maryland para el día 16 de febrero del 2023, donde la licenciada presenta la propuesta del Plan de Intervención como una alternativa para la mejora de la unidad educativa y con la importancia de garantizar la privacidad de sus integrantes.

Se presenta el diagrama expuesto anteriormente, los recursos necesarios y el presupuesto del plan de intervención y los honorarios de la licenciada.

Se proyectará durante la reunión un esquema realizado en Prezi sintetizando el Plan de Intervención ofrecido.

Organización del espacio y recursos.

La capacitación tendrá lugar en una de las aulas del nivel secundario, la que disponga la institución. Éstas poseen:

- Pizarra digital
- Pizarra de fibra de vidrio.
- Internet banda ancha.

El coffebreak tendrá lugar en la galería de la escuela.

Utilizaremos los siguientes recursos:

- Pizarras (digital y común)
- Proyector
- Las notebooks disponibles en la escuela.
- Vajilla para el coffebreak (Termos, tazas, dispenser de jugo, cucharas y platos)

Primer encuentro: Presentación y diagnóstico con docentes *(180')*

La Licenciada realizará una tarjeta de invitación a los docentes involucrados en la capacitación. La misma será enviada por el equipo directivo a los mismos, mediante mail e informado en una circular, detallando días, horarios y su obligatoriedad.

Se comienza la jornada con la presentación de la licenciada. Para esto, la docente presentará un video titulado *"Se dice de mi"* donde muestra qué dicen de ella algunas personas de su familia, amigos y compañeros de trabajo. *(15')*

Luego de la presentación de la Licenciada, se le propone a los docentes jugar al *"Quién soy?",* juego en el que pasarán y de manera aleatoria, se pondrá en pantalla (a sus espaldas) el nombre de otro profesor. El resto, deberá darle pistas sobre esa persona y el jugador deberá adivinar de quién se trata. *(60')*

A continuación, se presentará el esquema de Prezi, mostrado en la reunión con el equipo directivo, donde la Licenciada comentará brevemente en qué consistirá el taller. *(15')*

Breakcoffe y descanso- *(30')*

A continuación, se pedirá a cada docente que, cuenten qué saben a cerca de la ciberseguridad, que cuenten cómo utilizan las TIC en sus espacios curriculares, si saben los riesgos de la web, cómo se sienten al utilizarlas, cómo vivieron la virtualidad en la pandemia, etc. *(15')*

Luego, utilizando las notebooks a disposición ingresen al link de la Bornstorm y coloquen una palabra que sintetice para ellos el uso de las TIC con los estudiantes.

Finalizado el trabajo, se expondrá el mismo en el proyector para leerlo y comentarlo entre todos. *(15')*

A continuación, se les pedirá que ingresen al link de Padlet (https://onx.la/bf9acy) realicen una entrada donde pongan cada uno qué esperan del taller como si fuera un aviso clasificado donde estén dispuestos a realizar un trueque. *Por ejemplo: Docente de matemática ofrece mates amargos durante toda la capacitación a cambio de aprender a usar un aula virtual. (30')*

Para finalizar el taller, la licenciada les brindará un link de drive, (https://onx.la/16043) donde podrán ver, a medida que transcurren los encuentros, el material audiovisual, teórico y sus producciones.

En el primer documento del drive encontrarán un documento donde deberán completar la tabla con sus datos *(nombre, materia que dicta y correo electrónico).* Esto será utilizado por la licenciada para comunicarse con los integrantes. También se les brindará un correo electrónico al que podrán comunicarse durante la capacitación por consultas o dudas que puedan surgirles.

Responsable	Lic. Cinthya Romero
Recursos	Computadoras, proyector, pizarra digital
Instrumento evaluativo	Bornstorm colaborativa – Asistencia y participación

SEGUNDO MOMENTO

Segundo encuentro con docentes *(180')*

Objetivos:

- Conocer los conceptos básicos de la ciberseguridad.
- Relacionar los contenidos aprendidos con su práctica diaria en el uso de las TIC.

Se comienza el primer encuentro visualizando en pantalla los avisos clasificados creados en Padlet el encuentro anterior. *(20')*

Se presentará a continuación el Power Point (https://onx.la/710f9) donde se explicará de manera breve, qué es la ciberseguridad y su importancia en las instituciones educativas. *(60')*

A continuación se recuperará la información del Power Point, la Licenciada registrará lo que recuerden y expongan los docentes en la pizarra digital, pudiendo ir deslizando páginas y descargando el archivo para luego compartirlo en el drive. *(40')*

Coffebreak y descanso *(30')*

Se propone realizar un "dominó gigante" que sintetice los conceptos claves de la ciberseguridad y el uso responsable de las TIC, expuestos por la licenciada y debatidos entre todos anteriormente.

El dominó se realizará en el gimnasio del establecimiento educativo por razones de espacio.

Responsable	Lic. Cinthya Romero
Recursos	Computadoras, proyector, pizarra digital, fichas de dominó
Instrumento evaluativo	Dominó conceptual

Tercer encuentro con docentes *(180')*

Objetivos:

- Identificar los riesgos a los que están expuestos al utilizar la web en el ámbito educativo.
- Reconocer los riesgos en sus propias prácticas.

Se pedirá a los docentes que formen grupos dividiéndose en cuatro grupos. A cada uno de ellos se les asignará de manera aleatoria, un sobre que contendrá una tarjeta que relate un caso donde se ve afectada la ciberseguridad o donde no se realice un uso responsable de las TIC. Deberán detallar cuál fue el problema detectado y cómo creen que se puede resolver y prevenir. *(30')*

Cada grupo presentará una viñeta online, contando brevemente el caso asignado, mediante la aplicación Pixton (https://www.pixton.com/) para que al proyectarlas, cuenten a sus compañeros cómo proponen resolverlo y cómo se podría prevenir, alentando también a la participación del resto de los docentes.

Se propone un debate entre todas las formas de prevenir y/o solucionar el conflicto presente en el caso de cada grupo. Proponiendo además, posibles casos o situaciones previas que conozcan o los haya tenido como protagonistas. *(60')*

Coffebreak y descanso *(30')*

En el segundo momento, se les solicitará a los docentes crear, en grupos paralelos duales, preguntas para una especialista en ciberseguridad que nos visitará el próximo encuentro. *(30')*

Las preguntas se socializarán en una puesta en común y se definirá el cuestionario en Google form con 10 preguntas. (https://onx.la/61726) *(30')*

Responsable	Lic. Cinthya Romero
Recursos	Computadoras, proyector, pizarra digital, Sobres que incluyan las tarjetas con casos
Instrumento evaluativo	Viñetas – Cuestionario

Cuarto encuentro con docentes *(180')*

Objetivos:

- Profundizar, con la visita de la especialista, las distintas formas de prevenir ciberataques.
- Promover el uso responsable de las TIC en la institución educativa.

Iniciando el taller, se presenta a la especialista en ciberseguridad Ángeles Romero quien observando previamente lo trabajado por el cuerpo docente , ampliará la información sobre los riesgos de los ciberataques y forma de prevenirlos, promoviendo un uso responsable de las TIC *(30')*

A continuación, uno de los docentes realizará a Ángeles las preguntas formuladas el encuentro anterior. *(20')*

Se propone a los docentes, con la información obtenida, armar un podcast con recomendaciones a cerca del uso responsable de las TIC para los estudiantes, el mismo será realizado en el programa Zencastr (https://zencastr.com/) , previamente descargado en una computadora, que luego podrá colgarse en la web de la institución para que pueda acceder toda la comunidad. *(70')*

Coffebreak y descanso *(30')*

Para finalizar el taller se propone crear de manera colaborativa un flyer publicitario en Canva con consejos sobre el uso responsable de las TIC, publicitando el podcast, que se socializará con el resto de la comunidad educativa. *(30')*

Se envía por mail a los docentes, que para el próximo encuentro, seleccionen de sus planificaciones, alguna donde puedan incluir las TIC.

Responsable	Lic. Cinthya Romero – Dev. Ángeles Romero
Recursos	Computadoras, proyector, pizarra digital, micrófono.
Instrumento evaluativo	Creación y uso del podcast, flyer promoviendo la ciberseguridad.

Quinto encuentro con docentes *(180')*

Objetivos:

- Intervenir secuencias didácticas donde sean utilizadas las TIC, promoviendo el uso responsable en los estudiantes.
- Crear un plan de acción que evidencie el uso responsable de las TIC en la comunidad educativa.

En el inicio de la capacitación propone a los docentes que analicen cada uno sus secuencias didácticas, buscando como incluir en la misma las TIC para potenciar alguna actividad propuesta. (30')

Se solicita formar grupos paralelos duales, como única consigna para la conformación de las parejas, se pide que no sean docentes de la misma área, con objetivo de enriquecer el trabajo desde puntos de vista diferentes.

Entre las parejas, intercambiarán sus planificaciones con la intervención realizada. Su compañero deberá analizar si el uso de las TIC en esa actividad se produce

de manera segura. El proceso de análisis de las secuencias, será guiado por la licenciada mediante consignas expuestas en la pizarra digital. (60')

- El uso de las TIC en el trabajo, ¿Enriquece la actividad?
- ¿Se utilizan páginas o aplicaciones seguras y autorizadas para el uso en menores de edad?
- ¿Se protege la identidad de los estudiantes?

Luego del análisis, se les propone a las parejas, incluir en esa actividad con las TIC, un momento donde capaciten a los estudiantes en el uso responsable de la herramienta a utilizar y la importancia de un ciber entorno seguro. *(30')*

Coffebreak y descanso *(30')*

De manera colaborativa, se propone a los docentes la creación de un plan de acción que promueva el uso responsable de las TIC y propicie en la institución un ciberentorno seguro para la comunidad educativa. El mismo, será realizado con la colaboración de la Lic. Romero y se publicará en el drive. (60')

Dicho plan se socializará con la comunidad a través del departamento de informática y estará a disposición en la sala de informática de la escuela.

Tanto las secuencias intervenidas, como el plan de acción supervisado, se pondrán en práctica en la segunda mitad del ciclo lectivo, programando un último encuentro en noviembre para evaluar su efectividad y realizar ajustes en el caso de ser necesario. Se solicita realizar un registro de evidencias.

La Lic. Romero brindará un mail donde los docentes podrán solicitar ayuda en el desarrollo de sus actividades y en la acción del plan, si lo necesitan.

Responsable	Lic. Cinthya Romero
Recursos	Computadoras, proyector, pizarra digital, secuencias didácticas.
Instrumento evaluativo	Intervención de las secuencias, elaboración del plan de acción.

