FUNDACIÓN ECOS
Educación para Comunidades Sostenibles

COMPENDIO DE CONTENIDOS ESENCIALES SOBRE ACCESO Y USO DE LA INFORMACIÓN Y ELABORACIÓN DE TECNOLOGÍAS PROPIAS

Créditos

CONTENIDOS

Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL)

Fundación Charles Darwin (FCD)

Galápagos Hub para la Sostenibilidad, Innovación y Resiliencia(GAHUB)

REVISIÓN DE TEXTOS

Oscar Jaya

Johny Mazón

Fernanda Loayza

Joyce Robalino

Ana María Loose

Martín Narváez

Miriam Chacón

COORDINACIÓN GENERAL

Fundación Educación para Comunidades Sostenibles (ECOS)

©ECOS, 2023

La reproducción parcial o total de esta publicación, en cualquier forma y por cualquier medio mecánico o electrónico, está permitida siempre y cuando sea autorizada por los editores y se cite correctamente la fuente.

DISTRIBUCIÓN GRATUITA

Para citar este documento:

Fundación Educación para Comunidades Sostenibles (2023). “Compendio de Contenidos Esenciales sobre “Acceso y Uso Consciente de la Información y Elaboración de Tecnologías Propias”. Puerto Ayora, Galápagos.

TABLA DE CONTENIDOS

Introducción a la Seguridad de la Información

¿Qué es la información?

La información se refiere a los datos organizados y procesados que tienen algún significado o utilidad para las personas. Es el resultado del procesamiento y análisis de datos, lo que les da contexto, relevancia y sentido. La información puede ser representada en diferentes formas, como texto, números, gráficos, imágenes, sonidos, entre otros medios.

La información es fundamental en todas las áreas de la vida, desde la comunicación y el aprendizaje hasta la toma de decisiones y la realización de actividades cotidianas. Es un recurso valioso que proporciona conocimiento, permite la comprensión de situaciones y fenómenos, y facilita la transmisión de ideas y conceptos.

En el entorno digital, la información adquiere un papel aún más relevante debido a la facilidad de acceso, almacenamiento y distribución que ofrecen las tecnologías de la información y la comunicación. La era digital ha dado lugar a una explosión de información, con vastas cantidades de datos disponibles en línea y en diversas bases de datos.

La calidad de la información se basa en su precisión, relevancia, actualidad y confiabilidad. La veracidad y la exactitud de la información son aspectos fundamentales para tomar decisiones informadas y evitar la propagación de información falsa o engañosa.

¿Qué es la seguridad de la información?

La seguridad de la información se refiere a la protección de la información contra accesos no autorizados, divulgación, alteración, destrucción o cualquier otro tipo de incidente que pueda comprometer su confidencialidad, integridad o disponibilidad. Consiste en la implementación de medidas y controles técnicos, organizativos y legales para salvaguardar la información, ya sea almacenada electrónicamente o en formatos físicos, de manera que solo las personas autorizadas tengan acceso a ella y se mantenga protegida de posibles amenazas y riesgos.

La seguridad de la información se ocupa de proteger la información en todas sus formas, ya sean datos personales, secretos comerciales, información financiera, propiedad intelectual o cualquier otro tipo de información sensible y valiosa. Esto implica la adopción de políticas de seguridad, el establecimiento de procedimientos y directrices, la implementación de tecnologías de seguridad, la capacitación de personal y la concienciación sobre las buenas prácticas en cuanto al manejo y protección de la información.

Aspectos relevantes

a. La seguridad de la información asegura que solo las personas autorizadas tendrán acceso a la información confidencial de una persona u organización, evitando así fugas de información o filtraciones.
b. La seguridad de la información protege la integridad de los datos, impidiendo su alteración, modificación o eliminación no autorizada. Esto garantiza que la información sea precisa y confiable.
c. La seguridad de la información asegura que la información esté disponible para las personas autorizadas cuando la necesiten.
d. En la actualidad, los ciberataques son una amenaza constante. La seguridad de la información ayuda a prevenir y reducir los efectos de estos ataques, protegiendo los sistemas, la información y los activos de una organización.

Importancia de la seguridad de la información en la era digital

En la era digital, los ciberataques son una amenaza constante. La seguridad de la información en la era digital es esencial para proteger la privacidad, prevenir el fraude, garantizar la confidencialidad empresarial, mitigar las amenazas cibernéticas, cumplir con las regulaciones y garantizar la continuidad del negocio. Es fundamental para mantener la confianza de los usuarios, clientes y socios en un entorno digital cada vez más conectado y dependiente de la tecnología.

La protección de la privacidad en línea es de suma importancia en la era digital por las siguientes razones:

a. **Protección de datos personales:** Cuando compartimos información en línea, ya sea en redes sociales, formularios de registro o compras en línea, estamos revelando datos personales sensibles. Proteger nuestra privacidad nos ayuda a evitar que esta información caiga en manos equivocadas y se utilice de manera fraudulenta o perjudicial.
b. **Prevención del robo de identidad:** La falta de privacidad en línea puede conducir al robo de identidad. Los ciberdelincuentes pueden recopilar información personal para realizar actividades ilegales en nuestro nombre, como solicitar crédito, abrir cuentas bancarias o cometer fraudes financieros. Proteger nuestra privacidad ayuda a prevenir estos casos y a salvar nuestra identidad.
c. **Evitar el acoso y el ciberacoso:** La falta de privacidad en línea puede exponernos a acosadores y ciberacosadores. Mantener nuestra información personal y nuestras actividades en línea protegidas nos ayuda a reducir el riesgo de ser objeto de acoso, intimidación o acecho en línea.

d. **Preservar la reputación en línea**: La privacidad en línea juega un papel crucial en la pérdida de nuestra reputación. La información que compartimos en línea puede tener un impacto duradero en cómo nos perciben los demás. Proteger nuestra privacidad nos permite tener un mayor control sobre la imagen que proyectamos y evitar situaciones embarazosas o perjudiciales en el futuro.
e. **Control sobre la información personal:** La protección de la privacidad en línea nos brinda mayor control sobre nuestra información personal. Nos permite decidir qué información compartimos, con quién la compartimos y cómo se utiliza. Esto nos empodera y nos ayuda a proteger nuestra privacidad y dignidad en el mundo digital.
f. **Salvaguardar la confidencialidad profesional:** Para aquellos que trabajan en entornos profesionales, la privacidad en línea es esencial para proteger la confidencialidad de la información sensible relacionada con el trabajo.

¿Qué son los datos personales?

Los datos personales son cualquier información que identifique o pueda utilizarse para identificar a una persona específica. Estos datos pueden ser recopilados, almacenados, procesados y utilizados por organizaciones o individuos para diversos fines.

Es importante destacar que los datos personales pueden ser sensibles o no sensibles. Los datos personales sensibles son aquellos que revelan información especialmente protegida, como origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, orientación sexual, datos biométricos o de salud. Estos datos suelen estar sujetos a mayores regulaciones y protecciones debido a su naturaleza más delicada, donde su divulgación o utilización indebida puede causar daño a la seguridad o integridad de una persona.

En muchos países, existen leyes y regulaciones específicas que protegen los datos personales y establecen principios y requisitos para su tratamiento adecuado y seguro. Estas leyes varían en cada jurisdicción, pero su objetivo principal es garantizar que los datos personales sean utilizados de manera ética y protegidos de acceso no autorizado o uso indebido.

Algunos ejemplos de información personal sensible incluyen:

a. **Información de identificación personal:** Nombre completo, número de identificación nacional, número de seguridad social, pasaporte, licencia de conducir, etc.
b. **Datos de contacto:** Número de teléfono, direcciones postales, direcciones de correo, electrónico u otra información que permita comunicarse con la persona.
c. **Información financiera:** Números de cuenta bancaria, tarjetas de crédito o débito, historial crediticio, números de seguridad de tarjetas, información de transacciones financieras, etc.

d. **Datos biométricos:** Huellas dactilares, reconocimiento facial, voz, escaneos de retina, información genética, etc.
e. **Información de salud:** Historial médico, condiciones médicas, registros de tratamiento, información de medicamentos, resultados de pruebas médicas, etc.
f. **Datos de ubicación:** Información que revela la ubicación geográfica en tiempo real o histórica de una persona, como la dirección de residencia, el historial de ubicaciones compartidas en aplicaciones de navegación o redes sociales, etc.
g. **Información confidencial del trabajo:** Información relacionada con el empleo, como datos de nómina, registros de desempeño, contratos laborales, información de contacto profesional, etc.
h. **Información personal de menores:** Datos personales de niños y adolescentes, incluidos nombres, fechas de nacimiento, información escolar o actividades extracurriculares, etc.

En general, cualquier dato que pueda utilizarse para identificar o comprometer la privacidad de una persona se considera información personal sensible y debe ser tratada con cuidado y protegida adecuadamente.

Actividades sugeridas con estudiantes:

Genera un debate en el aula sobre los siguientes temas:

- ☐ ¿Para qué usamos internet en la actualidad?
- ☐ ¿Cuánto tiempo estamos en internet diariamente?
- ☐ ¿Qué tipo de aplicaciones o paginas son las que más usan los estudiantes?
- ☐ ¿Qué información comparten los estudiantes en redes sociales?
- ☐ ¿Qué tipo de información se considera sensible?
- ☐ ¿Qué información personal compartimos en internet?
- ☐ ¿Cuánto tiempo estamos en internet?
- ☐ La ética en el manejo de la información.
- ☐ ¿La evolución de la tecnología es siempre positiva?
- ☐ ¿Qué información puede compartirse en redes y cuál no para mantener la seguridad y privacidad?
- ☐ La presión social en las redes.

