Áreas Transversales: Sociales, Castellano, matemáticas, artística, sociales, economía, inglés.

Elabora: Gigliola Martínez

TIEMPO: 1 ___ 2 X

COMPETENCIAS: Orientación al resultado, cognitivo

PROPÓSITO:

Conocer acerca de las Políticas de buenas contraseñas y seguridad informática en adolescentes

INDICADORES DE DESEMPEÑO:

Reconocimiento de las políticas para establecer contraseñas a los datos personales y comerciales; además, formas y herramientas para prevenir inseguridad en la red para los niños.

TEMA: Políticas De Buenas Contraseñas y seguridad informática Para Adolescentes

METODOLOGÍA INSTITUCIONAL C3

CONCIENTIZACIÓN

Vídeo: CONSEJOS de CIBERSEGURIDAD para NIÑOS y ADOLESCENTES - CiberINseguro Kids & Teens

CONCEPTUALIZACIÓN

Leer:

LA SEGURIDAD INFORMÁTICA PARA ADOLESCENTES.

Se refiere al conjunto de prácticas, conocimientos y medidas diseñadas para proteger la información personal y dispositivos tecnológicos que los adolescentes usan al navegar por internet, utilizar redes sociales, aplicaciones móviles, o al interactuar en línea.

Se centra en:

1. **Proteger la privacidad** : Enseñar a los adolescentes a mantener segura su información personal (como nombres, direcciones, contraseñas y fotos) para evitar que sea utilizada sin su consentimiento.
2. **Seguridad en redes sociales** : Explicar cómo configurar las opciones de privacidad en plataformas como Instagram, TikTok o WhatsApp, y las consecuencias de compartir demasiado.
3. **Ciberacoso** : Informarles sobre los riesgos del ciberacoso (o bullying digital) y cómo actuar si lo experimentan o lo presencian.
4. **Phishing y fraudes** : Publicidad sobre correos o mensajes sospechosos que intentan robar información personal o financiera.
5. **Ciberseguridad básica** : Instruir sobre el uso de contraseñas seguras, la instalación de software antivirus, la importancia de las actualizaciones y cómo evitar descargar archivos de fuentes no confiables.

El objetivo es empoderar a los adolescentes para que naveguen de manera segura y responsable en el entorno digital.

Aquí algunos aspectos esenciales para que los adolescentes se mantengan seguros en línea:

1. Contraseñas seguras
- Usar contraseñas robustas
- Combinar letras mayúsculas y minúsculas, números y símbolos.
- Cambiar las contraseñas con regularidad
- Utilizar un administrador de contraseñas para almacenarlas de

2. Privacidad en redes sociales
- Configurar adecuadamente la privacidad en redes sociales para limitar quién puede
- Evitar compartir detalles sensibles como la dirección, número de
- Ser cauteloso al agregar a personas desconocidas

3. Cuidado con el ciberacoso
- Ser consciente de las señales de ciberacoso y saber cómo reportar o bloquear a usuarios que se comportan de manera inapropiada.
- Hablar con un adulto de confianza si se experimenta ciberacoso o se recibe contenido perturbador.

4. Evitar el phishing y los fraudes
- No hacer clic en enlaces o descargar archivos de fuentes desconocidas o sospechosas
- Desconfiar de correos electrónicos, mensajes o anuncios que prometen premios o regalos inesperados.

5. Uso de antivirus y actualizaciones
- Mantener siempre el dispositivo con un software antiv
- Realizar actualizaciones del sistema operativo y aplicaciones regularmente para corregi

6. Navegación segura
- Usar conexiones seguras (https) al navegar por la web, especialmente al ingresar información personal.
- Evite conectarse a redes Wi-Fi públicas sin utilizar una VPN (red privada virtual).

7. No compartir información sensata
- Evitar publicar fotos o videos comprometidos que podrían ser usados en su contra en el futuro
- Tenga cuidado con los juegos o aplicaciones que solicitan acceso a información personal oa la cámara y micrófono

8. Control y supervisión parental
- Los padres pueden utilizar herramientas de control parental para ayudar a monitorear y limitar el acceso a ciertos con
- Establecer un diálogo abierto con los padres o tutores sobre la actividad en línea

9. Estar atentos a la identidad digital
- Mantener una buena reputación en línea evitando comentarios ofensivos o comportamientos tóxicos, ya que lo que se publica en internet puede tener consecuencias a la

10. Conciencia sobre la desinformación
- Aprender a identificar noticias falsas y desinformación. Contrastar la información de varias fuentes antes de creer y compartir contenido.

