Colegio Inmaculada Concepción
Puerto Montt

PROTOCOLO DE AULAS DIGITALES

En el año 2021 el colegio adquirió nuevas tecnologías para que nuestros alumnos y alumnas tengan acceso al conocimiento a través de estas nuevas herramientas, logrando un aprendizaje de calidad en un entorno digital agradable y motivante. Se equiparon con televisores y computadores (torres) todas las salas de clases, en tanto, todos los notebooks se trasladaron al laboratorio de computación de enseñanza básica, renovando el equipamiento. Con este propósito el Equipo de Informática Educativa del colegio, ha diseñado el presente protocolo dando a conocer el marco que circunscribe la actuación que los usuarios deben tener frente al uso de dichas herramientas.

I.-FUNDAMENTACIÓN

En la actualidad el uso de herramientas tecnológicas en educación y nuestra sociedad se ha multiplicado con mucha celeridad y es absolutamente necesario educar a nuestros alumnos y alumnas en ciudadanía digital.

¿Qué es la educación ciudadana digital?

Para el Ministerio de Educación la ciudadanía digital abarca:

Conocimientos sobre:

- El uso de la Tecnologías de la Información y la Comunicación.
- Conocer nuestro derechos y deberes digitales
- Comprender el impacto que la Tics. tienen sobre la vida personal y el entorno.

Se desarrollan habilidades como:

- Responsabilidad
- Seguridad digital
- La autorregulación
- Etica
- Libertad
- Participación
- Desenvolverse en un ecosistema digital.

1.-POLITICAS DE CIBERSEGURIDAD

(tomado del documento "Consejo de seguridad 360° de Entel) (3)

Aprendizaje permanente

Los ataques informáticos que afectan a la seguridad se producen por desconocimiento de la ciberseguridad. Por ello es importante practicar un aprendizaje permanente ya sea formal e informal de los usuarios respecto de esta importante temática.

Crear una cultura de ciberseguridad. Es absolutamente necesario abrir espacio a esta nueva cultura a través de lo siguiente:

- Crear, mantener, informar y revisar políticas de ciberseguridad:
- Uso de software y hardware
- Políticas de contraseñas
- Políticas de carácter técnico: mantenimiento, copias de seguridad, protección de datos, sobre las memorias externas, entre otras.
- Políticas de carácter formativo: deberes y derechos digitales.

Ciberseguridad de terceros

Fallas en la seguridad en los sistemas de sus proveedores o colaboradores. Concientizar sobre los ciberriesgos informáticos por intrusión. Es decir, estar en contante comunicación con estos agentes externos.

Constante actualización

Disponer de un sistema informático actualizado a nivel de software como hardware.

Simulacros

Realizar simulacros regularmente. Por ejemplo, de email phishing.

Innovación tecnológica

Introducir novedades y buscar formas de mejorar la seguridad permanentemente. Cada año surgen nuevas herramientas y dispositivos que permiten construir sistemas más seguros.

Plan de contingencias

Elaborar un plan de contingencias, cuando algo no funciona o se producen fallos. Situaciones como:

Qué hacer cuando un computador tiene virus (Ransomware)

Qué hacer cuando ocurre un corte de luz o una baja de energía.

Qué hacer en caso de pérdida o robo.

Seguridad en la nube

Cuando se almacena información pueden ocurrir varios riesgos, para evitarlos adoptar un servicio de seguridad en la nube, pensando en lo catastrófico que puede llegar a ser la pérdida de información o datos.

2.-DERECHOS DIGITALES

2.1.-¿Qué son los derechos digitales?

Los derechos digitales se encuentran en la Declaración Universal de los Derechos Humanos de la ONU, aplicados al mundo online. Su objetivo fundamental es garantizar el acceso a internet, acortando la brecha digital y un adecuado uso de la red como un bien común perteneciente a la humanidad. (1). A continuación se presenta una guía de derechos digitales basados en el documento de la ONU y la Guía de Convivencia Digital de la Unicef (2), la que nos señala cuales son los derechos y deberes que poseen los alumnos y alumnas en materia de las Tics.