Amenazas en el uso de internet y redes sociales

¿Qué son las redes sociales?

En la era digital, el uso de Internet y las redes sociales ha transformado la forma en que nos comunicamos, obtenemos información y nos relacionamos con los demás. Las redes sociales son plataformas en línea que permiten a las personas conectarse y compartir contenido digital con otras personas. Estas plataformas facilitan la interacción social y la comunicación a través de internet, permitiendo a los usuarios crear perfiles, compartir información, publicar mensajes, fotos, videos y participar en diversas actividades sociales en línea. Sin embargo, junto con los beneficios, también surgen diversas amenazas y riesgos asociados. Es importante estar consciente de estas amenazas para poder navegar por el mundo digital de manera segura y protegida.

Algunas de las redes sociales más populares en la actualidad incluyen Facebook, Twitter, Instagram, LinkedIn, Snapchat y TikTok, entre muchas otras. Cada una de estas redes sociales tiene sus propias características y enfoques particulares, pero comparten el objetivo común de facilitar la interacción y la comunicación entre las personas en línea.

Es importante tener en cuenta que el uso de redes sociales también implica consideraciones de privacidad y seguridad, ya que la información compartida en estas plataformas puede ser accesible para otros usuarios y, en algunos casos, para terceros. Por lo tanto, es fundamental tomar precauciones y ajustar las configuraciones de privacidad según las preferencias individuales.

Tipos de amenazas

Las amenazas en el uso de Internet y redes sociales son variadas y evolucionan constantemente. Desde el robo de identidad y el fraude en línea hasta el ciberacoso y la difusión de contenido malicioso, estas amenazas pueden tener consecuencias graves tanto a nivel personal como a nivel de seguridad digital. Algunas amenazas incluyen:

a. **Ciberacoso**: Los niños y jóvenes pueden ser víctimas de acoso, intimidación o insultos en las redes sociales, lo que puede tener un impacto emocional y psicológico negativo en ellos.
b. **Suplantación de identidad:** Existe el riesgo de que alguien pueda crear un perfil falso y hacerse pasar por otra persona, lo que puede llevar a situaciones de engaño o manipulación, extorsión y estafas.
c. **Compartir información personal:** Los niños y jóvenes pueden ser propensos a compartir información personal en las redes sociales, como su dirección, número de teléfono o detalles de su vida diaria, lo que puede ponerlos en riesgo de ser víctimas de abuso, acecho, secuestro, robos.

d. **Contenido inapropiado:** En las redes sociales, los niños y jóvenes pueden encontrarse con contenido inapropiado, como imágenes violentas, pornografía o lenguaje ofensivo, lo que puede afectar su bienestar emocional y desarrollo.
e. **Adicción y tiempo excesivo en línea:** El uso excesivo de las redes sociales puede llevar a la adicción y al aislamiento social, lo que puede interferir con el rendimiento académico y las relaciones personales.
f. **Exposición a estafas y engaños:** Los niños y jóvenes y adultos pueden ser víctimas de estafas en línea, como promociones falsas o solicitudes de dinero.
g. **Problemas de autoestima y comparación social:** Las redes sociales contribuyen a problemas de autoestima en niños y jóvenes, ya que constantemente se comparan con los demás y se sienten presionados por encajar en ciertos estándares de belleza o éxito.
h. **Riesgo de compartir contenido inapropiado:** Los niños y jóvenes pueden verse tentados a compartir imágenes o mensajes inapropiados, lo que puede tener consecuencias graves, como el ciberacoso o el daño a su reputación.
i. **Pérdida de privacidad:** La falta de comprensión sobre la privacidad en las redes sociales puede llevar a los niños y jóvenes a compartir información sensible con un público más amplio de lo que desean, lo que puede tener repercusiones negativas a largo plazo.

Es esencial que los padres, educadores y cuidadores estén al tanto de estos peligros y trabajen en conjunto para educar a los niños y jóvenes sobre el uso seguro y responsable de las redes sociales. También es importante establecer reglas y límites claros para proteger su bienestar en línea.

Otro tipo de amenazas

Grooming

El grooming es una práctica en línea en la que un adulto establece una relación con un niño o adolescente a través de Internet, con el objetivo de ganar su confianza y eventualmente abusar sexualmente de ellos. Los groomers suelen utilizar manipuladoras tácticas, como el establecimiento de una amistad falsa, la creación de perfiles falsos o la utilización de información personal compartida por el menor, para construir una relación de confianza. Comúnmente son adultos que se hacen pasar por niños o adolescentes.

El grooming puede ocurrir en diferentes plataformas en línea, como redes sociales, salas de chat, aplicaciones de mensajería y juegos en línea.

Al protagonista del grooming se lo denomina groomer y tiene como objetivo final persuadir al menor para que participe en actividades sexuales o envíe imágenes o videos de contenido

sexual. El grooming es una forma de abuso sexual en línea y puede tener graves consecuencias para las víctimas, incluyendo daño emocional, trauma y violencia sexual.

Cómo evitar ser víctima de Grooming:

1. Privacidad y configuración de seguridad: Asegúrese de que los perfiles de las redes sociales de los niños y adolescentes tengan configuraciones de privacidad adecuadas. Limita el acceso a la información personal y las publicaciones solo a amigos de confianza.
2. Evita aceptar a personas desconocidas en redes sociales.
3. Evitar chatear con desconocidos.
4. No entables relaciones de confianza con personas que interactúas en juegos en línea.
5. Jamás envíes imágenes personales a desconocidos, ni las compartas por internet.

Sexting

El sexting es el acto de enviar, recibir o compartir contenido sexualmente explícito, como mensajes, imágenes o videos, a través de dispositivos electrónicos, especialmente teléfonos móviles o redes sociales. El término "sexting" es una combinación de las palabras "sexo" y "texting" (envío de mensajes de texto en inglés).

Riesgos asociados con el sexting:

a. **Difusión no consensuada:** Existe el riesgo de que las imágenes o videos enviados como sexting se compartan sin el consentimiento de la persona que los envió, lo que puede resultar en una pérdida de control sobre su privacidad y la difusión no deseada de contenido íntimo.
b. **Exposición pública:** El contenido de sexting puede ser compartido en línea, lo que puede llevar a que se vuelva viral y se difunda enormemente. Esto puede tener graves consecuencias para la reputación y la imagen personal de la persona involucrada.
c. **Ciberacoso y bullying:** Las imágenes o vídeos de sexting pueden ser utilizadas como herramientas para acosar, chantajear o intimidar a la persona que los envió. Esto puede llevar a daños emocionales, psicológicos y sociales significativos.
d. **Consecuencias legales:** En muchos lugares, el sexting entre menores de edad se considera ilegal, ya que puede constituir la producción, posesión o distribución de material pornográfico infantil. Esto puede tener graves consecuencias legales y penales para las personas involucradas.
e. **Pérdida de control sobre la privacidad:** Al enviar contenido de sexting, se pierde el control sobre quién puede acceder a él y cómo puede ser utilizado. Esto puede dar lugar a una violación de la privacidad y la exposición no deseada de la intimidad.

f. **Daño emocional y psicológico:** El sexting puede tener un impacto emocional y psicológico negativo en las personas involucradas. Sentimientos de vergüenza, culpa, ansiedad y depresión pueden surgir como resultado de la difusión no consensuada o la amenaza de difusión.
g. **Riesgo de extorsión:** Las imágenes o vídeos de sexting pueden ser utilizados como medio de extorsión, donde la persona que los tiene intenta obtener beneficios o favores sexuales bajo la amenaza de difundir el contenido.
h. **Riesgos de seguridad en línea:** Al enviar imágenes o vídeos de sexting, se corre el riesgo de que los dispositivos electrónicos o las cuentas en línea sean hackeados, lo que podría permitir que terceros accedan a contenido íntimo y lo utilicen de manera inapropiada.

Es importante tener en cuenta estos riesgos al considerar el sexting y promover una educación integral sobre el consentimiento, la privacidad y las consecuencias asociadas. Es fundamental fomentar un ambiente de confianza y comunicación abierta donde los jóvenes puedan buscar apoyo y orientación en caso de enfrentar situaciones relacionadas con el sexting.

Phishing

El phishing es un término utilizado para describir una técnica de ciberataque en la que los estafadores intentan engañar a las personas para que revelen información personal confidencial, como contraseñas, números de tarjetas de crédito o datos bancarios. El objetivo del phishing es obtener acceso no autorizado a cuentas o información sensible.

Los estafadores de phishing suelen utilizar métodos como el envío de correos electrónicos o mensajes de texto falsos que parecen provenir de instituciones legítimas, como bancos, empresas o plataformas en línea populares. Estos mensajes falsos suelen solicitar a los destinatarios que proporcionen información confidencial o que hagan clic en enlaces maliciosos que redirigen a sitios web falsos diseñados para robar datos personales.

El phishing puede ser altamente sofisticado y convincente. Los estafadores pueden utilizar tácticas como el uso de logotipos y diseños similares a los de empresas legítimas, el uso de lenguaje persuasivo o urgente para incitar a las personas a actuar rápidamente y la creación de sitios web falsos que imitan perfectamente los originales.

