"Protegiendo tu vida digital: Creando espacios seguros en el ciberespacio"

"Si nuestro objetivo es proteger..."

Ingeniero Diego Armando Salazar Barrón

Presentación para sesión de seminario sobre violencia digital del Programa UNAMITA ¡Ciérrale a la brecha digital! 2023

El objetivo de proteger la vida digital es garantizar la seguridad y privacidad de la información y actividades en línea de las personas, así como proteger los dispositivos y sistemas digitales contra amenazas cibernéticas.

Esto implica la implementación de medidas de seguridad adecuadas para prevenir el acceso no autorizado, la divulgación indebida, la modificación o la destrucción de datos digitales.

Además, proteger la vida digital también implica educar a las personas sobre buenas prácticas de seguridad cibernética, fomentar la conciencia sobre la importancia de mantener ética en un ambiente digital.

OBJETIVOS

OBJETIVOS PARTICULARES

1. Garantizar la seguridad y privacidad de la información y actividades en línea de las personas.
2. Proteger los dispositivos y sistemas digitales contra amenazas cibernéticas.
3. Implementar medidas de seguridad adecuadas para prevenir el acceso no autorizado, divulgación indebida, modificación o destrucción de datos digitales.
4. Educar a las personas sobre buenas prácticas de seguridad cibernética.
5. Fomentar la conciencia sobre la importancia de mantener ética en un ambiente digital.
6. Conocer políticas y regulaciones que promuevan la protección de la vida digital, incluyendo la legislación y cumplimiento de normas de privacidad y seguridad.
7. Establecer programas de capacitación y concientización en seguridad cibernética dirigidos a diferentes grupos de usuarios, incluyendo a niños, jóvenes, adultos y personas mayores.
8. Promover la innovación en el desarrollo de soluciones y tecnologías seguras que protejan la vida digital de forma efectiva y sostenible.
9. Fomentar la participación activa de la sociedad civil en la promoción y defensa de la protección de la vida digital, incluyendo la colaboración con organizaciones y expertos en seguridad cibernética.

OBJETIVOS

DEFINICIONES

"No hay espacio que sea completamente seguro al 100%, pero podemos trabajar para tener un nivel de control adecuado."

ESPACIO SEGURO EN INTERNET

Firewall: Un firewall es una barrera de seguridad, ayuda a filtrar el tráfico de red no autorizado y protege contra posibles ataques desde el exterior.

Antivirus y antimalware: Los programas antivirus y antimalware ayudan a detectar, prevenir y eliminar software malicioso.

Actualizaciones de software y parches de seguridad: Mantener el software, aplicaciones y sistemas operativos actualizados con los últimos parches de seguridad es esencial para proteger la vida digital.

Contraseñas fuertes: El uso de contraseñas seguras y únicas es una práctica básica de seguridad cibernética.

Autenticación de dos factores: La autenticación de dos factores (2FA) añade una capa adicional de seguridad a las cuentas en línea. Con la 2FA habilitada, se requerirá un segundo factor de autenticación, como un código enviado a través de SMS o una aplicación de autenticación, además de la contraseña, para acceder a una cuenta.

DEFINICIONES

Copias de seguridad regulares: Realizar copias de seguridad periódicas de los datos importantes es una práctica esencial para proteger la vida digital.

Educación en seguridad cibernética: La concientización y educación en seguridad cibernética son fundamentales para proteger la vida digital.

Privacidad en redes sociales y ajustes de privacidad: Configurar adecuadamente la privacidad en las redes sociales y revisar regularmente los ajustes de privacidad en las cuentas en línea es importante para proteger la vida digital.

Análisis de seguridad y monitoreo: Implementar herramientas de análisis de seguridad y monitoreo para detectar posibles amenazas cibernéticas en tiempo real y tomar medidas adecuadas para mitigarlas.

Respaldo de información sensible: En caso de tener información sensible o valiosa en dispositivos digitales, es recomendable realizar respaldos de esa información en lugares seguros y fuera de línea, como discos duros externos o servicios de almacenamiento en la nube cifrados.