TERCER MOMENTO: Evaluación y cierre *(120')*

15 días antes del encuentro, se les solicita por mail a los docentes, evidencias de las clases implementadas con las secuencias didácticas (registros fotográficos, actividades de los estudiantes, situaciones surgidas en el momento)

Se abre un espacio de puesta en común acerca de las experiencias de los docentes, guiando la participación, con un dado con las siguientes preguntas:

- ¿Surgió algún obstáculo referido al uso de las TIC?
- ¿Alguna situación expuso un riesgo para la ciberseguridad?
- ¿Qué respuesta han tenido sus estudiantes?
- ¿Cómo modificó en su práctica esta capacitación?

A continuación, la licenciada hará una devolución de los trabajos realizados por los docentes a lo largo de la capacitación. (60')

Coffebreak y descanso (30')

Se entrega a los docentes un certificado de participación (30')

Responsable	Lic. Cinthya Romero
Recursos	Proyector, cubo, certificados
Instrumento evaluativo	Grilla evaluativa

Retroalimentación al Equipo Directivo *(40')*

La Lic. Romero, compartirá con el equipo directivo de la Unidad Educativa Maryland los resultados de la capacitación, haciendo entrega de una narrativa que dé cuenta del proceso y dejando a disposición del equipo, el drive de acceso con el trabajo.

Recursos humanos, materiales y edilicios

	Recursos humanos	**Recursos materiales**	**Recursos edilicios**
Responsable	Lic. Cinthya Romero		
Especialista invitada	Dev.Ángeles Romero		
Destinatarios	Cuerpo docente de nivel medio y coordinadora del departamento de informática		
Gastos de librería		Certificados, papelería, fibrones.	
Breakcoffe		Alquiler de vajilla, Café, té, productos de panadería	
Aparatos tecnológicos		Pizarra digital, proyector, computadoras, micrófonos	
Espacios			Aula, dirección, gimnasio

Evaluación

Esta capacitación de ciberseguridad en el ámbito educativo, cuenta con un proceso de evaluación constante y permanente durante su transcurso.

Se propicia en cada instancia evaluativa la capacidad reflexiva, el trabajo colaborativo y el aprendizaje procesual, lo que favorece la implementación de la evaluación formativa. Al respecto Anijovich y Cappeletti, exprensan que:

> La evaluación formativa se aplica con la intención de obtener evidencias sobre la situación de cada estudiante, con respecto a la meta perseguida, desde el comienzo del proceso y no al final, para que el profesor pueda ir reorientando su proceso de enseñanza, a partir de los resultados que se vayan obteniendo, en las evaluaciones formativas aplicadas. (Rebecca Anijovich y Graciela Cappeletti, 2019)

En cada encuentro, se realiza una instancia evaluativa que refleje lo trabajado en el mismo, con instancias de auto evaluación y co evaluación entre los participantes impulsando la capacidad de conciencia sobre su estado de aprendizaje.

Se utilizan diversos instrumentos evaluativos que incluyen grillas, dominó conceptual, análisis de casos, entrevista. Se introducen también, diversas aplicaciones y programas con el objetivo de que los docentes puedan conocerlos, manipularlos y usarlos en sus propias prácticas.

> Cada tipo de instrumento permite evaluar diferentes aspectos de los aprendizajes de los alumnos, es garantizar la pertinencia y calidad técnica del programa considerado integralmente, así como la de cada uno de sus componentes. Es importante hacer notar que la gran disponibilidad de instrumentos de diferente carácter, alcance y función, es un factor de enriquecimiento del abanico de

posibilidades que se abren para el diseño de programas de evaluación (Camillioni, 2008)

Se realizará un registro de las instancias, evidencias fotográficas y se acumulará al final de los encuentros una carpeta virtual en Drive con todo el contenido, donde los docentes podrán ingresar cuando lo necesiten y utilizarlo como recursos que puedan servirles más adelante.

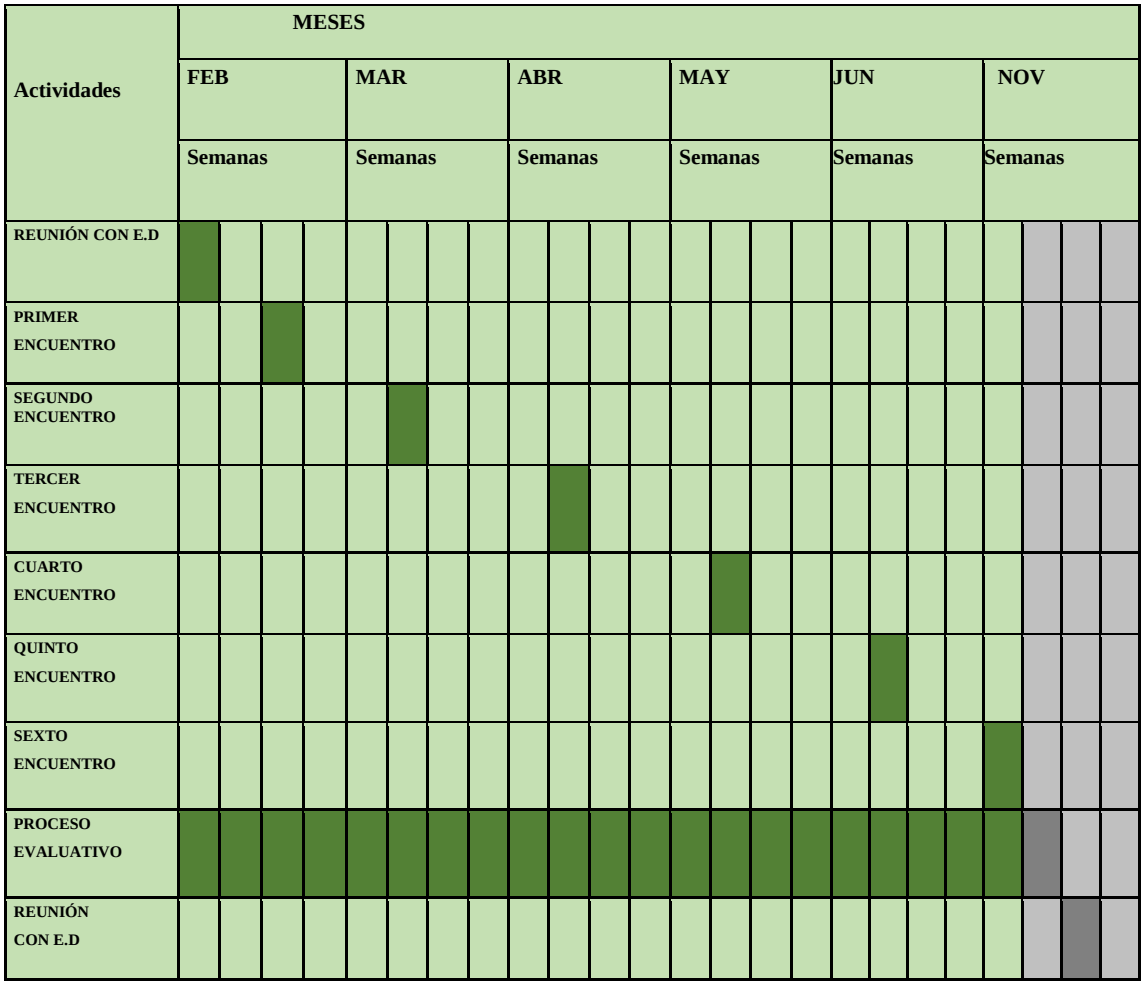
La evaluación final consistirá en la elaboración de un plan de acción que promueva el uso responsable de las TIC para crear un ámbito seguro entre la comunidad educativa.

Serán presentados los resultados obtenidos en el proceso evaluativo al equipo directivo de la Unidad Educativa Maryland en una reunión de retroalimentación al finalizar el plan.

Presupuesto

Concepto	Precio Unitario	Total
Honorarios de la Lic. Cinthya Romero	$6000 por encuentro con docentes (7)	$42.000
Honorarios de la Dev. Ángeles Romero	$5000	$5000
Alquiler de micrófono	$800 por hora	$2500
Alquiler de vajilla	$1000 por encuentro	$7000
Café, té y productos de panadería	$2500 por encuentro	$17500
Insumos de librería	Cubo $500 (cartón, afiche) Dominó $1000 (cartón, afiches, fibrón) Sobres y tarjetas $500 Certificados $2000	$4000

Diagrama de Gantt



Resultados esperados

Mediante el plan de intervención “Ciberseguridad en ambientes educativos” propuesto por la Lic. Cinthya Romero para la Unidad Educativa Maryland, se espera que el cuerpo docente capacitado adquiera los conocimientos básicos en ciberseguridad y desarrolle competencias digitales que les permitan aplicar las TIC en sus clases, de manera segura, optimizando y potenciando su práctica docente. Esto se extiende a todo el personal de la institución, quienes se pretende, sean capacitados luego mediante el departamento de informática.

Se espera a su vez, que los estudiantes de la Unidad Educativa Maryland reconozcan los peligros que existen en la web y tomen decisiones responsables y a conciencia sobre el uso adecuado de la misma, acompañados por sus docentes y familias.

Las herramientas que obtendrán a lo largo de los talleres, junto a la seguridad de los docentes de estar capacitados en el tema, se verá reflejado en mejora de la oferta educativa que ofrece la institución con las competencias propias del siglo XXI.

Conclusión

En la Unidad Educativa Maryland se observó, luego de explorar el material ofrecido por la Universidad Siglo XXI, que en su programa de formación permanente al cuerpo docente, no se tenía en cuenta la capacitación en ciberseguridad, una área que no puede desatenderse.

Se dispone entonces, realizar una intervención en la institución donde se capacite a los docentes y al departamento de informática acerca de ciberseguridad en los ambientes educativos promoviendo el uso responsable de las TIC.

Se realizó una investigación, buscando un apoyo teórico de autores especializados en educación, ciberseguridad y las TIC. También, se analizaron los programas nacionales y provinciales del Ministerio de Educación sobre las TIC en la escuela y la ciberseguridad.

A partir de ello, se organizó con el equipo directivo de la escuela, una reunión informativa donde fue presentado el plan de intervención y la propuesta de la Lic. Romero, para dar comienzo luego, a la formación de los docentes.

La capacitación se desarrolló en el establecimiento educativo desde el mes de febrero al mes de noviembre de 2023, con 6 encuentros presenciales con los docentes del nivel secundario, de tres horas de duración cada uno. Al finalizar, se propone retroalimentar al personal y a los directivos, presentando los resultados obtenidos.