Es importante estar atento al phishing y tomar medidas para protegerse. Algunas recomendaciones incluyen:

a. **Desconfiar de mensajes no solicitados:** No confíes en mensajes de correo electrónico, mensajes de texto o llamadas telefónicas no solicitadas que pidan información personal o financiera.

b. **Verificar la autenticidad:** Si recibe un mensaje sospechoso que parece provenir de una empresa o institución, verifique su autenticidad antes de proporcionar información sensible. Puedes hacerlo contactando directamente a la empresa a través de un canal de comunicación oficial.
c. **No hacer clic en enlaces sospechosos:** Evita hacer clic en enlaces incluidos en mensajes sospechosos. En su lugar, visite el sitio web oficial de la empresa o institución directamente a través de su navegador.
d. **Revise cuidadosamente la URL:** Antes de ingresar información en un sitio web, asegúrese de que la URL sea legítima y esté correctamente escrita. Los estafadores a menudo crean sitios web con URL similares pero ligeramente diferentes a las de las empresas reales.
e. **Mantener software actualizado:** Mantén tu sistema operativo, navegador y programas de seguridad actualizados para que te ayuden a protegerte contra técnicas de phishing conocidas.

Aspectos relevantes para identificar si un correo es falso:

a. **Verificación del remitente:** Examine cuidadosamente la dirección de correo electrónico del remitente. Los correos electrónicos falsos a menudo utilizan direcciones similares pero ligeramente diferentes a las empresas o instituciones legítimas. Presta atención a errores ortográficos o caracteres adicionales en el dominio.
b. **Solicitudes de información personal:** Ten precaución si el correo electrónico solicita información personal confidencial, como contraseñas, números de tarjetas de crédito o datos de seguridad social. Las entidades legítimas generalmente no solicitan este tipo de información a través del correo electrónico.
c. **Errores gramaticales y ortográficos:** Presta atención a los errores gramaticales o de ortografía en el correo electrónico. Los correos electrónicos legítimos suelen ser revisados y editados con atención, mientras que los correos falsos pueden contener errores evidentes.
d. **Urgencia o amenazas:** Ten cuidado si el correo electrónico te insta a tomar medidas urgentes o contiene amenazas de consecuencias negativas si no actúa de inmediato. Los estafadores a menudo utilizan estas tácticas para presionar a las personas a revelar información personal o realizar acciones no deseadas.
e. **Enlaces y archivos adjuntos sospechosos:** Evite hacer clic en enlaces o descargar archivos adjuntos en correos electrónicos sospechosos. Puede contener malware o dirigirte a sitios web falsos diseñados para robar tus datos. Siempre verifique la autenticidad del correo electrónico antes de interactuar con los enlaces o archivos adjuntos.

Recuerda que es importante mantenerse vigilante y confiar en tu instinto. Si algo parece sospechoso o no te sientes cómodo con un correo electrónico, es mejor no responder ni

tomar ninguna acción hasta que puedas verificar su autenticidad. Siempre es recomendable contactar directamente a la empresa o institución a través de canales oficiales para confirmar la legitimidad del correo electrónico. Ejemplo de un correo falso.

<u>Aspectos relevantes para identificar una página web falsa:</u>

a. **URL sospechosa:** Observa la dirección URL de la página web. Las páginas web falsas a menudo utilizan URL que parecen similares a las de sitios web legítimos, pero con pequeñas diferencias o errores ortográficos. Verifique cuidadosamente el dominio y asegúrese de que coincida con la página web oficial.
b. **Diseño y contenido de baja calidad:** Las páginas web falsas suelen tener un diseño deficiente, con imágenes de baja calidad, errores de diseño y falta de coherencia en

la presentación de contenido. Presta atención a los errores gramaticales, ortográficos o de traducción, ya que son indicadores de una página web poco confiable.

c. **Falta de información de contacto y política de privacidad:** Las páginas web legítimas suelen proporcionar información de contacto clara, como dirección física, número de teléfono y dirección de correo electrónico. Además, suelen tener una política de privacidad que explica cómo se manejan los datos personales. Si una página web no ofrece esta información o su política de privacidad es vaga o inexistente, puede ser sospechosa.
d. **Certificado SSL ausente:** Verifica si la página web utiliza un certificado SSL (Secure Sockets Layer) para cifrar la comunicación y proteger los datos del usuario. Un candado cerrado o el uso de "https://" en la URL indica que la página web es segura. Si no ves ninguna de estas señales, es mejor no proporcionar información personal en ese sitio web.
e. **Ofertas demasiado buenas para ser verdad:** Si una página web ofrece productos o servicios a precios significativamente más bajos que otras tiendas en línea, es probable que sea sospechosa. Las páginas web falsas a menudo intentan atraer a los usuarios con ofertas irresistibles para estafarlos. Investigue y compare precios en varias fuentes antes de realizar una compra en línea.

Recuerda que es importante ser cauteloso al navegar por Internet y verificar cuidadosamente la autenticidad de las páginas web antes de proporcionar información personal o realizar transacciones. Siempre utilice fuentes confiables y asegúrese de proteger sus datos personales en línea.

Ejemplo pagina web real:

La educación y la precaución son fundamentales para protegerte contra el phishing. Mantente alerta y desconfía de cualquier solicitud de información personal o financiera que parezca sospechosa.

Ciberbullying o Ciberacoso

El ciberbullying o ciberacoso se refiere al uso de tecnologías digitales, como teléfonos móviles, redes sociales, aplicaciones de mensajería y sitios web, para acosar, intimidar, amenazar o humillar a alguien. A diferencia del acoso tradicional, el ciberacoso se lleva a cabo a través de plataformas en línea y se caracteriza por la facilidad de difusión y el anonimato que ofrecen estas tecnologías.

El ciberacoso puede manifestarse de varias formas, incluyendo:

a. Insultos y comentarios ofensivos en publicaciones, comentarios o mensajes privados.
b. Difusión de rumores o información falsa sobre alguien para dañar su reputación.
c. Suplantación de identidad, creación de perfiles falsos para acosar o engañar a otros.
d. Exclusión y aislamiento deliberado, impidiendo que alguien participe en actividades en línea o en grupos.
e. Envío masivo de mensajes negativos o amenazantes a través de múltiples plataformas.
f. Publicación y difusión de imágenes o videos humillantes o comprometedores sin consentimiento.
g. Acoso sexual, incluyendo el envío no deseado de contenido sexual o solicitudes inapropiadas.
h. Creación de memes o contenido gráfico ofensivo dirigido a alguien en particular.
i. Hostigamiento constante a través de mensajes o comentarios repetitivos y perturbadores.

El ciberacoso puede tener graves consecuencias para la salud emocional y mental de las personas afectadas. Puede causar ansiedad, depresión, baja autoestima, aislamiento social e incluso llevar pensamientos suicidas o deserción escolar.

Es importante tomar medidas para prevenir y combatir el ciberacoso. Algunas recomendaciones incluyen:

a. Mantener la información de privacidad y seguridad en línea, configurando adecuadamente las opciones de privacidad en las redes sociales y evitando compartir información personal con personas desconocidas.
b. No responder ni participar en provocaciones o mensajes ofensivos.
c. Bloquear o denunciar a los acosadores en las plataformas en línea.

d. Guardar evidencia del acoso, como capturas de pantalla o copias de mensajes, para respaldar cualquier informe o denuncia.
e. Buscar apoyo de adultos de confianza, como padres, profesores o consejeros escolares, y comunicarles lo que está sucediendo.
f. Promover una cultura de respeto y empatía en línea- Fomentar comportamientos positivos y solidarios.
g. Fomentar la comunicación abierta y el diálogo con los niños y adolescentes para que se sientan cómodos compartiendo sus experiencias en línea.
h. Promover la conciencia y empatía hacia las víctimas del ciberacoso, mostrando apoyo y solidaridad.

Actividades sugeridas con estudiantes:

- ☐ Genera un debate en el aula usando material audiovisual sobre grooming, Sexting, Ciberbullying, Phishing. Principio del formulario

https://www.youtube.com/watch?v=21uGsQYMr2Q

https://www.youtube.com/watch?v=Ds3GP7ypzes

https://www.youtube.com/watch?v=HENLc45X0lc

https://www.youtube.com/watch?v=OdixH25nCHk

https://www.youtube.com/watch?v=Pa2ttVRA-xU

https://www.youtube.com/watch?v=tch4ShnGwd0

https://www.youtube.com/watch?v=pAohWiuNPYo

https://www.youtube.com/watch?v=kxpEb6xtg0o

https://www.youtube.com/watch?v=tw9NyDkt0Oc

https://www.youtube.com/watch?v=Esde5ek_Yao

- ☐ Genera grupos de trabajo en el aula, solicitar a los estudiantes hacer representación de un escenario de ciberbullying en el ambiente escolar, y un escenario de grooming.
- ☐ Forma grupo de trabajo con el objetivo que cada grupo realice un video de toma de conciencia para evitar el ciberbullying en el ambiente escolar y evitar las amenazas en el uso de internet y redes sociales.

Medidas de Seguridad

Contraseñas seguras

Las contraseñas seguras son una parte fundamental de la protección de nuestras cuentas en línea y de mantener nuestra información personal a salvo de posibles amenazas cibernéticas. En un mundo digital cada vez más interconectado, donde almacenamos y compartimos una gran cantidad de información confidencial, es crucial entender la importancia de crear contraseñas sólidas y únicas para cada una de nuestras cuentas.