DEFINICIONES

RIESGOS Y AMENAZAS

“La dependencia excesiva de la tecnología y la conexión constante a internet también plantean preocupaciones sobre la adicción digital y la pérdida de privacidad."

ESPACIO SEGURO EN INTERNET

Ciberacoso o Ciberbullying:
Publicación de textos, imágenes, videos o audios que son compartidos por medios sociales, mensajes de texto, juegos en línea para agredir o humillar a alguien.

Grooming:
Acción deliberada por una persona adulta, la cual contacta a un niño, niña o adolescente a través de los medios electrónicos para ganar su confianza y con ello obtener videos o imágenes de carácter sexual.

Sexting:
Se refiere al uso de fotografías y/o videos producidos por uno mismo de connotación sexual y enviado a otras personas. Dicho material puede ser utilizado como un atacante para extorsionar a la víctima, para obtener más material de esta connotación y con ello nos lleva a lo que llamamos Sextorsión.

Ataques de ingeniería social: Los ataques de ingeniería social implican manipular psicológicamente a las personas para obtener información confidencial o acceso a sistemas o cuentas, a menudo a través de técnicas de manipulación o persuasión.

RIESGOS Y AMENAZAS

Redes Wi-Fi públicas no seguras: El uso de redes Wi-Fi públicas no seguras, como las disponibles en cafeterías, aeropuertos o lugares públicos, puede ser riesgoso, ya que los datos transmitidos a través de estas redes pueden ser interceptados y comprometer la privacidad y seguridad del usuario.

Descargas de archivos no seguros: Descargar archivos, programas o software de fuentes no confiables o desconocidas puede exponer los dispositivos a malware y otros programas maliciosos que pueden dañar o comprometer la seguridad del sistema.

Robo de identidad: El robo de identidad implica el uso no autorizado de la información personal de alguien para cometer fraude, como abrir cuentas bancarias, realizar compras en línea o cometer otros delitos cibernéticos.

Exposición no intencionada de archivos sensibles: Si se comparten enlaces públicos de archivos almacenados en la nube de manera inadvertida o inapropiada.
El uso de servicios de almacenamiento en la nube, como Dropbox, Google Drive o Microsoft OneDrive, MEGA, etc.

RIESGOS Y AMENAZAS

Phishing: Es una forma de ataque cibernético en la que los delincuentes se hacen pasar por una entidad confiable, como una empresa, una organización o una persona, para obtener información confidencial del usuario, como contraseñas, números de tarjeta de crédito o datos personales. Los ataques de phishing suelen realizarse a través de correos electrónicos, mensajes de texto o sitios web falsificados.

Malware: Es un software malicioso que se instala en los dispositivos del usuario sin su consentimiento, con el objetivo de dañar, robar información o comprometer la seguridad del sistema.

Suplantación de identidad o "pharming": Redirigen el tráfico de Internet para redirigir a los usuarios a sitios web falsificados con el objetivo de robar información personal o financiera.

Fuga de información: Se refiere a la pérdida no autorizada de información sensible o confidencial del usuario.

Uso inapropiado de redes sociales: Esto incluye la publicación imprudente de información personal o confidencial en redes sociales, la revelación de detalles de ubicación o planes de viaje, la aceptación de solicitudes de amistad o interacción con personas desconocidas, y la exposición a contenido inapropiado o peligroso.

CREA UN ESPACIO SEGURO PARA NIÑOS Y NIÑAS

“Velar por la seguridad de los niños, niñas y adolescentes durante su navegación en internet, mediante la implementación de medidas de seguridad apropiadas."

ESPACIO SEGURO EN INTERNET

El control parental es una herramienta útil para ayudar a minimizar los riesgos que pueden enfrentar las niñas, niños y adolescentes en la Internet pero no son 100% efectivos.

Otras recomendaciones:
Verificar que el dispositivo cuente con las ultimas actualizaciones tanto en el sistema operativo como en sus aplicaciones.