El plan de intervención tuvo como fortalezas la predisposición de todos los agentes intervinientes, los recursos que posee la institución educativa y la retroalimentación permanente entre las partes, pudiendo acompañar todo el proceso según fuera necesario.

Como debilidad, se tuvo que acotar la cantidad de docentes para hacerlo únicamente con los del nivel secundario, quedando la posibilidad de que esta capacitación pueda extenderse luego a toda la comunidad educativa.

Se sugiere que, a partir de la implementación del plan de acción, se realicen los ajustes necesarios teniendo en cuenta las necesidades de la institución y los avances tecnológicos y de ciber delitos que puedan ir surgiendo.

Referencias

Anijovich, R. (2021). *Evaluar para aprender*. Ciudad Autónoma de Buenos Aires. Aique.

Brunner, J.J. (2000, Enero) Educación: Escenarios de Futuro. Nuevas tecnologías y sociedad de la información. *PREAL* (16), p. 15.

Camillioni, A. (1998). *La evaluación de los aprendizajes en el debate didáctico contemporáneo.* Buenos Aires. Miño y Dávila.

Dirección Nacional de Ciberseguridad (2018). Innovación Pública. Tecnologías de la Información. *Ciberseguridad.* Recuperado de:

https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad

Dussel, I. (2011). *Aprender y enseñar en la cultura digital*. Buenos Aires. Santillana.

Españon Perez, A. (2022) *¿Cómo elaborar un plan de ciberseguridad?*. Colombia. Recuperado de:

https://blog.wearedrew.co/ciberseguridad/como-elaborar-un-plan-de-ciberseguridad

Giant, N (2016). *Ciberseguridad para la i generación*. Madrid. Narcea Ediciones. Recuperado de:

https://www.entramar.mvl.edu.ar/uso-responsable-de-las-tic-en-las-escuelas/

Ley Nacional de Educación N° 26.206 (2006) http://www.bnm.me.gov.ar/giga1/documentos/EL002610.pdf

Lombardi, G (1997) *La capacitación docente y sus desafíos*. Ministrerio de Educación. Buenos Aires. Recuperado de: http://www.bnm.me.gov.ar/giga1/documentos/EL004475.pdf

Marés, L (2021) *Claves y caminos para enseñar en ambientes virtuales*. Ciudad Autónoma de Buenos Aires. 2021. Educ.ar S.E

ONU. (2015), Transformar nuestro mundo: La Agenda 2030 para el Desarrollo Sostenible, Resolución aprobada por la Asamblea General de las Naciones Unidas el 25 de septiembre de 2015.

Perez, R (2021) *Ciberseguridad y competencia digital.* Gaptain. 15-5 Recuperado de: https://gaptain.com/blog/?s=ciberseguridad+y+convivencia

Picciteli, E (2022) *La palabra de un experto en ciberseguridad.* La Brújula24. 27-8 Recuperado de:

https://www.labrujula24.com/notas/2022/08/27/cualquier-cosa-que-hagamos-en-el-mundo-digital-repercute-en-el-mundo-fisico-n237915/

Prensky, N. (2013). *Enseñar a nativos digitales*. México. SM Ediciones.

Secretaría de Innovación y Calidad Educativa. (2017). *Marco Nacional de Integración de los Aprendizajes: hacia el desarrollo de capacidades.* Buenos Aires: Ministerio de Educación de la Nación.

Secretaría de Promoción de Igualdad y Calidad Educativa (2018). *Tecnologías de la Información y la Comunicación en la escuela.* Recuperado de: www.igualdadycalidadcba.gov.ar.

Unicef (2017). *Niños en un mundo digital*. New York. División de comunicaciones de Unicef.

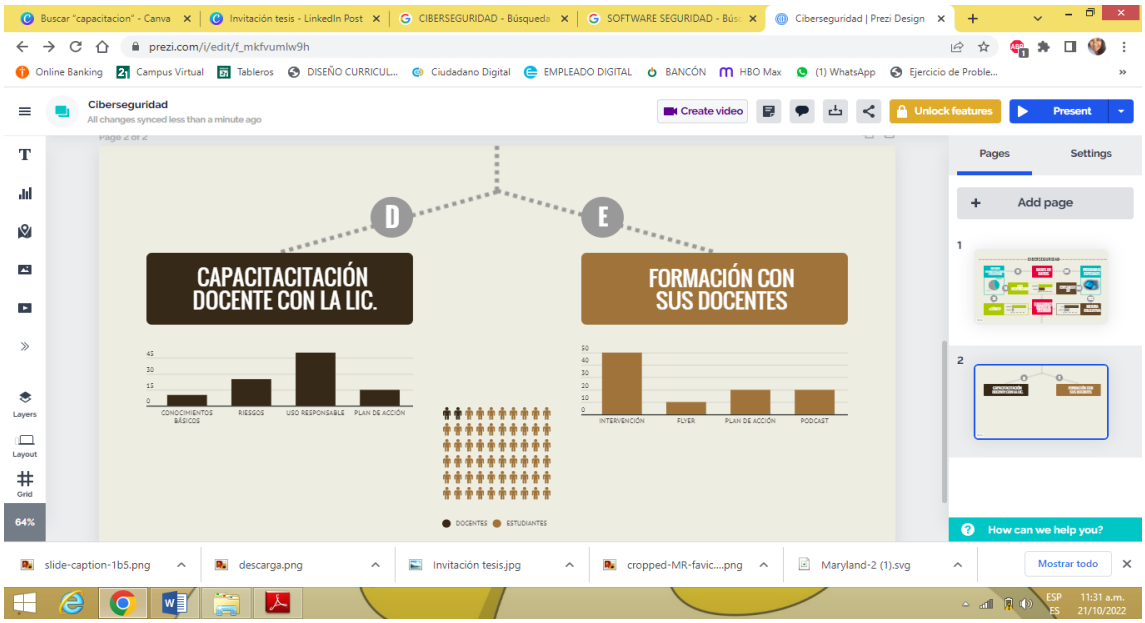
Universidad Siglo 21. (2021). Modulo 0, Plan de Intervención Unidad Educativa Maryland. Recuperado de: https://siglo21.instructure.com/courses/16993/pages/plan-de-intervencion-modulo-0#org3

Anexo

Reunión con el Equipo Directivo

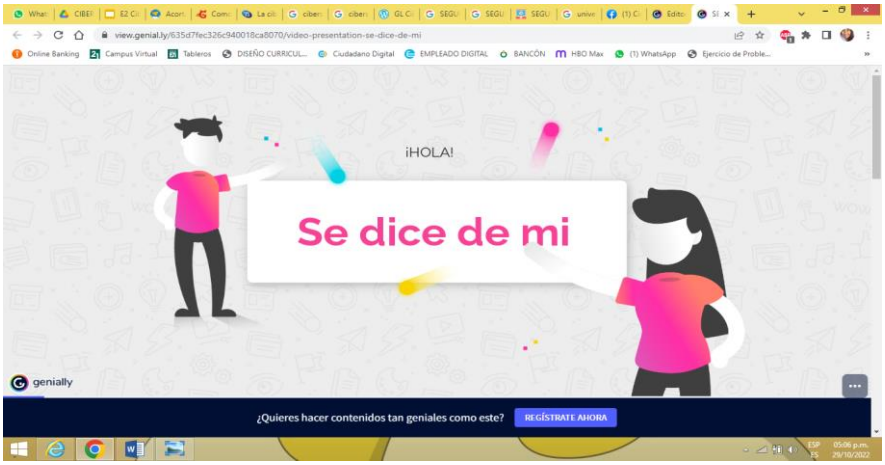
Invitación para los docentes *(Fuente: elaboración propia)*

Prezi:



Fuente: https://prezi.com/i/f_mkfvumlw9h/ *Elaboración propia (2022)*

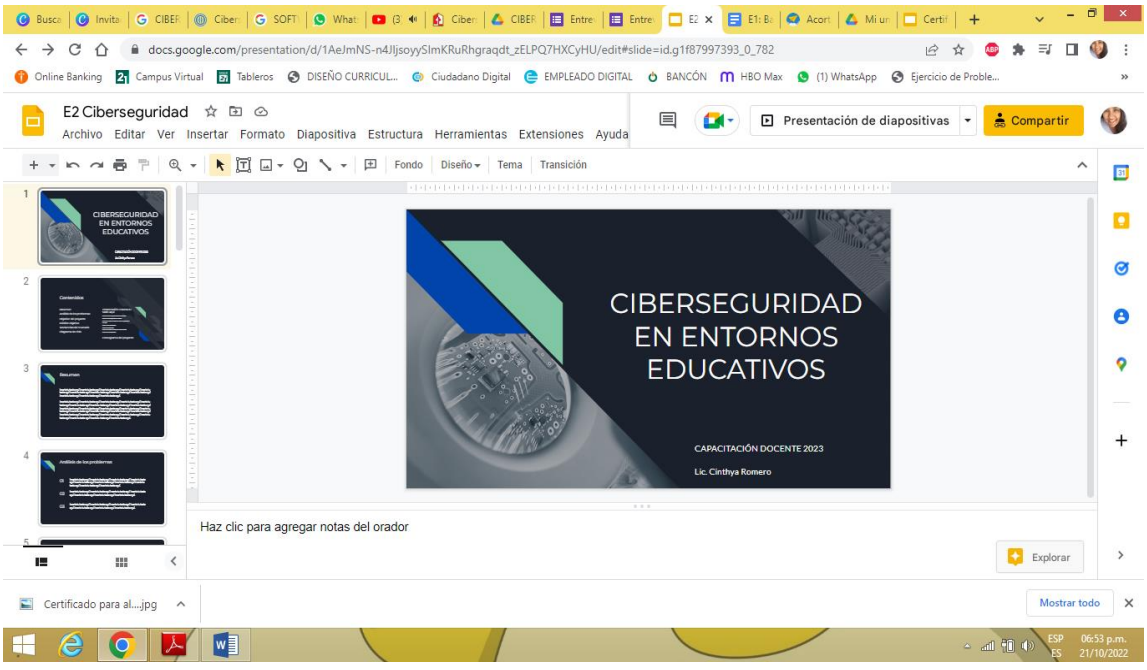
Genially:

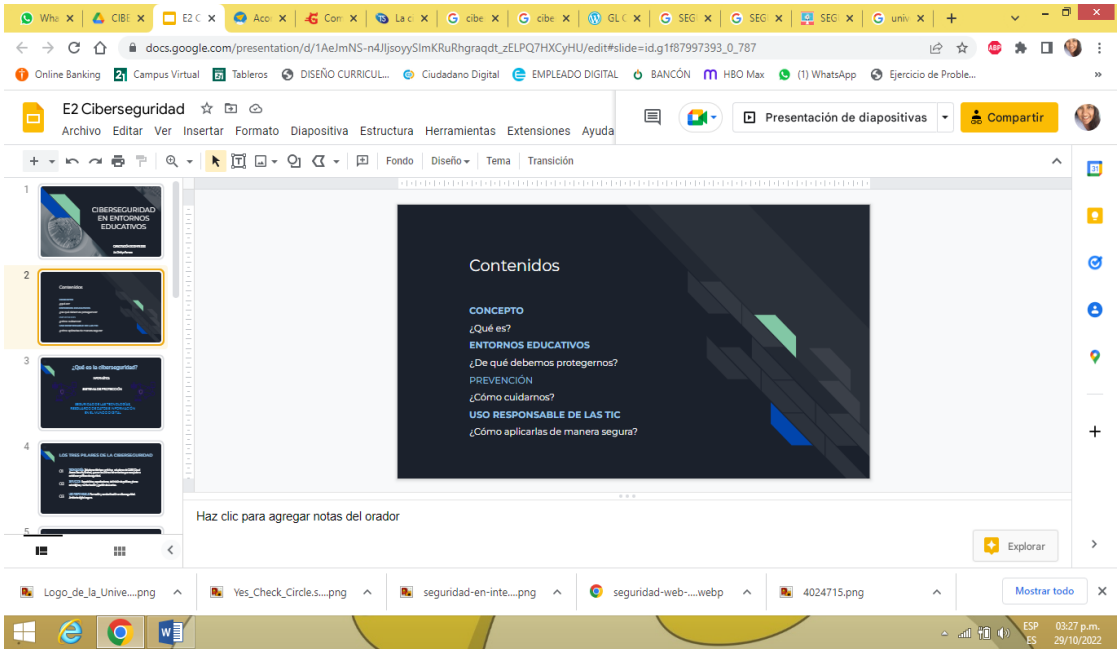


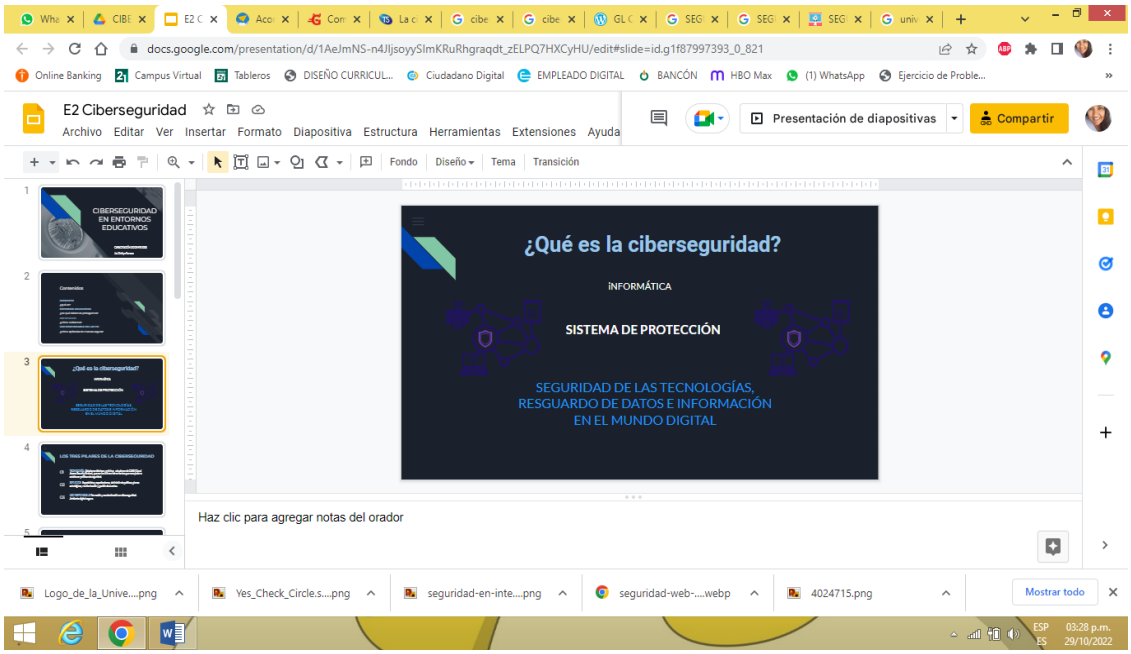
https://view.genial.ly/635d7fec326c940018ca8070/video-presentation-se-dice-de-mi

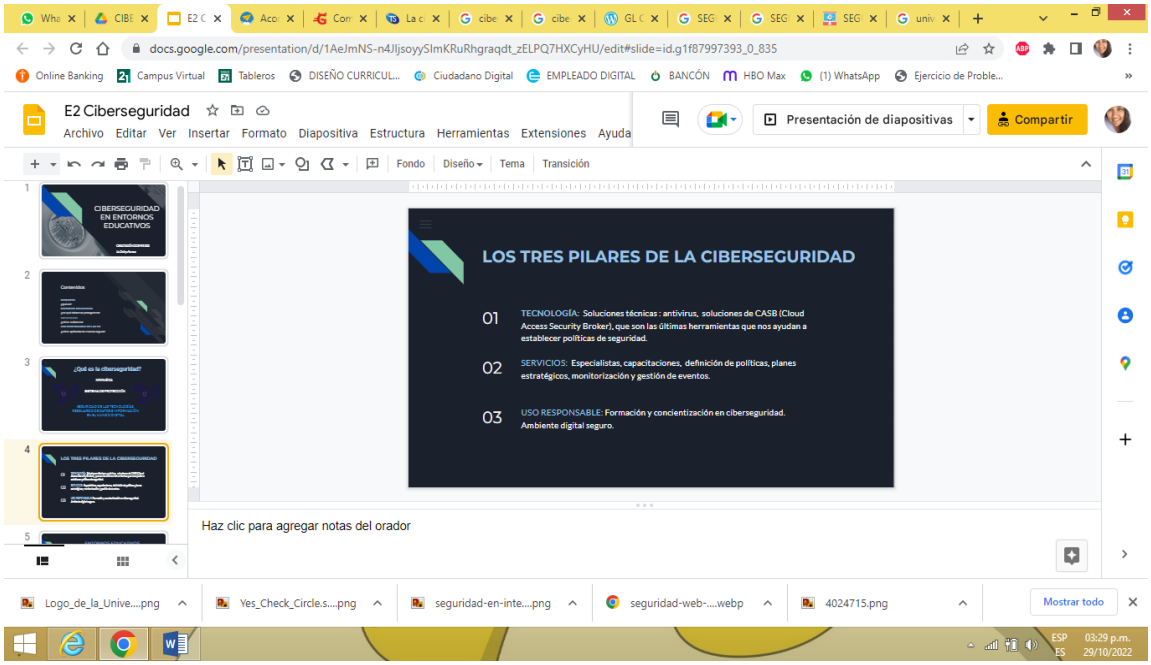
Elaboración propia (2022)