Una contraseña segura es aquella que es difícil de adivinar o descifrar, incluso para aquellos que intentan acceder ilegalmente a nuestras cuentas. Una contraseña fuerte debe combinar una combinación de letras (mayúsculas y minúsculas), números, caracteres especiales.

El uso de contraseñas seguras es esencial porque muchas veces los ciberdelincuentes utilizan programas automatizados que prueban diferentes combinaciones de contraseñas hasta encontrar la correcta. Si nuestras contraseñas son débiles o fáciles de adivinar, aumentamos el riesgo de que nuestras cuentas estén comprometidas y nuestra información personal o financiera caiga en manos equivocadas.

Consejos para crear una contraseña segura

a. **Longitud:** Utiliza contraseñas que tengan al menos 8 caracteres como mínimo. Cuanto más larga sea la contraseña, mayor será la dificultad para que sea adivinada o descifrada.
b. **Complejidad:** Combina letras (mayúsculas y minúsculas), números y caracteres especiales (como !, @, #, $, %, etc.) en tus contraseñas. La inclusión de diferentes tipos de caracteres aumenta la complejidad y la seguridad de la contraseña.
c. **Evita información personal:** Evita utilizar información personal fácilmente deducible o relacionada contigo, como tu nombre, fecha de nacimiento, nombres de familiares, números de teléfono, etc. Los atacantes pueden utilizar esta información para adivinar tu contraseña.
d. **Evita secuencias y patrones obvios:** Evita el uso de secuencias numéricas o letras consecutivas en tus contraseñas, como "12345678" o "qwerty". Estas secuencias son fáciles de adivinar.
e. **Evita palabras del diccionario:** Evita utilizar palabras comunes o palabras del diccionario como contraseñas. Los atacantes pueden utilizar diccionarios y programas automatizados para probar combinaciones de palabras y adivinar contraseñas más fácilmente.

f. **No reutilices contraseñas:** Es importante utilizar contraseñas únicas para cada cuenta. Si reutilizas la misma contraseña en múltiples plataformas, un solo fallo de seguridad podría dañar todas tus cuentas.
g. **Cambia tus contraseñas periódicas:** Es recomendable cambiar tus contraseñas de forma periódica, al menos cada 3-6 meses. Esto ayuda a reducir el riesgo en caso de que una contraseña se vea comprometida.
h. **Activa la autenticación de dos factores:** Donde esté disponible, habilita la autenticación de dos factores. Esta capa adicional de seguridad exige un segundo factor de autenticación, como un código enviado a su teléfono móvil, para acceder a su cuenta.

Recuerda que generar contraseñas seguras es fundamental para proteger tus cuentas y mantener tu información personal a salvo. Tómate el tiempo necesario para crear contraseñas únicas y sigue las mejores prácticas de seguridad en todo momento.

Actualización de software y antivirus

La actualización de software y antivirus es importante por varias razones:

a. **Parches de seguridad:** Las actualizaciones de software y antivirus suelen incluir parches y correcciones para vulnerabilidades conocidas. Estas vulnerabilidades podrían ser aprovechadas por hackers o ciberdelincuentes para acceder a su sistema o infectar con malware. Al mantener tu software y antivirus actualizados, te aseguras de tener la protección más reciente contra las amenazas conocidas.
b. **Protección contra nuevas amenazas:** Los desarrolladores de software y proveedores de antivirus están constantemente investigando y monitoreando nuevas amenazas y técnicas de ataque. Al mantener tu software actualizado, te aseguras de recibir las últimas defensas y capacidades de detección contra las amenazas emergentes.
c. **Protección de datos y privacidad:** Las actualizaciones de software y antivirus a menudo incluyen mejoras en la protección de datos y privacidad. Estas actualizaciones pueden fortalecer los mecanismos de cifrado, agregar funciones de protección de identidad y proporcionar controles de privacidad más robustos. Mantenga su software actualizado te ayuda a proteger tus datos personales y a mantener tu privacidad en línea.

En resumen, la actualización regular de software y antivirus es esencial para mantener tu sistema protegido contra las últimas amenazas, asegurar el rendimiento y la estabilidad, garantizar la compatibilidad y proteger tus datos y privacidad. Recuerda habilitar las actualizaciones automáticas y estar atento a las notificaciones de actualización para mantener tu sistema seguro y protegido.

Actividades sugeridas con estudiantes:

- ☐ Proporciona a los estudiantes una lista de contraseñas y pídeles que las evalúen en términos de fortaleza. Discuta con ellos los diferentes aspectos de una contraseña segura, como su longitud, complejidad.
- ☐ Realiza un juego de roles en el que los estudiantes asuman el papel de "atacantes" y traten de "romper" las contraseñas creadas por otros estudiantes. Esto ayudará a los estudiantes a comprender la importancia de las contraseñas seguras y las vulnerabilidades que pueden existir en las contraseñas débiles.
- ☐ Proporciona a los estudiantes diferentes escenarios y pídeles que generen contraseñas seguras adecuadas para cada situación. Por ejemplo, pueden crear contraseñas seguras para cuentas de redes sociales, correo electrónico o servicios en línea.
- ☐ Pídeles a los estudiantes identificar si los computadores que usan en casa poseen antivirus, que sistema operativo usan y si estos están actualizados.

Uso responsable de la información y datos personales

El uso responsable de la información y los datos personales implica tratar la información obtenida de otros individuos o fuentes en línea de manera ética y consciente. Se refiere a respetar los derechos y la privacidad de las personas, así como asumir las responsabilidades asociadas con el uso de esa información. Algunos aspectos clave del uso responsable de la información y los datos personales incluyen obtener el consentimiento informado antes de recopilar, utilizar o compartir datos personales, proteger la privacidad de las personas, utilizar la información y los datos sólo para los fines específicos acordados, mantener la información precisa y actualizada, compartir la información de manera segura y con las personas autorizadas, y estar consciente de los riesgos y amenazas en línea para tomar medidas de seguridad adecuadas. Al ser responsables en el manejo de la información, contribuimos a construir un entorno digital más seguro y confiable para todos.La seguridad en las redes sociales es de vital importancia en la actualidad debido a la creciente influencia de estas plataformas en nuestra vida diaria. Las redes sociales nos permiten conectarnos, compartir contenido, interactuar con otros y mantenernos informados, pero también nos exponen a diversos riesgos y amenazas.

Competencias clave en la era digital

En esta era digital, hay varias competencias clave que una persona debe tener al usar y elegir información. Estas competencias ayudan a navegar eficazmente en el entorno digital, evaluar la calidad de la información y tomar decisiones informadas. Algunas de estas competencias clave son:

1. **Pensamiento crítico:** El pensamiento crítico es esencial al utilizar y elegir información en línea. Implica tener una actitud analítica y cuestionadora hacia la información, evaluarla de manera objetiva y considerar múltiples perspectivas antes de llegar a conclusiones. El pensamiento crítico ayuda a discernir entre información confiable y engañosa, y a tomar decisiones fundamentadas.
2. **Identificación de fuentes confiables y verificables:** En la era digital, es crucial poder discernir entre fuentes confiables y aquellas que pueden proporcionar información incorrecta o engañosa. La competencia en la identificación de fuentes confiables implica evaluar la reputación, la autoridad y la credibilidad de las fuentes de información antes de considerarlas como fuentes válidas. Esto implica verificar la fuente, buscar evidencia de respaldo, considerar la objetividad y tener en cuenta el contexto en el que se presenta la información.
3. **Evaluación de la calidad y relevancia de la información:** No toda la información disponible en línea es de alta calidad o relevante para nuestras necesidades. La competencia en la evaluación de la calidad y relevancia de la información implica analizar y valorar críticamente la información que se encuentra, considerando su

pertinencia, objetividad, actualidad, fundamentos científicos o académicos y otros criterios relevantes. Esto nos ayuda a utilizar información precisa y confiable en nuestras decisiones, trabajos académicos o actividades diarias.

4. **Comunicación efectiva y respetuosa en línea:** La comunicación en línea es una parte integral de nuestra vida digital. La competencia en la comunicación efectiva y respetuosa en línea implica desarrollar habilidades para expresarse de manera clara, comprensible y respetuosa en los diversos entornos digitales, como redes sociales, foros de discusión o correos electrónicos. Esto implica la capacidad de transmitir mensajes de manera efectiva, respetar las opiniones de los demás, evitar el lenguaje ofensivo y promover una comunicación constructiva.
5. **Protección de datos personales y privacidad:** En la era digital, la protección de los datos personales es esencial. La competencia en la protección de datos personales y privacidad implica comprender los riesgos asociados con la divulgación de información personal en línea y adoptar medidas para protegerla. Esto incluye tener conocimiento sobre las políticas de privacidad, utilizar contraseñas seguras, mantener actualizado el software de seguridad, evitar compartir información personal sensible en lugares no seguros y comprender cómo se manejan y protegen los datos personales por parte de las plataformas digitales.
6. **Prevención de la desinformación y las fake news:** En el entorno digital, la desinformación y las fake news son una preocupación importante. La competencia en la prevención de la desinformación implica desarrollar habilidades para detectar y evitar la propagación de información falsa o engañosa. Esto implica verificar la veracidad de la información, buscar múltiples fuentes, evaluar la credibilidad de los medios y las noticias, y comprender cómo se difunde la desinformación en línea.
7. **Gestión de la sobrecarga de información:** En la era digital, se enfrenta a una gran cantidad de información disponible. La competencia en la gestión de la sobrecarga de información implica tener habilidades para filtrar, organizar y sintetizar la información de manera eficiente. Esto ayuda a encontrar la información relevante, evitar la saturación de información y tomar decisiones informadas en medio de la avalancha de datos.
8. **Conciencia de la privacidad y la seguridad:** La conciencia de la privacidad y la seguridad es fundamental al utilizar y compartir información en línea. Implica comprender los riesgos asociados con la divulgación de datos personales, utilizar medidas de seguridad adecuadas (como contraseñas seguras y autenticación de dos factores), comprender las políticas de privacidad de las plataformas digitales y proteger la información personal.
9. **Uso responsable de las redes sociales y plataformas digitales:** Las redes sociales y otras plataformas digitales son herramientas poderosas, pero también requieren un uso responsable. La competencia en el uso responsable de las redes sociales y plataformas digitales implica comprender y respetar las normas de conducta en línea, ser consciente del impacto de nuestras acciones y palabras en otros usuarios, y

utilizar estas plataformas de manera ética y responsable, evitando el ciberacoso, la difamación

Consejos para el uso seguro de redes sociales.