Cubrir o apagar cámaras web cuando no las estén utilizando.

La cuenta del niño no debe de ser personal, es muy útil generar una cuenta que el padre, madre o tutor pueda administrar y con la cual pueda tener el control sobre las configuraciones, contraseñas, datos de la cuenta, así como evitar tener datos personales (dirección real, número de teléfono, o señas muy particulares).

Enseñar al niño sobre los riesgos y amenazas que pueden existir en la red y como evitarlos.

Usar un bloqueador de anuncios (Ublock Origin) y navegador como Brave para evitar los anuncios que puedan generarse de índole sexual, violencia, etc.

RECOMENDACIONES ADICIONALES

Advertir al niño, niña o adolescente sobre los riesgos de compartir fotografías, número de teléfono, dirección del domicilio, país, ciudad o cualquier información personal o de su familia.

Comentar los riesgos de estar en altas horas de la noche, se tienen estadísticas que depredadores sexuales utilizan horas de la madrugada para contactar a niños, niñas y adolescentes.
Sextorsión: Es más común de lo que cree | ICE

Prevenirles sobre los delitos que se comenten a través de la Internet, sobre todo de la suplantación de identidades para que estén alertas al momento que reciben solicitudes de amistad.

Detén la sextorsión | Consejos para compañías tecnológicas (detenlasextorsion.org)

RECOMENDACIONES ADICIONALES

CREA TU ESPACIO SEGURO

“La concientización sobre la seguridad en línea es esencial para promover un espacio seguro en internet, educando a los usuarios sobre los riesgos y cómo protegerse.”

ESPACIO SEGURO EN INTERNET

Algunas sugerencias para crear un espacio seguro digital incluyen:

- Promover la conciencia sobre la privacidad y la seguridad en línea, educando a los usuarios sobre las mejores prácticas para proteger su información personal y evitar riesgos en línea.

- Fomentar una cultura de respeto y tolerancia en línea, promoviendo la empatía, el respeto a la diversidad y el diálogo constructivo, y abordando temas como el ciberacoso, el discurso de odio y la discriminación en línea.

- Proporcionar recursos de apoyo en línea, como líneas de ayuda o chats de apoyo emocional, para aquellos que necesiten ayuda o asesoramiento en situaciones difíciles o de crisis.

- Realizar actualizaciones y mejoras constantes para mantener la seguridad y la privacidad de los usuarios, así como estar atentos a las necesidades y preocupaciones de los adolescentes y adultos en el entorno digital.

SUGERENCIAS

Es importante recordar que la seguridad en línea es un proceso continuo y requiere de esfuerzos constantes para adaptarse a los cambios en la tecnología y en el comportamiento en línea. es esencial establecer políticas y normas claras sobre el uso responsable de la tecnología, tanto a nivel individual como familiar o comunitario.

Finalmente, es importante considerar la colaboración con expertos en seguridad en línea, organizaciones dedicadas a la protección de los derechos digitales y entidades gubernamentales para obtener orientación y recursos actualizados en la creación de un espacio seguro digital para adolescentes y adultos.

SUGERENCIAS

APLICACIONES

Microsoft Family Safety: Es una aplicación de control parental que permite a los padres supervisar y controlar el acceso a Internet de sus hijos, establecer límites de tiempo, bloquear sitios web inapropiados y rastrear la actividad en línea.

AppLock: Es una aplicación de bloqueo de aplicaciones que permite a los adolescentes y jóvenes proteger sus aplicaciones con contraseña o huella digital, evitando el acceso no autorizado a sus aplicaciones y datos personales.