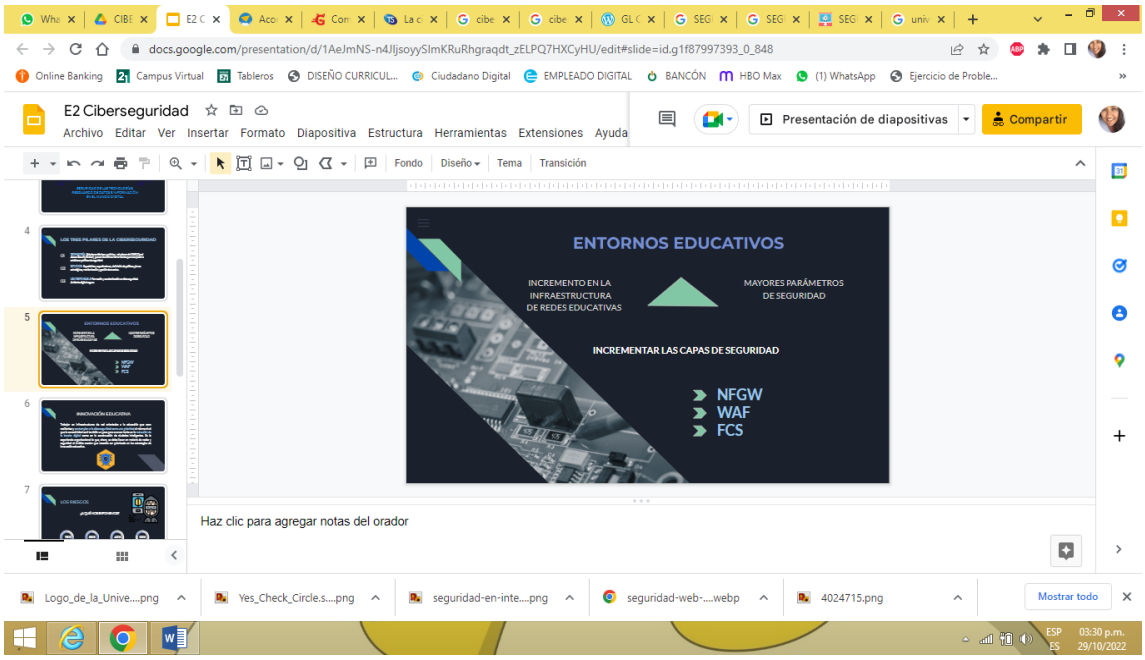
Segundo encuentro

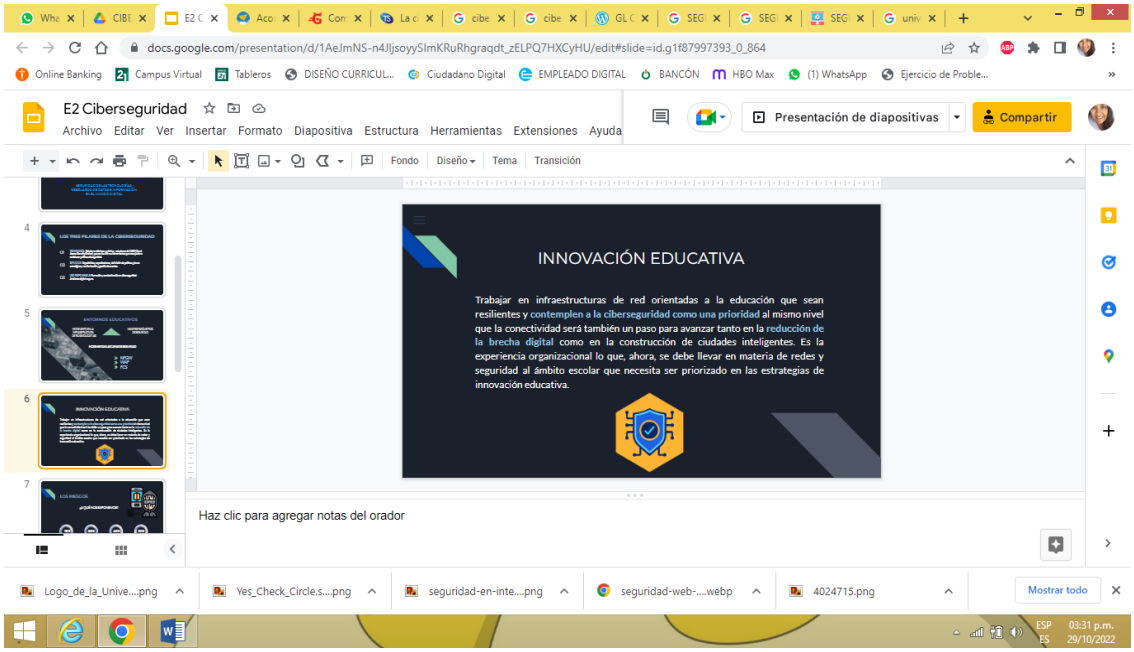


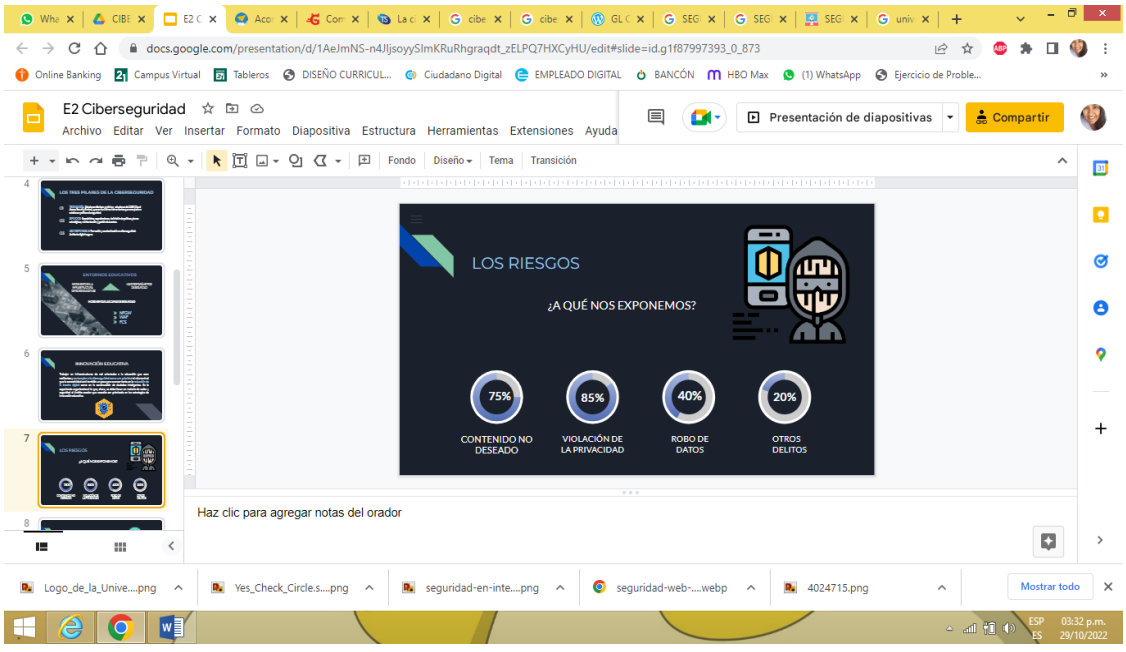

docs.google.com/presentation/d/1AeJmNS-n4JIjsoyySlmKRuRhgraqdt_zELPQ7HXCyHU/edit#slide=id.g1f87997393_0_787
E2 Ciberseguridad
Archivo Editar Ver Insertar Formato Diapositiva Estructura Herramientas Extensiones Ayuda
Presentación de diapositivas
Compartir
Fondo Diseño Tema Transición
Contenidos
CONCEPTO
¿Qué es?
ENTORNOS EDUCATIVOS
¿De qué debemos protegernos?
PREVENCIÓN
¿Cómo cuidarnos?
USO RESPONSABLE DE LAS TIC
¿Cómo aplicarlas de manera segura?
Haz clic para agregar notas del orador
Explorar
Logo_de_la_Unive....png
Yes_Check_Circle.s....png
seguridad-en-inte....png
seguridad-web-....webp
4024715.png
Mostrar todo
ESP
ES
03:27 p.m.
29/10/2022

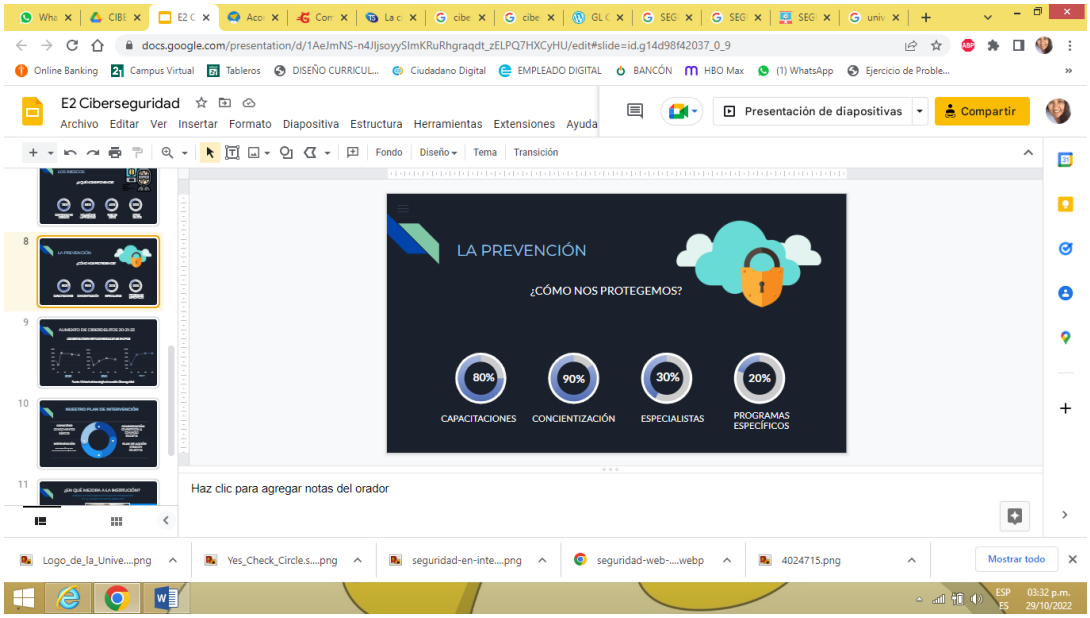

docs.google.com/presentation/d/1AeJmNS-n4JIjsoyySlmKRuRhgraqdt_zELPQ7HXCyHU/edit#slide=id.g1f87997393_0_821
E2 Ciberseguridad
Archivo Editar Ver Insertar Formato Diapositiva Estructura Herramientas Extensiones Ayuda
Presentación de diapositivas
Compartir
Fondo Diseño Tema Transición
¿Qué es la ciberseguridad?
INFORMÁTICA
SISTEMA DE PROTECCIÓN
SEGURIDAD DE LAS TECNOLOGÍAS,
RESGUARDO DE DATOS E INFORMACIÓN
EN EL MUNDO DIGITAL
Haz clic para agregar notas del orador
Logo_de_la_Unive....png
Yes_Check_Circle.s....png
seguridad-en-inte....png
seguridad-web-....webp
4024715.png
Mostrar todo
ESP
ES
03:28 p.m.
29/10/2022

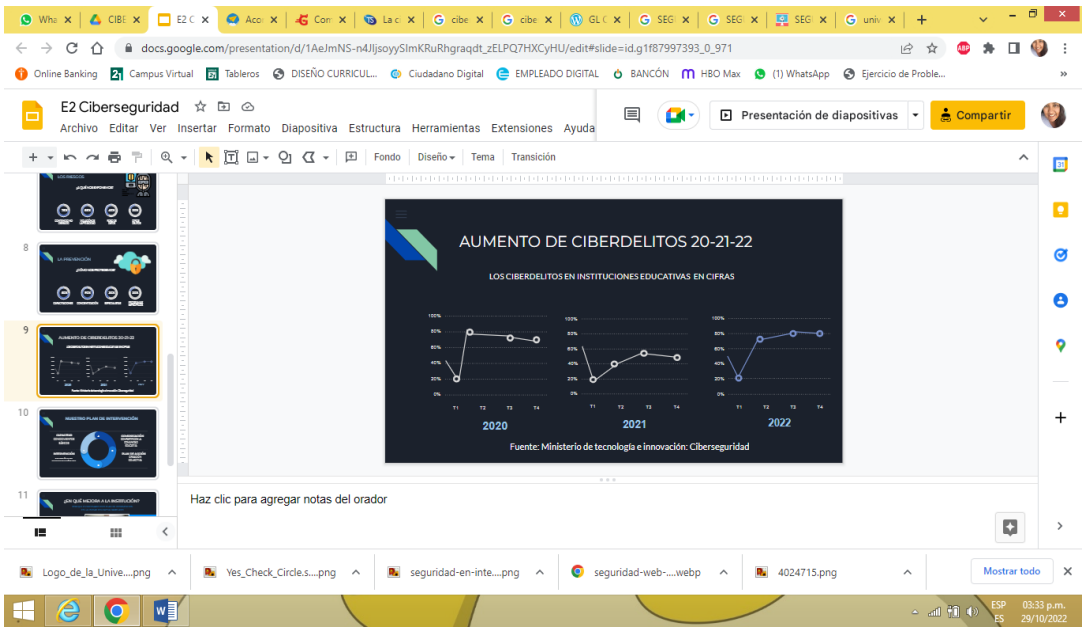

docs.google.com/presentation/d/1AeJmNS-n4JljsoyySlmKRuRhgraqdt_zELPQ7HXCyHU/edit#slide=id.g1f87997393_0_835
E2 Ciberseguridad
Archivo Editar Ver Insertar Formato Diapositiva Estructura Herramientas Extensiones Ayuda
Presentación de diapositivas
Compartir
Fondo
Diseño
Tema
Transición
LOS TRES PILARES DE LA CIBERSEGURIDAD
01 TECNOLOGÍA: Soluciones técnicas : antivirus, soluciones de CASB (Cloud Access Security Broker), que son las últimas herramientas que nos ayudan a establecer políticas de seguridad.
02 SERVICIOS: Especialistas, capacitaciones, definición de políticas, planes estratégicos, monitorización y gestión de eventos.
03 USO RESPONSABLE: Formación y concientización en ciberseguridad. Ambiente digital seguro.
Haz clic para agregar notas del orador
Logo_de_la_Unive....png
Yes_Check_Circle.s....png
seguridad-en-inte....png
seguridad-web-....webp
4024715.png
Mostrar todo
ESP
ES
03:29 p.m.
29/10/2022