La seguridad en las redes sociales implica adoptar medidas para proteger nuestra privacidad, controlar la información que compartimos, prevenir el acceso no autorizado a nuestras cuentas y estar alerta ante posibles amenazas. Esto implica configurar adecuadamente la privacidad de nuestras cuentas, utilizar contraseñas fuertes y únicas, ser selectivos al aceptar solicitudes de amistad, evitar compartir información personal sensible y ser conscientes de las prácticas seguras en el uso de estas plataformas.

Aquí tienes 10 consejos importantes para que los adolescentes utilicen las redes sociales de manera segura:

a. **Configura adecuadamente la privacidad:** Ajuste la configuración de privacidad en sus perfiles de redes sociales para tener el control de quién puede ver información y publicaciones. Limita el acceso solo a personas de confianza y evita compartir información personal sensible en plataformas públicas.
b. **Sé selectiva con las solicitudes de amistad:** Acepta únicamente solicitudes de amistad de personas que conoces en la vida real. Evita agregar personas desconocidas o que parezcan sospechosas.
c. **Piensa antes de publicar:** Antes de compartir una publicación, imagen o video, considera el impacto que puede tener. Recuerda que lo que publicas en línea puede ser permanente y puede afectar tu reputación en el futuro.
d. **Protege tu información personal:** Evita compartir información personal, como tu dirección, número de teléfono, número de cédula, o detalles de tus rutinas diarias, en las redes sociales. No subas fotos de tus pertenencias.
e. **No te involucres en ciberacoso:** No participas en ciberacoso ni hostigamiento en línea. Sé respetuoso con los demás y denuncia cualquier actividad abusiva o inapropiada que encuentres en las redes sociales.
f. **Utiliza contraseñas seguras**: Crea contraseñas fuertes y únicas para tus cuentas en redes sociales. No compartas tus contraseñas con nadie y cámbialas periódicamente para mantener tu cuenta protegida.
g. **No compartes tu ubicación en tiempo real:** Evita compartir constantemente tu ubicación en tiempo real a través de las redes sociales. Esto puede ser peligroso y permitir que personas no deseadas conozcan tu paradero.
h. **Aprende a identificar estafas y fraudes:** Sé cauteloso con los enlaces, ofertas o mensajes que recibe en las redes sociales. Aprende a identificar estafas y fraudes en línea y evita compartir información personal o financiera en respuesta a estas solicitudes.

i. **No confíes en extraños en línea:** No compartes información personal ni te involucres en conversaciones privadas con personas que no conoces en la vida real. Los depredadores en línea pueden fingir ser alguien que no son para obtener información o establecer contacto para posibles estafas.
j. **Habla con un adulto de confianza:** Si te sientes incómodo, amenazado o experimentas algún tipo de situación preocupante en las redes sociales, habla con un adulto de confianza, como tus padres, un profesor o un consejero escolar. Ellos podrán brindarte el apoyo y la orientación necesaria.

La seguridad de la información es crucial para proteger nuestra privacidad, prevenir el robo de identidad, evitar el ciberacoso y garantizar una experiencia en línea positiva. Al tomar medidas proactivas para protegernos y educarnos sobre los riesgos, podemos disfrutar de las redes sociales de manera segura y responsable.

Actividades sugeridas con estudiantes:

- ☐ Pide a la estudiantes configuren la privacidad de todas sus redes sociales.
- ☐ Evaluación de fuentes de información: Pide a los estudiantes que seleccionen publicaciones o noticias en las redes sociales y las evalúen en términos de veracidad y confiabilidad. Discuten cómo verificar la información antes de compartirla y cómo detectar noticias falsas o desinformación en línea. Algunos tips para evaluar fuentes de información pueden ser la utilización de sitios académicos reconocidos como Google académico, repositorios de universidades, Páginas webs de organizaciones o fuentes de noticias reconocidas de posturas políticas opuestas, como por ejemplo: CNN y Telesur.
- ☐ Anima a los estudiantes a crear contenido positivo y constructivo en las redes sociales. Pueden trabajar en proyectos de colaboración en línea, promover mensajes de inclusión y respeto, o compartir información útil y relevante para su comunidad.

Innovación tecnológica

La tecnología y el uso de la información

La tecnología desempeña un papel fundamental en el uso y acceso consciente a la información. A través de las tecnologías de la información y la comunicación (TIC), tenemos acceso a una cantidad masiva de información en línea. Sin embargo, la tecnología también puede presentar desafíos en términos de la calidad y la confiabilidad de la información disponible.

La tecnología proporciona herramientas y plataformas que facilitan la búsqueda, el acceso y la gestión de la información. Los motores de búsqueda, las redes sociales, los sitios web especializados y otras aplicaciones digitales nos permiten explorar y descubrir información en diversos formatos y de diversas fuentes. Además, las tecnologías emergentes como la inteligencia artificial y el aprendizaje automático pueden ayudar a filtrar y personalizar la información de acuerdo con nuestras preferencias y necesidades.

Sin embargo, el acceso a una gran cantidad de información también puede llevar a la sobrecarga de información y a la dificultad para evaluar su calidad y confiabilidad. En este sentido, la tecnología también nos desafía a desarrollar competencias clave, como el pensamiento crítico y la evaluación de fuentes, para discernir entre la información confiable y la desinformación.

Además, la tecnología también tiene un impacto en la forma en que compartimos y comunicamos información. Las redes sociales y otras plataformas digitales nos brindan la capacidad de compartir información de manera rápida y global. Sin embargo, esto también implica la responsabilidad de compartir información de manera precisa, verificada y respetuosa.

La tecnología amplía nuestro acceso a la información y nos proporciona herramientas para gestionarla de manera más eficiente. Sin embargo, también plantea desafíos en términos de evaluación de la calidad de la información y la necesidad de desarrollar habilidades para utilizarla de manera consciente. Es fundamental utilizar la tecnología de manera crítica y responsable para aprovechar al máximo su potencial en el uso y acceso consciente a la información.

La tecnología y el desarrollo sostenible

En el contexto del desarrollo sostenible, las "tecnologías innovadoras" se refieren a soluciones técnicas y sistemas que están diseñados para abordar los desafíos ambientales, sociales y económicos de manera creativa, novedosa y efectiva. Estas tecnologías buscan promover la sostenibilidad al reducir el impacto ambiental negativo, fomentar la equidad social, ayudar a la creación de conocimiento y mejorar la eficiencia en el uso de recursos.

Las tecnologías innovadoras en el desarrollo sostenible pueden abarcar diversos campos y sectores, y su aplicación puede variar en función de las necesidades y características de cada lugar. En Galápagos, algunos ejemplos de tecnologías innovadoras incluyen:

a) **Energías renovables:** Incluyen tecnologías como la energía solar, eólica, hidroeléctrica, geotérmica y de biomasa. Estas fuentes de energía aprovechan recursos naturales y renovables, reduciendo así las emisiones de gases de efecto invernadero y la dependencia de los combustibles fósiles.
b) **Eficiencia energética:** Comprende tecnologías y sistemas que permiten reducir el consumo energético en edificios, industrias y transporte. Estas tecnologías incluyen iluminación LED, sistemas de gestión energética, electrodomésticos eficientes y vehículos de bajo consumo energético.
c) **Agricultura sostenible:** Implica el uso de tecnologías innovadoras en la producción agrícola, como la agricultura de precisión, la hidroponía, la agroforestería y la permacultura. Estas técnicas buscan minimizar el uso de agua, reducir los impactos ambientales y aumentar la productividad de manera sostenible.
d) **Gestión inteligente de residuos:** Involucra tecnologías para la clasificación, reciclaje y tratamiento de residuos sólidos y líquidos. Estos incluyen sistemas de recogida selectiva, compostaje, biogás y tecnologías de reciclaje avanzadas.
e) **Creación de conocimiento e investigación:** La innovación tecnológica permite grandes avances en la creación de conocimiento, investigación y la ciencia. Las nuevas tecnologías permiten acceder a nuevos lugares, eficientizar procesos, obtener datos nuevos o de manera más exacta, entre otros muchos beneficios.

Estos son solo algunos ejemplos de tecnologías innovadoras en el contexto del desarrollo sostenible. La innovación tecnológica desempeña un papel crucial para impulsar la sostenibilidad al proporcionar soluciones efectivas y escalables que pueden contribuir a un futuro más equitativo y ambientalmente responsable.