2.-2.- Guía de sensibilización sobre convivencia digital. Unicef (2)

Derecho al acceso a la información y la tecnología, sin discriminación por motivo de sexo, edad, recursos económicos, nacionalidad, etnia, lugar de residencia, etc.
Derecho a la libre expresión y asociación. Buscar, recibir y difundir informaciones e ideas de todo tipo por medio de la Red. Estos derechos solo podrán ser restringidos para garantizar: la protección de los niños y niñas de informaciones y materiales perjudiciales para su bienestar, desarrollo e integridad; y para el cumplimiento de las leyes, la seguridad, los derechos y la reputación de otras personas.
Derecho a la protección contra la explotación, el comercio ilegal, los abusos y la violencia de todo tipo que se produzcan utilizando Internet. Los niños y niñas tendrán el derecho de utilizar Internet para protegerse de esos abusos, para dar a conocer y defender sus derechos.
Derecho al desarrollo personal y a la educación, y a todas las oportunidades que las nuevas tecnologías como Internet puedan aportar para mejorar su formación. Los contenidos educativos dirigidos a niños y niñas deben promover su bienestar, desarrollar sus capacidades, inculcar el respeto a los derechos humanos y al medio ambiente y prepararlos para ser ciudadanos responsables en una sociedad libre
Derecho a la intimidad de las comunicaciones por medios electrónicos. Derecho a no proporcionar datos personales por la Red, a preservar su identidad y su imagen de posibles usos ilícitos.
Derecho al esparcimiento, al ocio, a la diversión y al juego, también mediante Internet y otras nuevas tecnologías. Para los niños**,** éstos no deben contener violencia gratuita, ni mensajes racistas, sexistas o denigrantes, y respeten los derechos y la imagen de los niños, niñas y otras personas.
Los padres y madres tendrán el derecho y la responsabilidad de orientar, educar y acordar con sus hijos e hijas un uso responsable de Internet: para ello los padres y madres también deben poder formarse en el uso de Internet e informarse de sus contenidos.

2.3.-DEBERES Y OBLIGACIONES

Todas las personas deben tomar medidas de seguridad en internet.

Se deben respetar las obligaciones de:

=Respetar la información y la privacidad de los demás

=Conocer tus derechos como el de los demás.

=Denunciar a los que violan tus derechos.

Reconocer y valorar la diversidad respetando los valores y creencias de los demás

Respetar la libertad de expresión

Respetar la propiedad intelectual

No discriminar ni agredir a los demás (ciberbuling, viralización de imágenes con contenidos inadecuados, etc)

Actuar con respeto ante los demás y no usar un lenguaje ofensivo y discriminatorio.

No hackear sistemas o redes.

No subir fakes news a internet o las redes.

No compartir archivos de manera ilegal.

No promover ni practicar la piratería.

Reportar el uso inapropiado de la tecnología.

No cometer robo de identidad en línea.

Cumplir las normas de comportamiento y leyes asociadas a los sitios web y redes que utilizas.

Tomar medidas de seguridad en los dispositivos personales, usando correctamente las contraseñas y antivirus.

No usar dispositivos de almacenamiento externo, como el pendrive que puede generar diversos daños en las redes y los dispositivos.

Emplear un servicio de seguridad en la nube, pensando en el daño que se produce con la pérdida de información o datos.

Aplicar estrategias de protección y seguridad en la información personal y la que recibes de otros.

II.-OBJETIVO GENERAL

Este protocolo tiene por finalidad educar a los alumnos y alumnas en el desarrollo de habilidades y actitudes que se desprenden del uso de estas herramientas tecnológicas que poseen las aulas tecnológicas del colegio, como; la responsabilidad, la seguridad digital, la participación, la libertad, la ética, conociendo sus deberes y derechos, de tal forma que se unan a esta nueva forma de interrelación que ofrece el ecosistema digital de forma autorregulada.

OBJETIVOS ESPECÍFICOS

1.- Formar a los alumnos y alumnas del colegio en el uso de las herramientas tecnológicos de acuerdo a los valores y actitudes que señala nuestro Proyecto Educativo.

2.- Conocer los derechos y deberes del ecosistema digital favoreciendo una actitud autorregulada.

3.- Promover en los alumnos y alumnas el uso de la seguridad digital para protegerse como personas y para utilizar dichas herramientas de forma segura.

4.- Abrir espacios de participación para los alumnos y alumnas buscando formar líderes en tecnología.

5.- Desarrollar planes de contingencia para cubrir eventos inesperados.