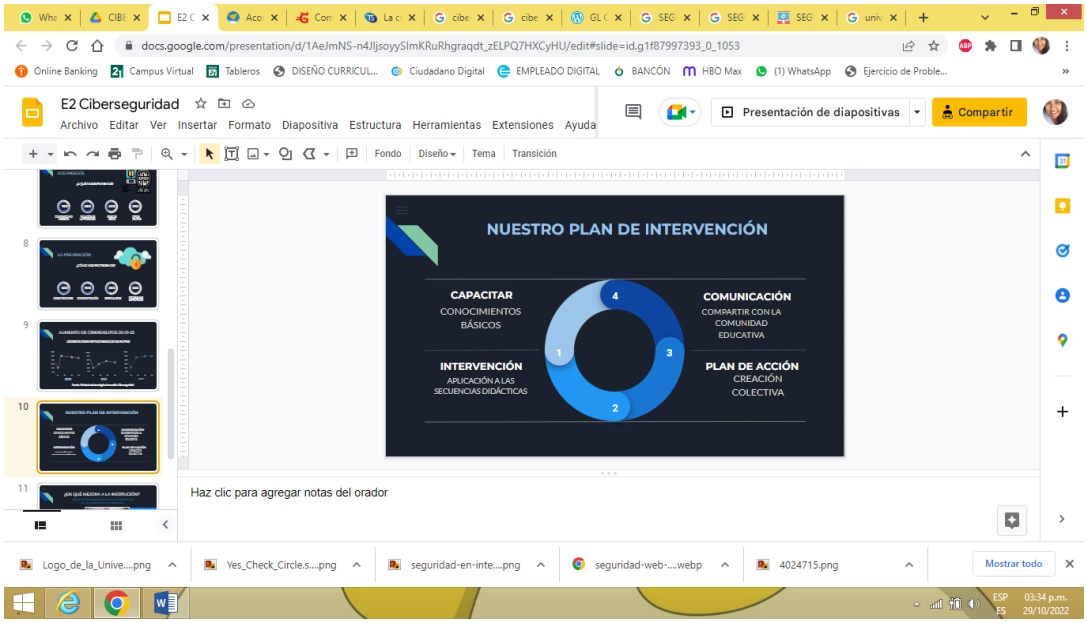

docs.google.com/presentation/d/1AeJmNS-n4JljsoyySlmKRuRhgraqdt_zELPQ7HXCyHU/edit#slide=id.g1f87997393_0_848
E2 Ciberseguridad
Archivo Editar Ver Insertar Formato Diapositiva Estructura Herramientas Extensiones Ayuda
Presentación de diapositivas
Compartir
Fondo
Diseño
Tema
Transición
ENTORNOS EDUCATIVOS
INCREMENTO EN LA INFRAESTRUCTURA DE REDES EDUCATIVAS
MAYORES PARÁMETROS DE SEGURIDAD
INCREMENTAR LAS CAPAS DE SEGURIDAD
NFGW
WAF
FCS
Haz clic para agregar notas del orador
Logo_de_la_Unive....png
Yes_Check_Circle.s....png
seguridad-en-inte....png
seguridad-web-....webp
4024715.png
Mostrar todo
ESP
ES
03:30 p.m.
29/10/2022

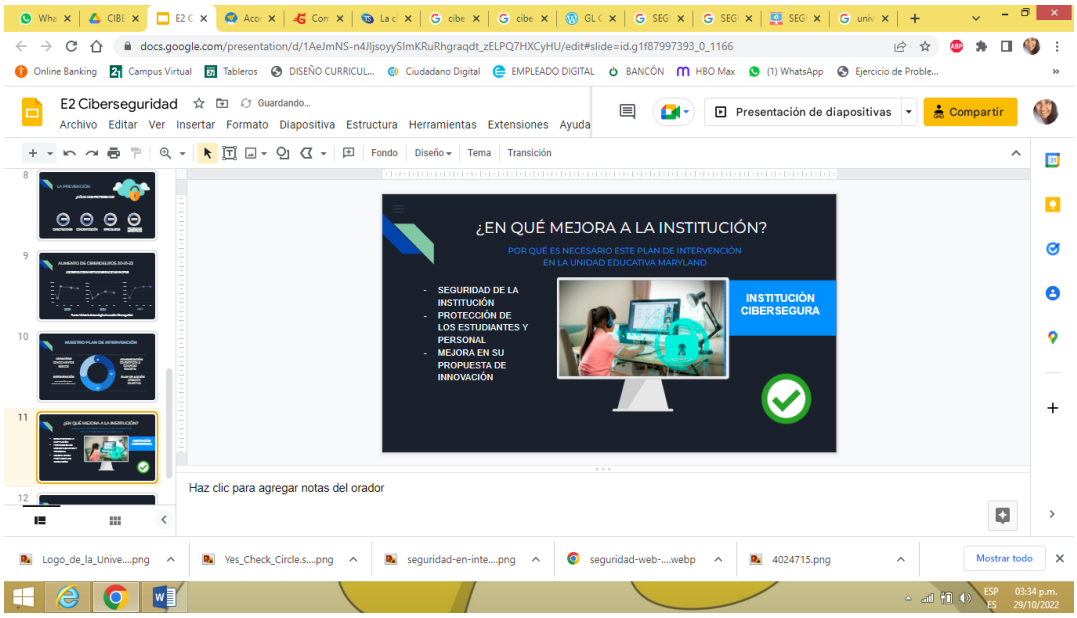

docs.google.com/presentation/d/1AeJmNS-n4JljsoyySImKRuRhgraqdt_zELPQ7HXCyHU/edit#slide=id.g1f87997393_0_864
E2 Ciberseguridad
Archivo Editar Ver Insertar Formato Diapositiva Estructura Herramientas Extensiones Ayuda
Presentación de diapositivas
Compartir
Fondo Diseño Tema Transición
INNOVACIÓN EDUCATIVA
Trabajar en infraestructuras de red orientadas a la educación que sean resilientes y contemplen a la ciberseguridad como una prioridad al mismo nivel que la conectividad será también un paso para avanzar tanto en la reducción de la brecha digital como en la construcción de ciudades inteligentes. Es la experiencia organizacional lo que, ahora, se debe llevar en materia de redes y seguridad al ámbito escolar que necesita ser priorizado en las estrategias de innovación educativa.
Haz clic para agregar notas del orador
Logo_de_la_Unive....png
Yes_Check_Circle.s....png
seguridad-en-inte....png
seguridad-web-....webp
4024715.png
Mostrar todo
ESP ES
03:31 p.m.
29/10/2022

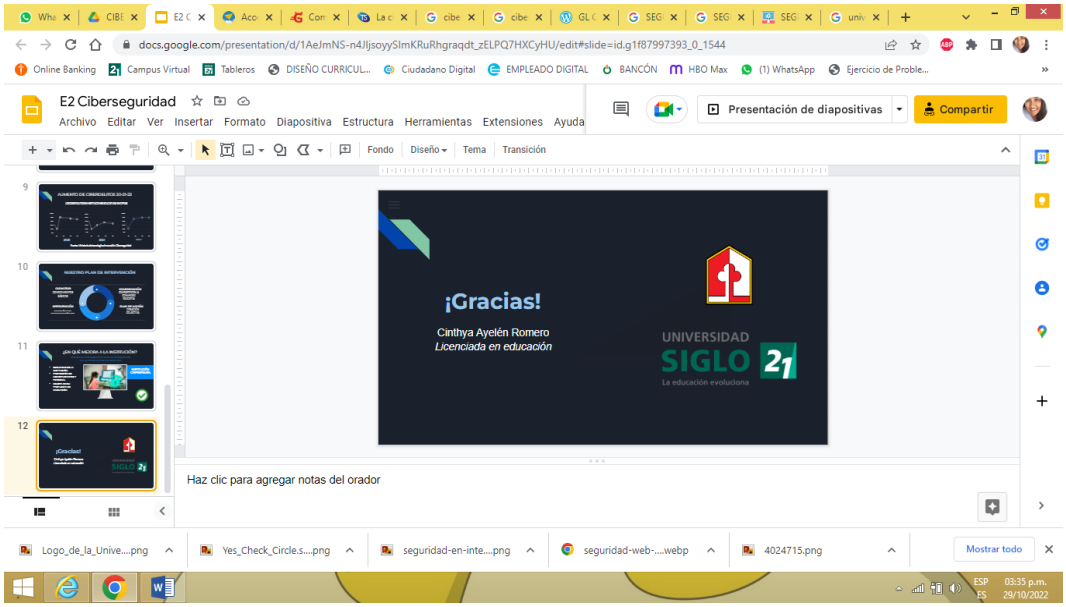

docs.google.com/presentation/d/1AeJmNS-n4JljsoyySImKRuRhgraqdt_zELPQ7HXCyHU/edit#slide=id.g1f87997393_0_873
E2 Ciberseguridad
Archivo Editar Ver Insertar Formato Diapositiva Estructura Herramientas Extensiones Ayuda
Presentación de diapositivas
Compartir
Fondo Diseño Tema Transición
LOS RIESGOS
¿A QUÉ NOS EXPONEMOS?
75%
CONTENIDO NO DESEADO
85%
VIOLACIÓN DE LA PRIVACIDAD
40%
ROBO DE DATOS
20%
OTROS DELITOS
Haz clic para agregar notas del orador
Logo_de_la_Unive....png
Yes_Check_Circle.s....png
seguridad-en-inte....png
seguridad-web-....webp
4024715.png
Mostrar todo
ESP ES
03:32 p.m.
29/10/2022