Innovación tecnológica en Galápagos

A continuación, presentamos algunos ejemplos de cómo se usa de la tecnología de manera innovadora en Galápagos:

Nombre del proyecto/iniciativa	**Catálogo de fotoidentificación de tiburón ballena / Wildbook for Sharks**
Descripción del proyecto/iniciativa	El catálogo global de tiburones ballena Wildbook for Whale Sharks es una base de datos de fotografías de encuentros con tiburones ballena.

	La plataforma es de acceso abierto para el uso de ciencia ciudadana e investigación. Es mantenida y utilizada por biólogos marinos para recopilar y analizar datos de avistamientos de tiburones para aprender más sobre su distribución, ecología y amenazas. El Proyecto del Tiburón Ballena de Galápagos (Galapagos Whale Shark Project), utiliza esta plataforma para el registro, identificación y monitoreo de tiburones ballena avistados en la Reserva Marina de Galápagos y el Pacífico Este Tropical. A través del uso de inteligencia artificial, el Wildbook usa fotografías del patrón de la piel detrás de las branquias de cada tiburón (ya que son diferentes en cada animal como las huellas digitales en humanos) para distinguir entre animales individuales y mantener un catálogo de individuos y re-avistamientos en la zona. Esta plataforma es alimentada por investigadores, turistas, guías y otros actores locales, siendo un ejemplo del uso de ciencia ciudadana para la conservación de especies amenazadas.
Tecnología relacionada con el proyecto/iniciativa	Inteligencia artificial
Link a proyecto/iniciativa	https://www.sharkbook.ai/

Nombre del proyecto/iniciativa	**Producción hidropónica de lechugas - Finca de Romer Ochoa**
Descripción del proyecto/iniciativa	La hidroponía es una tecnología innovadora en el campo de la agricultura y la producción de alimentos. Se refiere a un sistema de cultivo en el cual las plantas se cultivan en soluciones acuosas, sin la necesidad de suelo tradicional. La hidroponía se considera una tecnología innovadora debido a su capacidad para optimizar el uso de recursos, aumentar la productividad, permitir el cultivo en espacios limitados, proporcionar condiciones de cultivo controladas y reducir el impacto ambiental de la agricultura. Estas características la convierten en una opción atractiva para la producción de alimentos en el contexto del desarrollo sostenible..
Tecnología relacionada con el proyecto/iniciativa	Hidroponía
Link a proyecto/iniciativa	https://www.observatoriogalapagos.gob.ec/wp-content/uploads/2021/04/Directorio_Fincas_Agroturismo_gps.pdf

Nombre del proyecto/iniciativa	**Shark Count**
Descripción del proyecto/iniciativa	Herramienta de ciencia ciudadana que permite a los buzos y turistas que visitan el archipiélago ayudar a monitorear la vida marina en la Reserva Marina de Galápagos, especialmente de especies como: tiburones, tortugas marinas, rayas y peces. Esta aplicación muestra informes individuales de buzos en los 20 mejores sitios de buceo del archipiélago. Los cuadros y mapas muestran la cantidad de especies observadas durante cada inmersión, además de los mejores sitios y horarios para ver cada especie.
Tecnología relacionada con el proyecto/iniciativa	Aplicación móvil
Link a proyecto/iniciativa	https://sharkcount.org/

Nombre del proyecto/iniciativa	**Ensilado de pescado**

Descripción del proyecto/iniciativa	Producto hecho a base de residuos de pescado que es usado como suplemento nutricional para animales menores y como fertilizante orgánico. Los desechos son triturados a través de un molino para hacer ensilado de pescado. El ensilado de pescado es utilizado como insumo agropecuario, ya sea como fertilizante orgánico o como alimento para cerdos o pollos. Contribuye a reducir la presión existente sobre el relleno sanitario y el medioambiente en la isla.
Tecnología relacionada con el proyecto/iniciativa	Máquina para triturado de desechos, economía circular
Link a proyecto/iniciativa	https://www.conservation.org/ecuador/noticias/2021/12/22/transformando-los-desechos-de-la-pesca-en-una-alternativa-innovadora-para-la-econom%C3%ADa-circular-en-las-islas-gal%C3%A1pagos

Nombre del proyecto/iniciativa	**Galapagos Artesanal Seafood**
Descripción del proyecto/iniciativa	Emprendimiento local que promueve la pesca sostenible, con diferentes presentaciones al vacío de productos marinos, a través de su sistema de trazabilidad. Este consiste en una cámara a bordo y bitácora electrónica para registro del viaje de pesca, y etiquetas QR. La etiqueta QR permite al comprador verificar el viaje de pesca: dónde se pescó, cuáles especies y qué volumen fueron capturadas, el tipo de arte de pesca, si hubo pesca incidental o no. Además, este sistema permite registrar avistamiento de otras especies comerciales o especies protegidas, contribuyendo así a la investigación como ciencia ciudadana.
Tecnología relacionada con el proyecto/iniciativa	Sistema de Trazabilidad – Schellcatch (grabación y geolocalización), con etiquetas QR
Link a proyecto/iniciativa	Instagram: GalapagosArtesanalSeaFood


Nombre del proyecto/iniciativa	**Hacienda Tranquila**
Descripción del proyecto/iniciativa	Proyecto de Turismo Rural y Sostenible que promueve actividades como: agricultura, reforestación de especies endémicas, control de especies invasoras, investigación de aves marinas (petrel) y conservación de árboles endémicos Scalesia. Así también, cuenta con una estación meteorológica que registra datos valiosos para comprender mejor el impacto del cambio climático en la zona. Además, de fomentar la innovación de la actividad ganadera a través de la inseminación artificial y trasplante de embriones, para garantizar su calidad y su adaptación al cambio climático.
Tecnología relacionada con el proyecto/iniciativa	Inseminación artificial y trasplante de embriones
Link a proyecto/iniciativa	https://haciendatranquila.org/

Nombre del proyecto/iniciativa	**Story Map Letty**
Descripción del proyecto/iniciativa	Esta herramienta dinámica del Proyecto Huertos Tranquilos en la isla San Cristóbal consiste en un mapa para ilustrar la línea base y gradual de la adopción de plantas endémicas por familias galapagueñas (Lecocarpus Darwinii y Lecocarpus leptolobus), conociendo donde se encuentran sembradas y las características de cada planta.
Tecnología relacionada con el proyecto/iniciativa	Sistemas de información geográfica
Link a proyecto/iniciativa	https://storymaps.arcgis.com/stories/8bb2b24e2d014dcd8cb3e83b689d2b26
	

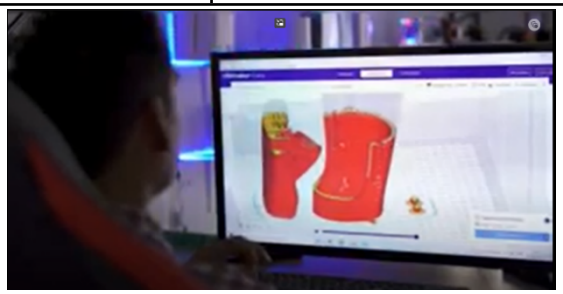
Nombre del proyecto/iniciativa	**Galapagos Inti Taller de Fotografía Experimental**
Descripción del proyecto/iniciativa	La cianitipia es un proceso fotográfico antiguo monocromático desde un negativo de imagen a través del cual se obtiene una impresión azul cian. El papel usado como soporte es un papel de alta calidad hecho también con técnicas antiguas sin ácidos de tal forma que logra resistencia, estabilidad y un toque especial. Cada impresión es original y única, hecha una por una; aún cuando se realizan más de una impresión del

	mismo negativo, cada impresión debido al proceso de la técnica es irrepetible. Todo el proceso es hecho a mano, la intensidad de la luz, la textura, el emulsionado del papel, el tiempo de exposición y el revelado influenciará y modificará el resultado final.
Tecnología relacionada con el proyecto/iniciativa	Cianotipia, Untotipia y Fitotipia
Link a proyecto/iniciativa	Instagram: galapagos_inti
 *Artista: Mónica Páez*	

Nombre del proyecto/iniciativa	**Precious Plastics**
Descripción del proyecto/iniciativa	Iniciativa que promueve la combinación de personas, máquinas, plataformas para crear un sistema de reciclaje global alternativo. En Galápagos, la iniciativa está enfocada en la creación de joyería y adornos de hogar reciclando plástico.
Tecnología relacionada con el proyecto/iniciativa	Máquinas de reciclaje de plástico para producción de materias primas.
Link a proyecto/iniciativa	Instagram: Preciousplasticgalapagos https://www.youtube.com/watch?v=ruVxGrF9s0E
 	

Nombre del proyecto/iniciativa	**Orcatec**
Descripción del proyecto/iniciativa	Soluciones y tecnologías ambientales que se inspiran en entender y aplicar los procesos naturales para mejorar la calidad de vida, la conexión con la naturaleza y la reducción de la contaminación, a través de: sistemas de purificación de aguas, calentadores solares y sistemas fotovoltáicos.
Tecnología relacionada con el proyecto/iniciativa	Energía solar
Link a proyecto/iniciativa	www.orcatec.ec

Nombre del proyecto/iniciativa	**Zona Móvil Galápagos**
Descripción del proyecto/iniciativa	Impresión 3D con plástico reciclado para adornos inspirados en Galápagos, llaveros, macetas y prótesis.
Tecnología relacionada con el proyecto/iniciativa	Impresión 3D
Link a proyecto/iniciativa	https://www.facebook.com/zonamovilec