III.-METODOLOGÍA

Participación: En una metodología de participación es importante impulsar la libertad, la responsabilidad y una actitud de autorregulación en lo referido al uso seguro de las herramientas digitales. Se trabajará en la formación de grupos y actividades que promuevan la formación ciudadana digital.

Publicidad. Publicar documentos y otros fundamentalmente digitales, referidos a la seguridad digital y el comportamiento que se debe tener en las redes sociales.

Autorregulación. El aprendizaje en un ambiente virtual es mucho más eficiente mediante el aprendizaje autorregulado, pues hace que el estudiante genere pensamientos, sentimientos y acciones, que le permiten tener iniciativas, motivación y autonomía para los aprendizajes que se proponen. De esta manera esta propuesta implica que los alumnos generen sus propias ideas y las lleven a la práctica en colaboración con los monitores.

IV.-ACTIVIDADES

ACTIVIDADES	CRONOGRAMA	RESPOSABLE
Objetivo 1		
Diagnosticar: aplicar un cuestionario a alumnos y alumnas y profesores sobre seguridad digital.	Mayo	Clovis Gutiérrez
Objetivo 2		
Difundir a través de medios digitales los derechos y deberes de un ciudadano digital	Mayo	Equipo de Informática
Objetivo 3		
Difundir una revista con temas valóricos sobre la seguridad digital	Mayo	Yerko Alexis Guerra
Objetivo 4		
Formar grupos de alumnos y alumnas que participen de estas iniciativas; delegados de informática, ACLE de informática.	Abril	Equipo de Informática
Organizar torneo de video juegos.	Mayo (inicio)	Encargado Yero Alexis
Realizar un concurso de una mascota digital para el colegio.	Semana aniversario	Clovis Gutiérrez

Objetivo 5

Diseñar planes de emergencia, sobre : Qué hacer cuando un computador tiene virus (Ransomware) Qué hacer cuando ocurre un corte de luz o una baja de energía. Qué hacer en caso de pérdida o robo.	Mayo ANEXO I.	Rubén Fritz

EVALUACIÓN

Objetivo 1

Diagnosticar: aplicar un cuestionario a alumnos y alumnas y profesores sobre seguridad digital.	**Formulario y análisis de resultados**. Publicación de resultados.

Objetivo 2

Difundir a través de medios digitales los derechos y deberes de un ciudadano digital	**Documentos digitales publicados**

Objetivo 3

Difundir una revista con temas valóricos sobre la seguridad digital	**Revista digital diseñada y publicada**

Objetivo 4

Formar grupos de alumnos y alumnas que participen de estas iniciativas.	**Registros escritos y audiovisuales**

Objetivo 5

Diseñar planes de emergencia	**Planes diseñados y difundidos**

V.-DESTINATARIOS

Los destinatarios de este protocolo s la comunidad educativa del Colegio Inmaculada Concepción de Puerto Montt.

VI.-NORMATIVA

Letra A. DE LA RELACIÓN CON LOS DEMÁS

1.- Es deber de toda persona miembro del colegio respetar la información y la privacidad de los demás.

2.- Es deber de todo miembro de la comunidad educativa denunciar cualquier tipo de violación de tus derechos digitales.

3.- Siempre en toda situación debemos reconocer y valorar la diversidad respetando los valores y creencias de lo demás.

4.- Respetar la libertad de expresión, garantizando la protección de toda la comunidad educativa, en especial a los niños y niñas, de informaciones y materiales perjudiciales para su bienestar, desarrollo e integridad. Incluye también el cumplimiento de las leyes, la seguridad, los derechos y la reputación de otras personas.

5.- Está totalmente prohibido no discriminar, ni agredir a los demás, desde un punto de vista persona, social y cultural usando un lenguaje ofensivo; a través del ciberbuling, la viralización de imágenes con contenidos inadecuados etc.

6.- Respetar la propiedad intelectual. Todo producto de cualquier índole que no es de mi propiedad debo citar al propietario una vez que hago de uso de él en internet y en las redes sociales.

7.-Cuando los alumnos realizan trabajos recopilando la información, deben respetar la propiedad intelectual citando a los autores y la fuente de donde obtuvo la información (escribiendo la cita de acuerdo a la normativa vigente).

8.- Los alumnos y/o alumnas pueden emplear los equipos para otras actividades; por ejemplo; escuchar música, realizar reforzamientos, estudiar con otros compañeros etc. siendo el **delegado de informática** quien autorizará dando aviso a los encargados de informática.