docs.google.com/presentation/d/1AeJmNS-n4JIjsoyySImKRuRhgraqdt_zELPQ7HXCyHU/edit#slide=id.g14d98f42037_0_9
E2 Ciberseguridad
Archivo Editar Ver Insertar Formato Diapositiva Estructura Herramientas Extensiones Ayuda
Presentación de diapositivas
Compartir
Fondo
Diseño
Tema
Transición
LA PREVENCIÓN
¿CÓMO NOS PROTEGEMOS?
80%
CAPACITACIONES
90%
CONCIENTIZACIÓN
30%
ESPECIALISTAS
20%
PROGRAMAS ESPECÍFICOS
Haz clic para agregar notas del orador
Mostrar todo
03:32 p.m.
29/10/2022


docs.google.com/presentation/d/1AeJmNS-n4JIjsoyySImKRuRhgraqdt_zELPQ7HXCyHU/edit#slide=id.g1f87997393_0_971
E2 Ciberseguridad
Archivo Editar Ver Insertar Formato Diapositiva Estructura Herramientas Extensiones Ayuda
Presentación de diapositivas
Compartir
Fondo
Diseño
Tema
Transición
AUMENTO DE CIBERDELITOS 20-21-22
LOS CIBERDELITOS EN INSTITUCIONES EDUCATIVAS EN CIFRAS
2020
2021
2022
Fuente: Ministerio de tecnología e innovación: Ciberseguridad
Haz clic para agregar notas del orador
Mostrar todo
03:33 p.m.
29/10/2022


docs.google.com/presentation/d/1AeJmNS-n4JIjsoyySlmKRuRhgraqdt_zELPQ7HXCyHU/edit#slide=id.g1f87997393_0_1053
E2 Ciberseguridad
Archivo Editar Ver Insertar Formato Diapositiva Estructura Herramientas Extensiones Ayuda
Presentación de diapositivas
Compartir
Fondo
Diseño
Tema
Transición
NUESTRO PLAN DE INTERVENCIÓN
CAPACITAR
CONOCIMIENTOS BÁSICOS
COMUNICACIÓN
COMPARTIR CON LA COMUNIDAD EDUCATIVA
INTERVENCIÓN
APLICACIÓN A LAS SECUENCIAS DIDÁCTICAS
PLAN DE ACCIÓN
CREACIÓN COLECTIVA
Haz clic para agregar notas del orador
Logo_de_la_Unive....png
Yes_Check_Circle.s....png
seguridad-en-inte....png
seguridad-web-....webp
4024715.png
Mostrar todo
ESP
ES
03:34 p.m.
29/10/2022

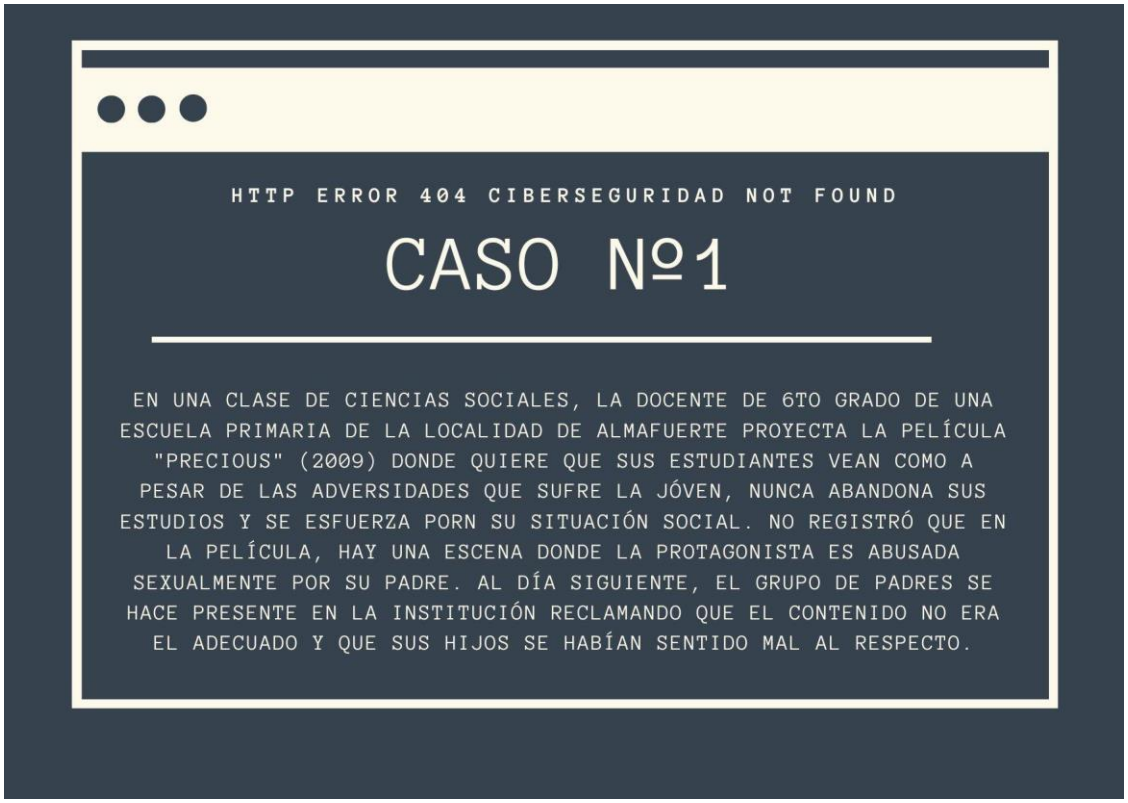

docs.google.com/presentation/d/1AeJmNS-n4JIjsoyySlmKRuRhgraqdt_zELPQ7HXCyHU/edit#slide=id.g1f87997393_0_1166
E2 Ciberseguridad
Guardando...
Archivo Editar Ver Insertar Formato Diapositiva Estructura Herramientas Extensiones Ayuda
Presentación de diapositivas
Compartir
Fondo
Diseño
Tema
Transición
¿EN QUÉ MEJORA A LA INSTITUCIÓN?
POR QUÉ ES NECESARIO ESTE PLAN DE INTERVENCIÓN EN LA UNIDAD EDUCATIVA MARYLAND
- SEGURIDAD DE LA INSTITUCIÓN
- PROTECCIÓN DE LOS ESTUDIANTES Y PERSONAL
- MEJORA EN SU PROPUESTA DE INNOVACIÓN
INSTITUCIÓN CIBERSEGURA
Haz clic para agregar notas del orador
Logo_de_la_Unive....png
Yes_Check_Circle.s....png
seguridad-en-inte....png
seguridad-web-....webp
4024715.png
Mostrar todo
ESP
ES
03:34 p.m.
29/10/2022



Fuente: https://onx.la/d2daa *Elaboración propia (2022)*

Tercer encuentro

Tarjeta de casos



HTTP ERROR 404 CIBERSEGURIDAD NOT FOUND

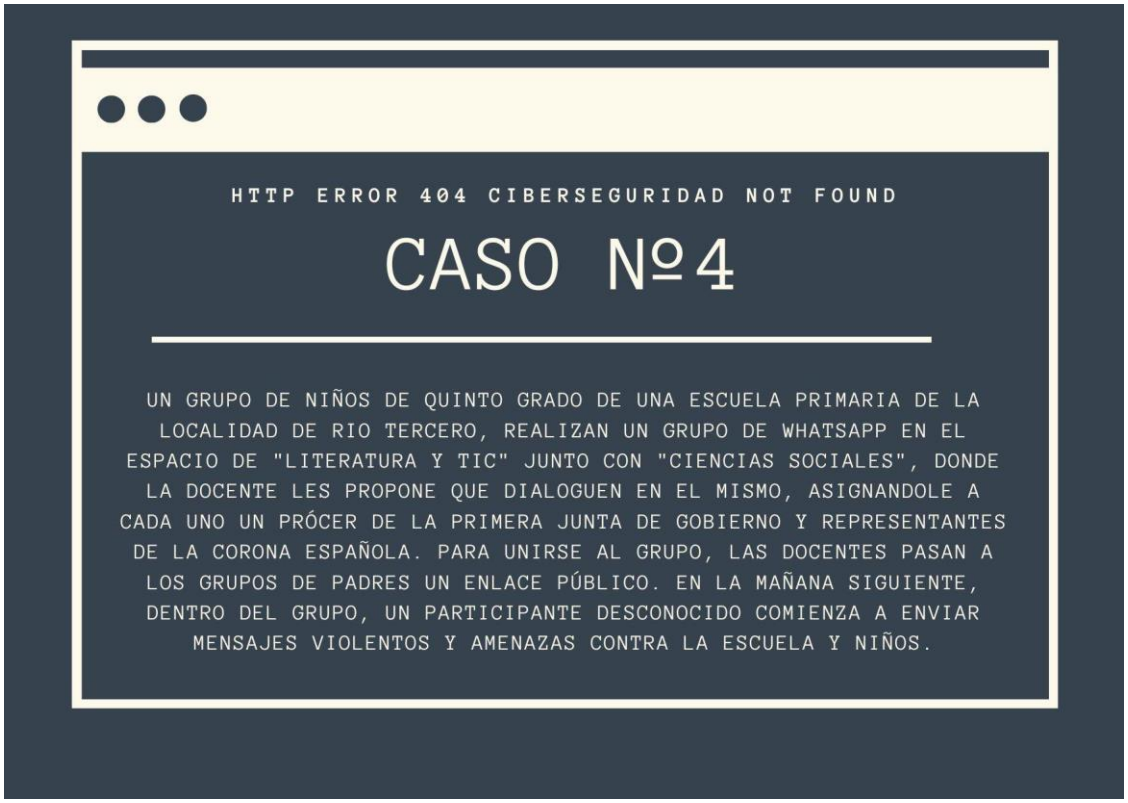
CASO Nº2

LA DOCENTE DE 4TO GRADO DE UNA ESCUELA PRIMARIA DE LA LOCALIDAD DE RÍO TERCERO, ORGANIZA PARA LA PROMESA DE LA BANDERA DE SUS ESTUDIANTES UNA TRANSMISIÓN EN VIVO DEL ACTO POR YOUTUBE, YA QUE DEBIDO A LAS RESTRICCIONES POR EL PROTOCOLO COVID19, LOS PADRES DE LOS ESTUDIANTES NO PODÍAN PARTICIPAR DEL MISMO.
A LA SEMANA SIGUIENTE LLEGA A LA ESCUELA UNA DENUNCIA Y UNA DEMANDA INICIADA POR EL PADRE DE UNA ESTUDIANTE, MANIFESTANDO QUE HABÍAN DIVULGADO LA IMÁGEN DE SU HIJA MENOR DE EDAD POR UN CANAL PÚBLICO.