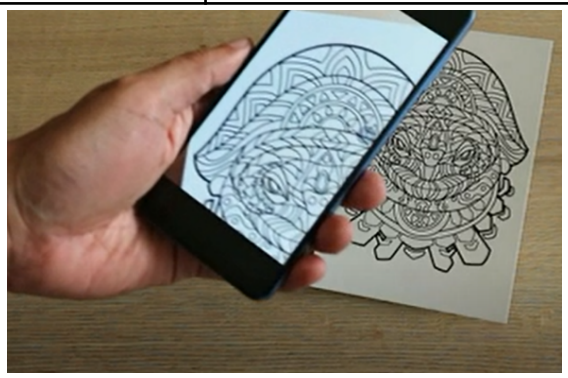


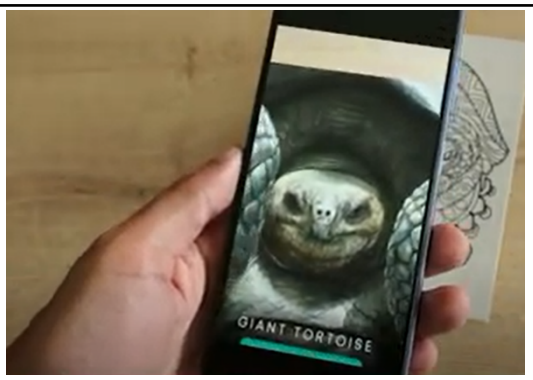
Nombre del proyecto/iniciativa	**Reconstrucción digital de la Casa Manuel J. Cobos**
Descripción del proyecto/iniciativa	Proyecto en favor de la educación y turismo cultural en Galápagos a través de la reconstrucción digital de un lugar emblemático e histórico del cantón San Cristóbal.
Tecnología relacionada con el proyecto/iniciativa	Software MAYA, Inteligencia Artificial KAIBER
Link a proyecto/iniciativa	-

Nombre del proyecto/iniciativa	**Barcode**
Descripción del proyecto/iniciativa	Catálogo de la biodiversidad de las islas Galápagos utilizando técnicas de muestreo no invasivas, como el ADN ambiental, con un enfoque en ecosistemas marino-costeros y técnicas de laboratorio como Metabarcoding que son capaces de generar una gran cantidad de información.
Tecnología relacionada con el proyecto/iniciativa	ADN Ambiental
Link a proyecto/iniciativa	https://noticias.usfq.edu.ec/2021/07/codigo-genetico-de-galapagos-el-mayor.html#:~:text=En%20septiembre%202020%2C%20el%20Galapagos,de%20c%C3%B3digo%20de%20barras%20gen%C3%A9tico

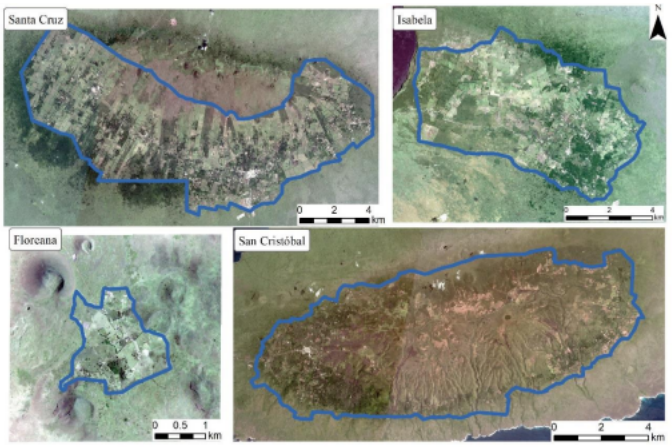
Nombre del proyecto/iniciativa	**Nunative**
Descripción del proyecto/iniciativa	Aplicación digital con información de los productores locales a la cual los clientes llegarán interactivamente mediante postales ilustradas. Estas postales usarán la realidad aumentada que son el vínculo entre el turista y la plataforma digital.
Tecnología relacionada con el proyecto/iniciativa	Realidad virtual, QR ilustrados

Link a proyecto/iniciativa	https://youtu.be/Usve5q-McGU





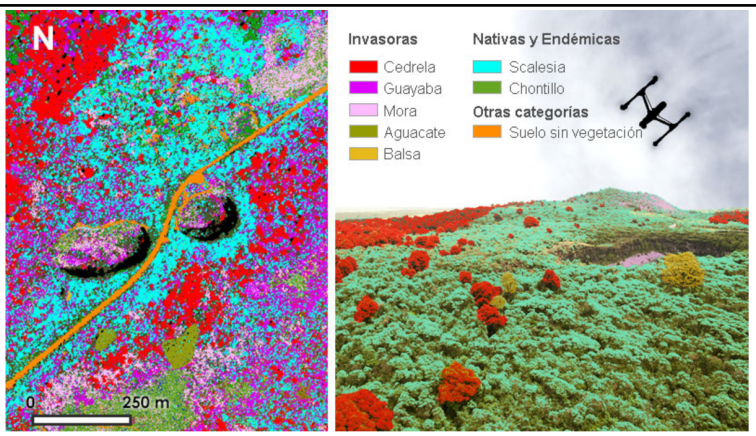
Nombre del proyecto/iniciativa	**Mapeo de agroecosistemas de Galápagos**
Descripción del proyecto/iniciativa **(hacer énfasis en cómo se vincula con el tema de sostenibilidad)**	Las zonas altas húmedas de las Islas Galápagos son biológicamente las áreas más diversas y productivas, y constituyen hábitats esenciales para especies endémicas de Galápagos, como las Tortugas gigantes, petreles, lechuzas, scalesia, miconia, etc. Las partes altas también son las áreas más propensas a ser colonizadas por especies invasoras, especialmente cuando los agricultores abandonan sus tierras. Además, en las zonas altas se puede producir alimentos localmente, por lo que son esenciales para la seguridad alimentaria de la provincia. Sin embargo, existe poca información sobre esta región. Este proyecto utilizó imágenes satelitales, drones y entrevistas con productores para crear el primer mapa de alta resolución del área agrícola de Galápagos. El mapa clasifica la cobertura del área agrícola en 20 categorías, relevantes tanto para el sector agrícola como para científicos de la conservación. El mapa completo en formato shapefile puede ser descargado desde la sección de materiales suplementarios en su publicación original (https://www.mdpi.com/2072-4292/12/1/65). Este proyecto busca fomentar la colaboración entre agricultura y conservación.
Subtema relacionado con el proyecto/iniciativa	Sensores remotos, Drones, Agricultura
Link a proyecto/iniciativa	https://franciscolaso.web.unc.edu/



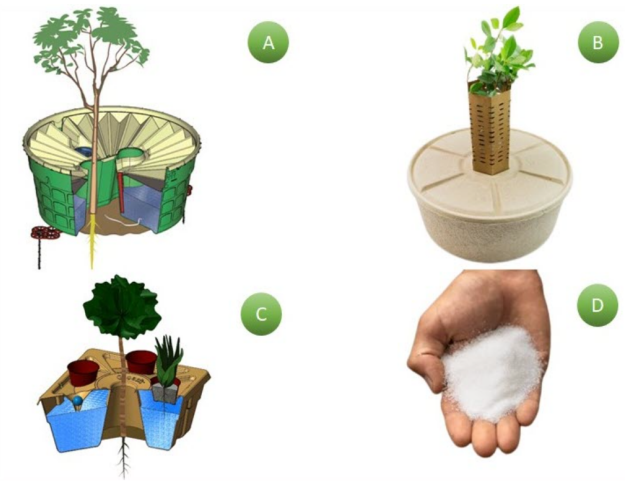
Nombre del proyecto/iniciativa	**Ecología de tiburones / Metodologías de investigación**
Descripción del proyecto/iniciativa	Para evaluar el estado poblacional, patrones de movimiento y rutas migratorias de las especies más comunes de tiburones en la Reserva Marina, el proyecto "Ecología de Tiburones", de la Fundación Charles Darwin, utiliza las siguientes herramientas metodológicas innovadoras: **- Telemetría satelital** La telemetría satelital es un sistema de transmisión de datos que utiliza satélites para enviar información a distancia. Consiste en el envío de datos desde una ubicación remota a través de un dispositivo o sensor, que se transmite al espacio utilizando un enlace de comunicación vía satélite. El satélite recibe los datos y los retransmite a una estación terrestre que los procesa y analiza. **- Cámaras BRUVS** Un BRUV (Baited Remote Underwater Video de sus siglas en inglés) es una herramienta de investigación comúnmente utilizada en el estudio de tiburones. Consiste en un sistema de cámara montado en una estructura con cebo para atraer tiburones u otros organismos marinos. La estructura se coloca en la columna de agua o en el fondo marino durante un tiempo determinado. La cámara graba imágenes de video del área circundante, lo que permite a los investigadores observar y estudiar el comportamiento, la abundancia y la diversidad de tiburones y otras especies marinas en su hábitat natural. Los BRUV proporcionan un método no invasivo para recopilar datos y se pueden desplegar en diversos entornos marinos para obtener información valiosa con fines de conservación y gestión. **-Vehículos operados remotamente** Un ROV (Remotely Operated Vehicle) es un vehículo operado de forma remota que se utiliza en investigaciones marinas. Consiste en un dispositivo sumergible controlado a distancia que está equipado con cámaras, luces y otros instrumentos científicos. Los ROV son utilizados para explorar y estudiar el océano a grandes profundidades donde es difícil para los humanos llegar. Los científicos pueden controlar el ROV desde la superficie y obtener imágenes de video de alta resolución, recolectar muestras y realizar mediciones en el entorno submarino. Estos vehículos son fundamentales para investigaciones en arrecifes de coral, estudios de vida marina, exploración de fondos marinos y en la inspección de estructuras submarinas. Los ROV permiten a los científicos llevar a cabo

	investigaciones detalladas y precisas en áreas que de otra manera serían inaccesibles.
Tecnología relacionada con el proyecto/iniciativa	Telemetría satelital, BRUVs y ROVs
Link a proyecto/iniciativa	https://www.darwinfoundation.org/es/investigacion/proyectos/tiburones https://www.darwinfoundation.org/es/publicaciones/educacion-ambiental/tiburones-de-la-reserva-marina-de-galapagos