Letra B.- DEL USO DE INTERNET

Un ciudadano digital debe mantener una actitud ética frente a todo lo que se produce en internet, las redes sociales y otras plataformas o herramientas. Todos los integrantes de la comunidad educativa deben actuar en consecuencia con el PEI:

1.- No debes hackear los sistemas o redes del colegio.
2.- No subir fakes news a internet o las redes sociales
3.- No promover ni practicar la piratería.
4.- No debes cometer robo de identidad en línea.
5.-Es obligación de todo integrante de la comunidad educativa reportar el uso inapropiado de la tecnología.

Letra C.- DE LA SEGURIDAD

Toda la comunidad educativa debe tomar medidas de seguridad ante el uso de internet.

1.-Todas las alumnas y todos los alumnos del colegio, tienen el deber de cuidar de los equipos instalados para la realización de las clases; computadores, televisores, equipos accesorios o periféricos. Ante cualquier peligro dar aviso de inmediato al delegado de informática, inspectoría o alguna persona del equipo de informática. Ante cualquier daño material producido en los equipos por negligencia, el curso debe hacerse cargo de su reparación o renovación

2.-Cuando un equipo del curso comienza a presentar fallas, el delegado de informática, dará aviso de inmediato al encargado de informática del colegio quien se hará responsable de buscar una solución.

3.- Aplicar estrategias de protección y seguridad a toda la información personal y la que recibes de otros.

4.-De la instalación de programas u otros. El soporte técnico o los encargados de informática evaluarán la instalación de programas u otro en los computadores, siendo ellos quienes tomen la decisión al respecto.

5.- Cumplir con las normas de comportamiento y leyes asociadas a los sitios web y redes que utilizas. Cada vez que aceptas estas indicaciones te obligas a respetarlas y asumirlas.

6.- Es muy importante tomar medidas de seguridad en los dispositivos personales, utilizando contraseñas seguras, además de antivirus.

7.- No usar dispositivos de almacenamiento externo, como el pendrive que puede generar diversos daños en las redes y dispositivos, como también pérdida de información Para evitar esto, emplear un servicio de seguridad en la nube. Por ejemplo, emplear el Google Drive que es una de las herramientas de Google que usa el colegio.

VII.- BIBLIOGRAFIA

1.-Para qué sirven los derechos digitales
https://www.ceupe.pe/blog/para-que-sirven-los-derechos-digitales.html

2.-Guia de sensibilización sobre convivencia digital
https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABRIL2017.pdf

3.- Infografía.Consejo de seguridad 360°. Entel Empresas.

ANEXO. I

Qué hacer cuando un computador tiene virus (Ransomware)

Cuando sospechas o te das cuenta que el computador tiene un virus, deténgase y haga lo siguiente, no intente intervenir:

1.- Apagar el equipo como corresponde.

2.- Una vez apagado desconecta el equipo de la corriente eléctrica.

3.- Desconecta también los equipos conectados al computador. Impresora, por ejemplo.

4.- Una vez realizada esta acción avisa al Encargado de Informática, ya sea de enseñanza básica o enseñanza media.

ESTE VIRUS PUEDE PRODUCIR MUCHO DAÑO A LOS EQUIPOS POR ESO ES MUY IMPORTANTE REALIZAR ESTA ACCIÓN COMPLETA.

¿Qué hacer cuando ocurre un corte de luz o una baja de energía?

1.- Apagar el equipo

2.- Desconectar el computador y el televisor de la corriente eléctrica.

3.- Desconecta todos los otros equipos conectados a la corriente eléctrica.

4.- Si el corte de energía es en la sala de clases, dar aviso de inmediato al encargado de informática.

5.- Si el corte de energía es generalizado espera a que llegue el encargado de informática a dar instrucciones.

AL DESCONECTAR LOS EQUIPOS DE LA ENERGÍA ELÉCTRICA SE PUEDE EVITAR EL DAÑO QUE SE PUEDE PRODUCIR POR LA ALTERACION DE ENERGÍA QUE RECIBEN.

¿Qué hacer en caso de pérdida o robo?

Cuando un equipo no está en su lugar, se ha perdido o sospecha de un robo:

Dar aviso de inmediato al encargado de informática.