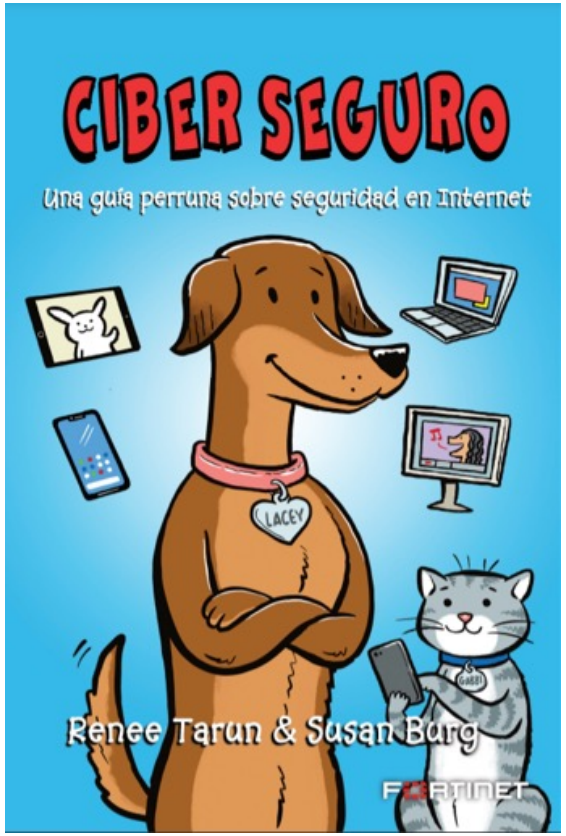
Signal: Es una aplicación de mensajería cifrada que ofrece un alto nivel de seguridad y privacidad en las comunicaciones en línea, protegiendo los mensajes y llamadas de ser interceptados o espiados por terceros.

Nordpass: Es una aplicación de gestión de contraseñas que ayuda a crear contraseñas seguras y únicas para cada cuenta en línea, evitando el uso de contraseñas débiles o repetidas y protegiendo la información de inicio de sesión.

Aplicaciones para un espacio seguro

Microsoft Authenticator: Autenticación de dos factores para cuentas en línea y servicios compatibles.
Google Find My Device: Rastreo y localización de dispositivos Android perdidos o robados.
Prey Antirrobo: Protección antirrobo para dispositivos móviles con funciones de rastreo, bloqueo y borrado remoto.
1.1.1.1: Faster & Safer Internet: Aplicación de DNS para una navegación más rápida y segura en Internet.
Firefox Focus: Navegador de privacidad con bloqueo de rastreadores y eliminación automática de datos.
Brave: Navegador web con enfoque en la privacidad, bloqueo de anuncios y recompensas de tokens.
iShredder Android 6: Herramienta de eliminación segura de datos para dispositivos Android, borrado irreparable de archivos.
Micro Guard Android 5: Protección de privacidad para micrófono y cámara en dispositivos Android, bloqueo de acceso no autorizado.
Camera Guard Android 6: Protección de privacidad para la cámara en dispositivos Android, evita el acceso no autorizado.

REFERENCIAS



http://dgos.xyz/7eh57n

https://global.fortinet.com/latam-lp-es-cibersafe

REFERENCIAS

is4k INTERNET SEGURA FORKiDS	https://www.is4k.es/
Controles parentales y guía didácticas 1 y 2.	http://dgos.xyz/g2mrdt
Prácticas, dinámicas para trabajar en el aula, sobre el uso seguro y responsable de internet.	http://dgos.xyz/95ge6a
Guía sobre el uso de controles parentales	

REFERENCIAS

https://www.is4k.es/

Guía SOS contra el Ciberacoso para Educadores

Se trata de un recurso elaborado por INCIBE-Red.es que explica cómo se debe actuar en los centros educativos ante situaciones de ciberacoso entre alumnos: cómo detectarlo, valorarlo y plan de actuación son algunos de los aspectos que recoge la guía.

http://dgos.xyz/4lpmrq

REFERENCIAS

https://www.incibe.es/

INSTITUTO NACIONAL DE CIBERSEGURIDADINCIBE TRABAJA PARA AFIANZAR LA CONFIANZA DIGITAL, ELEVAR LA CIBERSEGURIDAD Y LA RESILIENCIA Y CONTRIBUIR AL MERCADO DIGITAL DE MANERA QUE SE IMPULSE EL USO SEGURO DEL CIBERESPACIO EN ESPAÑA.

REFERENCIAS