Nombre del proyecto/iniciativa	**Mapeo de vegetación con imágenes satelitales y drones / Herramientas para procesos de restauración de ecosistemas**
Descripción del proyecto/iniciativa	Los mapas de vegetación proveen una importante herramienta para guiar acciones de manejo para la restauración de los ecosistemas terrestres en las Islas Galápagos. El proyecto “Mapeo de vegetación para la restauración de los ecosistemas” de la Fundación Charles Darwin, utiliza imágenes satelitales y de drones para generar mapas de muy alta resolución que muestran la distribución y abundancia de especies de plantas invasoras, como la mora (*Rubus niveus*), guayaba (*Psidium guajava*), cedrela (*Cedrela odorata*), cascarilla (*Cinchona pubescens*) y especies de plantas endémicas clave, como *Scalesia pedunculata* o *Miconia robinsoniana*.
Tecnología relacionada con el proyecto/iniciativa	Imágenes satelitales y drones.
Link a proyecto/iniciativa	https://www.darwinfoundation.org/es/investigacion/proyectos/mapeo-de-vegetacion-para-la-restauracion-de-ecosistemas



Nombre del proyecto/iniciativa	**Programa Galápagos Verde 2050 / Tecnologías ahorradoras de agua y herramientas para la restauración ecológica**
Descripción del proyecto/iniciativa	Un gran porcentaje del territorio de las islas Galápagos es árido. Los períodos de sequía y la falta de suministro de agua dulce crean dificultades para la implementación de procesos de restauración ecológica. Para abordar estos desafíos relacionados con el agua, el Programa Galápagos Verde 2050 recurre al uso de tecnologías ahorradoras de agua y otras herramientas recientemente desarrolladas, como Groasis Waterboxx ® (Waterboxx), Groasis Growboxx ®, Cocoon, Hydrogel y BioChar, que se han utilizado con éxito en todo el mundo para aumentar la supervivencia y el crecimiento de especies nativas de ambientes áridos. El uso de estas tecnologías puede acelerar los esfuerzos de restauración ecológica y reducir los costos de riego.
Tecnología relacionada con el proyecto/iniciativa	Tecnologías para ahorro de agua y agricultura sostenible: - Tecnología Groasis Waterboxx®. - Cajas biodegradables Cocoon. - Tecnología Growboxx - Hidrogel - BioChar
Link a proyecto/iniciativa	https://www.darwinfoundation.org/es/investigacion/proyectos/gv2050-recuperacion-especies-peligro-de-extincion-png http://www.galapagosverde2050.com/info/galapagos-verde-2050 https://www.youtube.com/watch?v=eEygoGorCDs https://www.youtube.com/watch?v=ZGG6O_NmQgM https://www.youtube.com/watch?v=KzrMstDZg0k https://www.youtube.com/watch?v=bTRNSh8e9LE



Nombre del proyecto/iniciativa	**Socioecología, evaluación y manejo de pesquerías artesanales en Galápagos: pasos hacia la sostenibilidad / Líneas de investigación y metodologías innovadoras**
Descripción del proyecto/iniciativa	La FCD junto con la Dirección del Parque Nacional Galápagos y otros socios están llevando a cabo investigaciones interdisciplinarias para lograr pesquerías sostenibles en Galápagos. Las investigaciones abarcan desde la biología y ecología de las especies, línea base de ecosistemas, tecnologías de captura, hasta la gobernanza, la sociología de los pescadores y la economía de la actividad pesquera. Los estudios científicos se desarrollar a través de diferentes líneas de investigación, que involucran metodologías o herramientas innovadoras: -Línea de investigación biológico-pesquera sobre las especies y ecosistemas asociados: • Análisis de metales en peces de Galápagos • Manglares: Sistema de información geográfica mediante uso de imágenes satelitales y drones; genética de especies y suelo; censo visual con cámara. • Intermareal: Uso de dron, fotocuadrantes, fotomosaicos, inteligencia artificial -Línea de investigación socio-económica: Sistema de trazabilidad del mar al consumidor mediante el uso de tecnologías innovadoras como cámaras a bordo, bitácoras electrónicas y etiquetado QR. -Línea social: Utilización de tecnologías sociales participativas como “El contenedor”, y “La comunidad de emprendimiento de alimentos del mar de Galápagos” -Línea cambio climático: Red de monitoreo de temperatura del mar mediante loggers y boyas oceánicas.
Tecnología relacionada con el proyecto/iniciativa	-Creación de conocimiento e investigación -Investigación participativa -Inteligencia artificial
Link a proyecto/iniciativa	https://www.darwinfoundation.org/es/investigacion/proyectos/socio-ecologia-evaluacion-y-manejo-de-pesquerias https://fcdgps.maps.arcgis.com/apps/Cascade/index.html?appid=0ea24aaa14a74790b65e82a288f709ca http://www.pescagalapagos.ec/es/el-proyecto

Nombre del proyecto/iniciativa	**Programa de ecología de movimiento de tortugas gigantes de Galápagos**
Descripción del proyecto/iniciativa	La migración de las tortugas gigantes de Galápagos cumple un papel fundamental en el mantenimiento saludable de sus poblaciones. Entender las implicaciones ecológicas, sociales y sanitarias de dicha migración nos permite disminuir las amenazas que enfrentan las tortugas y contribuir a su conservación. Para esto, el "Proyecto de ecología de movimiento de tortugas gigantes de Galápagos" utiliza las siguientes metodologías y herramientas innovadoras: -**Uso de GPS y VHF** para monitoreo de movimiento de tortugas adultas y juveniles: En la investigación del movimiento de tortugas gigantes, se emplea el sistema de posicionamiento global (GPS) y el radio de frecuencia muy alta (VHF) para rastrear y estudiar sus desplazamientos. Se coloca un dispositivo equipado con GPS y VHF en la tortuga, que registra su ubicación exacta a través de los satélites del sistema GPS. Esto permite obtener datos precisos sobre los lugares que visitan y las rutas que siguen. Además, el VHF proporciona una forma de seguimiento en tiempo real a través de la emisión de señales de radio, lo que permite a los investigadores localizar y seguir a las tortugas en el terreno. Esta combinación de tecnologías es esencial para comprender los patrones de migración, las áreas de alimentación y los hábitats utilizados por las tortugas gigantes, lo que contribuye a su conservación y manejo adecuado. **-Telemetría:** La telemetría satelital es un sistema de transmisión de datos que utiliza satélites para enviar información a distancia. Consiste en el envío de datos desde una ubicación remota a través de un dispositivo o sensor, que se transmite al espacio utilizando un enlace de comunicación vía satélite. El satélite recibe los datos y los retransmite a una estación terrestre que los procesa y analiza. **-PCR:** El uso de la PCR (Reacción en Cadena de la Polimerasa, por sus siglas en inglés) en la investigación de tortugas gigantes puede ser aplicado para diversas finalidades. Una de las aplicaciones más comunes es el análisis genético. Mediante la extracción de muestras de tejido, sangre o hisopados bucales de las tortugas, se pueden obtener muestras de ADN. La PCR permite amplificar y copiar selectivamente regiones específicas del ADN, lo que facilita el estudio de la diversidad genética, las relaciones filogenéticas entre poblaciones y la identificación de individuos. Además, la PCR también se utiliza para detectar la

	presencia de patógenos, como bacterias, virus o parásitos, que pueden afectar la salud de las tortugas gigantes. Estas aplicaciones de la PCR en la investigación contribuyen al conocimiento y la conservación de estas especies emblemáticas.
Tecnología relacionada con el proyecto/iniciativa	GPS y VHF, telemetría y PCR
Link a proyecto/iniciativa	https://www.darwinfoundation.org/es/investigacion/proyectos/programa-de-ecologia-de-movimiento-de-tortugas-de-galapagos https://www.youtube.com/watch?v=GVfLt9Kiih4 https://www.youtube.com/watch?v=wfaWJE0Q-ek https://www.darwinfoundation.org/es/blog-es/mujeres-en-la-ciencia/818-pcr-en-tortugas-gigantes-de-galapagos

Literatura citada

Boyd, D. (2014). It's Complicated: The social lives of networked teens. Yale University Press.

Boyd, D., & Ellison, N. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), 210-230.

Capurro, R., & Hjørland, B. (Eds.). (2003). The concept of information. Annual Review of Information Science and Technology, 37(1), 343-411.

Floridi, L. (2010). Information: A very short introduction. Oxford University Press.

Johnson, C. A. (2015). Digital information literacy in an information society: Implications for LIS professionals. The Library Quarterly, 85(2), 99-118.

Marwick, A., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. New Media & Society, 16(7), 1051-1067.

Van Dijck, J. (2013). The Culture of Connectivity: A critical history of social media. Oxford University Press.