11. Comportamiento ético en línea
- Sé respetuoso en tus interacciones y evita comportamientos dañinos o tó
- No descargues contenido ilegal (como software o películas pirateadas) ni participes en actividades ilegales en

Recursos adicionales para adolescentes

Existen múltiples plataformas y programas que ayudan a enseñar a los adolescentes sobre la seguridad en línea, como:
- **Google Family Link (Enlace familiar de Google)** : Herramienta de Google para que los padres supervisen la actividad en línea de sus hijos.
- **Ciberbullying.org**: Página web que ofrece recursos y consejos sobre cómo lidiar con el ciberacoso.
- **Be Internet Awesome (Sé genial en Internet): Programa educativo de Google que enseña a los niños sobre seguridad en línea.**

Adoptar buenas prácticas desde una edad temprana es esencial para que los adolescentes puedan navegar por la red de manera

POLÍTICAS DE BUENA CONTRASEÑA.

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático
Una contraseña, clave o password es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa.

Una **contraseña segura** es una **contraseña** que otras personas no pueden determinar fácilmente adivinándola o utilizando programas automáticos

Los tipos de contraseña son:

Cadena de caracteres: son caracteres, números y símbolos que se utiliza para tener el acceso a un determinado lugar. Las contraseñas pueden ir de las más sencillas, como los tres números para acceder a ciertas plazas de garaje, hasta las más complicadas combinaciones de caracteres, números y símbolos que se recomienda emplear para proteger la información más sensible;
Cadena de caracteres más un token: En este nivel, los passwords requieren una cadena de caracteres, números y símbolos más un token o ficha de algún tipo. Un ejemplo típico es el de los cajeros automáticos. Para acceder a éstos se necesita una tarjeta y un número personal identificativo o PIN. Se consideran más robustos ya que si pierdes u olvidas alguno de los dos requerimientos tu acceso será denegado;
Password biométricos: Consisten en utilizar alguna característica física no reproducible, como las huellas digitales o el aspecto de la cara, para permitir el acceso. Un ejemplo es el escáner de retina en el cual el interior del ojo se fotografía para la posterior identificación del sujeto. La retina contiene un patrón único de distribución de vasos sanguíneos fácilmente apreciable y que se puede utilizar para la identificación del individuo

POLITICAS DE BUENA CONTRASEÑA.

1. Se deben utilizar al menos 8 caracteres para crear la clave.
2. Se recomienda utilizar en una misma contraseña dígitos, letras y caracteres especiales.
3. Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas. Hay que tener presente el recordar qué letras van en mayúscula y cuáles en minúscula;
4. Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado.
5. Las contraseñas hay que cambiarlas con una cierta regularidad. Un 53% de los usuarios no cambian nunca la contraseña salvo que el sistema le obligue a ello cada cierto tiempo.
6. Utilizar signos de puntuación si el sistema lo permite. P. ej.: “Tr-.3Fre”. En este caso de incluir otros caracteres que no sean alfa-numéricos en la contraseña, hay que comprobar primero si el sistema permite dicha elección y cuáles son los permitidos. Dentro de ese consejo se incluiría utilizar símbolos como: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
7. Existen algunos trucos para plantear una contraseña que no sea débil y se pueda recordar más fácilmente. Por ejemplo se pueden elegir palabras sin sentido pero que sean pronunciables, etc. Nos podemos ayudar combinando esta selección con números o letras e introducir alguna letra mayúscula.
Otro método sencillo de creación de contraseñas consiste en elegir la primera letra de cada una de las palabras que componen una frase conocida, de una canción, película, etc. Con ello, mediante esta sencilla mnemotecnia es más sencillo recordarla. Vg: de la frase “Comí mucho chocolate el domingo 3, por la tarde”, resultaría la contraseña: “cmCeD3-:xLt”. En ella, además, se ha introducido alguna mayúscula, se ha cambiado el “por” en una “x” y, si el sistema lo permite, se ha colocado algún signo de puntuación (-). Acciones que deben evitarse en la gestión de contraseña

ACCIONES QUE SE DEBE EVITAR EN LAS CONTRASEÑAS.

1. Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios. Por ejemplo, si se utilizan varias cuentas de correo, se debe recurrir a contraseñas distintas para cada una de las cuentas
2. No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento. Y, por supuesto, en ninguna ocasión utilizar datos como el DNI o número de teléfono;

3. Hay que evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”)
4. No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
5. Hay que evitar también utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.
6. No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.
7. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ej: no poner como contraseña apodos, el nombre del actor o de un personaje de ficción preferido, etc.).
8. No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio ordenador o dispositivo (ej: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto dentro del ordenador),
9. No se deben utilizar palabras que se contengan en diccionarios en ningún idioma. Hoy en día existen programas de ruptura de claves que basan su ataque en probar una a una las palabras que extraen de diccionarios: Este método de ataque es conocido como “ataque por diccionario”;
10. No enviar nunca la contraseña por correo electrónico o en un sms. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
11. Si se trata de una contraseña para acceder a un sistema delicado hay que procurar limitar el número de intentos de acceso, como sucede en una tarjeta de crédito y cajeros, y que el sistema se bloquee si se excede el número de intentos fallidos permitidos. En este caso debe existir un sistema de recarga de la contraseña o “vuelta atrás”.
12. No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas.
13. No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).
14. Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes.

LECTURA DE CRÓNICA DE UN PEQUEÑO ATAQUE

Yo no me considero confiado tratándose de seguridad informática. Siempre mantengo mis equipos libres de **virus** y **spyware**, tengo instaladas las últimas actualizaciones de sistemas operativos y aplicaciones, nunca utilizo equipos públicos ni ando navegando por los rincones más oscuros del internet. Y aun así hace algunos meses un anónimo hacker me dio un buen susto. Un día descubrí que alguien había entrado a una de mis cuentas de correo y que una vez adentro envió correos a toda mi lista de contactos para venderles a mi nombre no recuerdo qué producto, para luego finalizar con el borrado de esa lista de contactos a fin -supongo- de que yo no pudiera escribirles para advertirles del engaño.
Fue un ataque básico, casi infantil. Y digo ésto porque el atacante bien pudo haber causado daños mayores: aparte de haber podido borrarlo todo, pudo también haber robado mi identidad secuestrando mi cuenta; sólo tenía que cambiar la contraseña para lograrlo. En el perfil de mi cuenta de correo habían datos personales y entre ellos los nombres de otras cuentas de correo que también usaban la misma contraseña. Luego una búsqueda en Google pudo haberle revelado al atacante en qué redes sociales estoy inscrito. O bien, revisando mis correos recibidos en los que solicité la reposición de alguna contraseña pudieron darle los datos necesarios para saquear mi cuenta de Paypal, etc. El efecto dominó pudo ser devastador. Apenas me di cuenta de lo ocurrido, y de lo que aún podía ocurrir, procedí rápidamente a cambiar todas mis contraseñas.

CONTEXTUALIZACIÓN

Luego de leer los documentos y observar el video.

SE PUEDE HACER LA ACTIVIDAD EN PAREJAS

ACTIVIDAD 1:

Realice una presentación en prezi o genially del tema

Actividad 2:

Cree una historia donde se observe el uso inadecuado de la seguridad informática.

Subir las actividades a Classroom.

RÚBRICA. DE TECNOLOGÍA E INFORMÁTICA

Actividad tecnología e informática					
Aspectos a evaluar	ESCALA DE CALIFICACIÓN				
	4.6 a 5.0 Desempeño superior	4.0 a 4.5 Desempeño Alto	3.0 a 3.9 Desempeño Básico	1.0 a 2.9 Desempeño bajo	Porcentaje
Crea informes escritos con adecuada redacción, ortografía.	Elabora eficientemente escritos con adecuada redacción, ortografía donde se identifican el tema tratado	Elabora medianamente escritos con adecuada redacción, ortografía donde se identifican el tema tratado.	Elabora escritos con problemas de redacción, ortografía donde se identifican el tema tratado	Elabora con dificultad escritos con problemas de redacción, ortografía sin identificar el tema tratado	50%
Utiliza herramientas ofimáticas on-line	Domina y utiliza herramienta de manera elevada para la elaboración de presentaciones.	Domina y utiliza la herramienta de manera eficaz adecuada para la elaboración de presentaciones.	Domina y utiliza la herramienta para la elaboración de piezas graficas. presentaciones.	Presenta dificultades para utilizar la herramienta en la elaboración de presentaciones.	50%
Total					100%

Fuente

Tomado de:

https://www.youtube.com/watch?v=fiv71yqyVz0

https://chatgpt.com/c/670f115c-a3a4-8008-944b-1916e508813e