HTTP ERROR 404 CIBERSEGURIDAD NOT FOUND

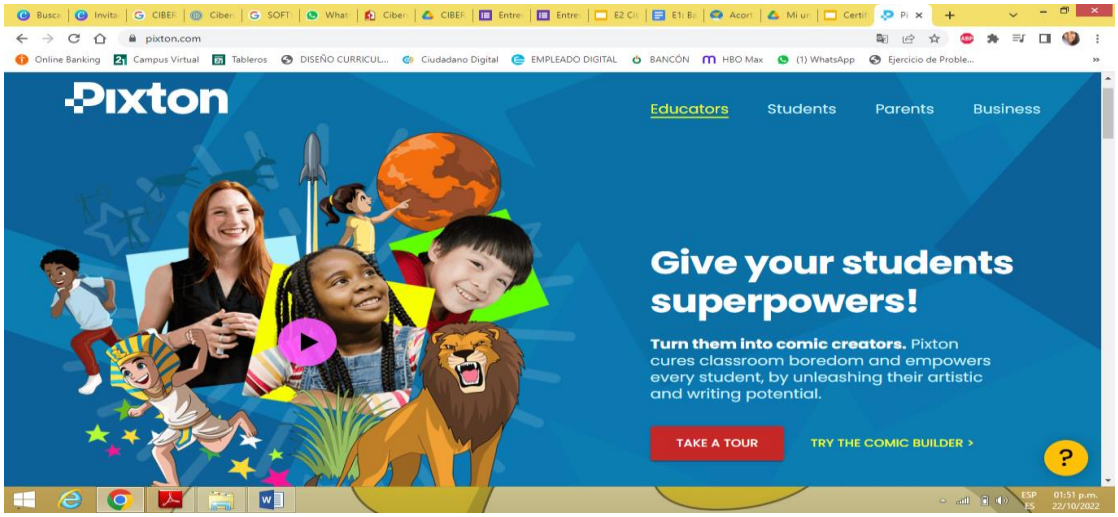
CASO Nº3

16 PADRES DE LOS ESTUDIANTES DE UNA ESCUELA SECUNDARIA DE LA LOCALIDAD DE RÍO TERCERO, RECIBEN EN EL TRANSCURSO DE LA MAÑANA, LLAMADOS QUE DICEN SER DE LA ESCUELA, DONDE MANIFIESTAN QUE SUS HIJOS HAN SUFRIDO UN ACCIDENTE ESCOLAR Y QUE PARA SER TRASLADADOS, NECESITAN UN TRANSFERENCIA A UNA CUENTA DE MERCADOPAGO DE LA INSTITUCIÓN, HASTA QUE LLEGUEN LOS PADRES AL NOSOCOMIO. LES BRINDAN A LOS PADRES, DATOS PERSONALES DE LOS ESTUDIANTES. 5 FAMILIAS CAEN EN LA ESTAFA Y REALIZAN LA TRANSFERENCIA.



Fuente: https://www.canva.com/ *Elaboración propia (2022)*

Viñetas Pixton



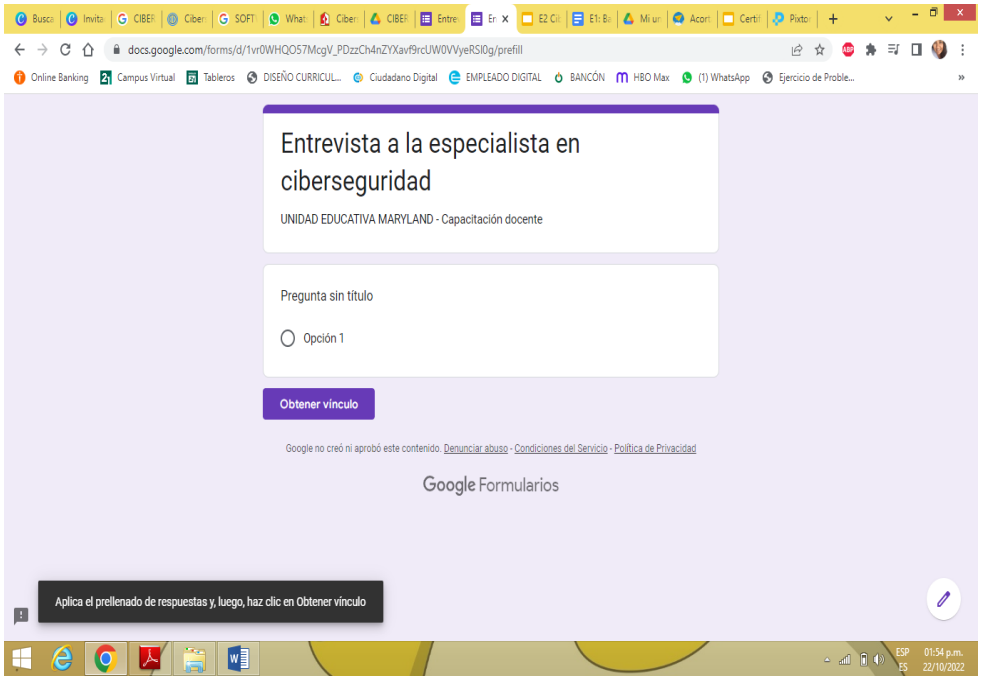
Fuente: https://www.pixton.com/

Dominó conceptual

LA CIBERSEGURIDAD	Conjunto de políticas, estrategias y acciones orientadas a elevar los niveles de seguridad de las personas frente a incidentes y delitos informáticos.
Elaborar un plan de acción favorece	Un ambiente ciberseguro en la Institución educativa
Ámbito seguro para el uso de la web	Utilizando: servidores autorizados, páginas web educativas, acceso restringido para estudiantes.
Favorece el cuidado y respeto por la identidad de los menos de edad	Existen leyes que protegen los derechos y la identidad digital
Ley Ley 26.388 de Delito informático Ley 25.326 de Protección de Datos Personales	Respaldadas por el Ministerio de Seguridad, área de ciberseguridad de la Nación.
Organismo que brinda protección a las infraestructuras críticas de información, generando y mejorando las capacidades de prevención, detección, respuesta y recupero ante incidentes de seguridad informática a nivel nacional.	Jefatura de Gabinete de Ministros: Innovación Pública.
Brindan los servicios de capacitación, denuncias de delitos informáticos, recomendaciones y un equipo de respuestas ante emergencias informáticas.	Tienen como objetivo alcanzar la información a toda la población de la República Argentina para evitar fraudes, crímenes informáticos y hackers.

Fuente: *elaboración propia (2022)*

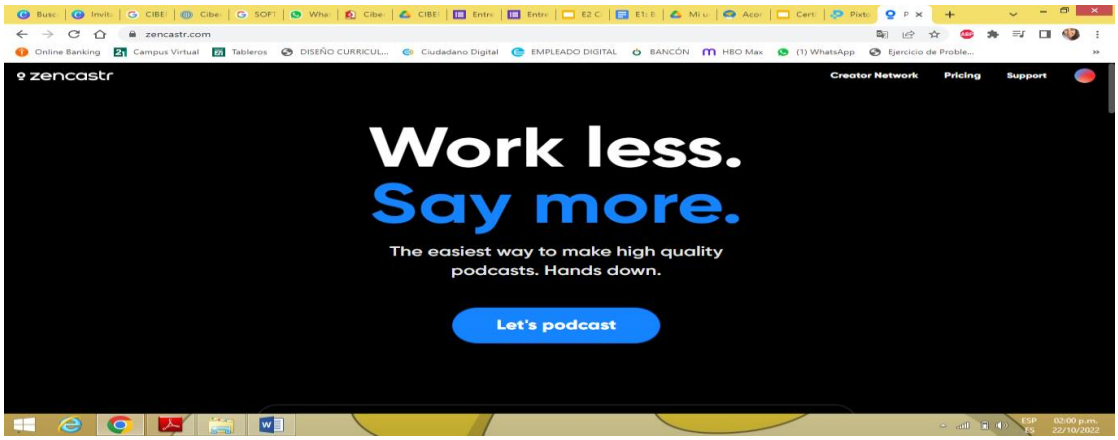
Google Form:



Fuente: https://onx.la/d2daa *Elaboración propia (2022)*

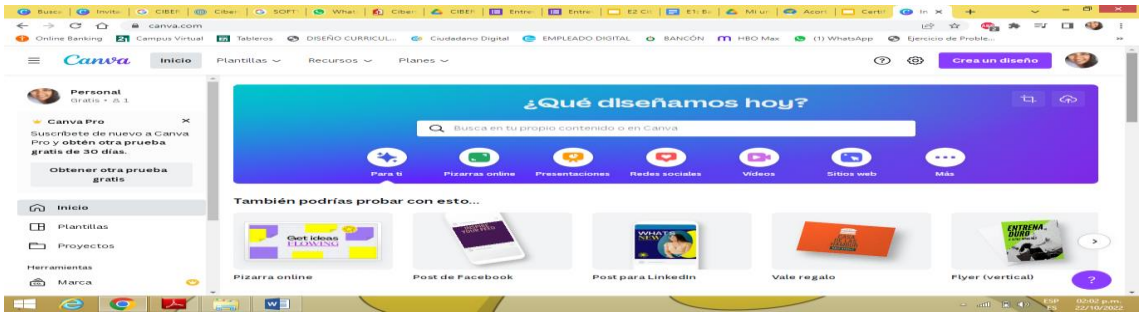
Cuarto encuentro

Zencastr



Fuente: https://zencastr.com/

Canva



Fuente: https://www.canva.com/

Sexto encuentro

Grilla evaluativa

Referencias: (S) Siempre / (G) Generalmente/ O (Ocasionalmente)/ N (Nunca)

Docente	¿Incluye las TIC para potenciar el aprendizaje de sus clases?	¿Realiza un uso responsable de las TIC?	¿Identifica los potenciales riesgos a los que está expuesto al utilizar la web?	¿Pone en acción estrategias de prevención contra el uso indebido de las TIC?	¿Planifica y ejecuta momentos de capacitación a sus estudiantes propiciando un uso responsable de las TIC?	¿Sigue el plan de acción elaborado con sus pares para la ciberseguridad en la institución?

Fuente: *elaboración propia 2022*

Certificado de asistencia

Fuente: Elaboración propia 2022.