



DC/SECURE

CATEGORÍA RETO

APP DE CYBERSEGURIDAD

EQUIPO:

- ESCOVEDO MONTENEGRO, YULIAN MABEL
- MORENO YAMO, FABIOLA MILENE
- VERA LEYVA, LAZLO ANTHONY

DOCENTE:

- SÁNCHEZ ORDÓÑEZ, CARLOS MARTÍN



INTRODUCCIÓN

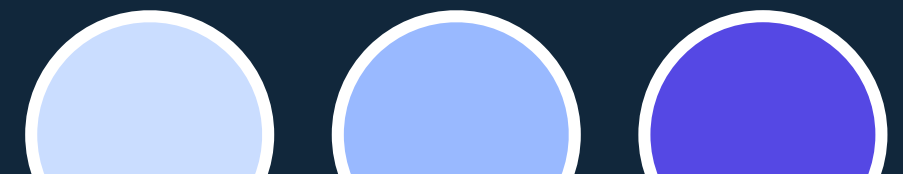
La inseguridad en la ciudadanía digital se refiere a la exposición a amenazas y riesgos en el entorno digital que pueden afectar negativamente a individuos, comunidades y sociedades. Estas amenazas incluyen el robo de información personal y financiera, el ciberacoso, el fraude y las estafas online, el discurso de odio y la adicción a las tecnologías. Las consecuencias de esta inseguridad pueden ser graves e incluyen daños económicos, psicológicos y a la reputación, exclusión social y pérdida de confianza.





JUSTIFICACIÓN

Existe una preocupación generalizada sobre la seguridad en línea, con un porcentaje significativo de personas que han experimentado problemas de seguridad en línea en algún momento. Además, se observa una diversidad de opiniones en cuanto a las medidas adicionales necesarias para mejorar la seguridad digital, destacando la necesidad de una mayor educación en seguridad digital y la implementación de medidas de autenticación de dos factores como posibles soluciones. Esto sugiere que la ciudadanía digital todavía enfrenta desafíos significativos en términos de proteger la información personal y mantenerse segura en el entorno digital.





PÚBLICO OBJETIVO



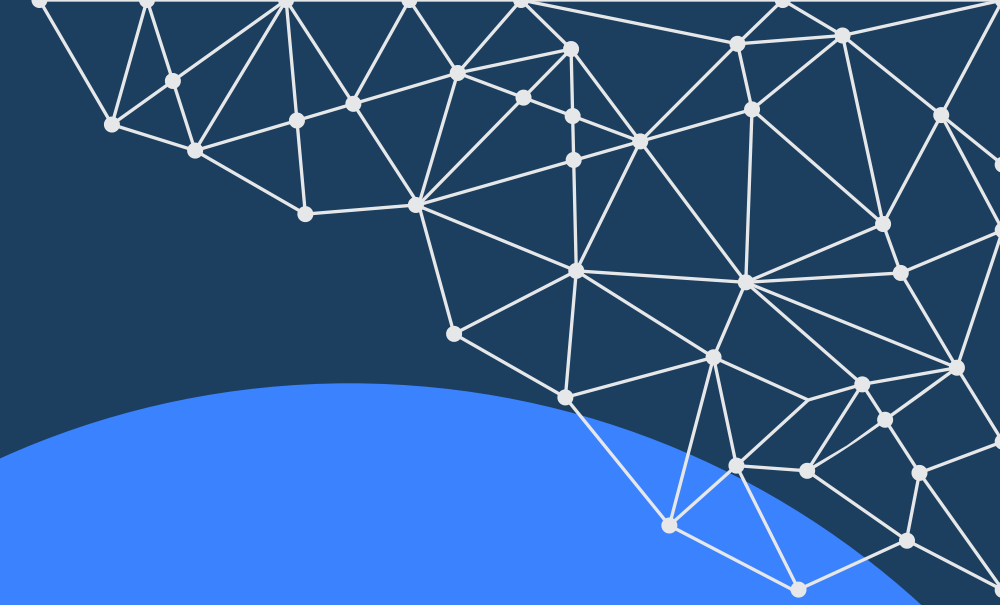
Grupos vulnerables por desconocimiento del mundo digital que enfrentan riesgos como el ciberacoso y fraudes.

OBJETIVO



Fortalecer la seguridad y confianza de los usuarios en el entorno digital al proporcionar herramientas integrales de seguridad, educación sobre riesgos en línea, apoyo a las víctimas y facilitar la presentación de denuncias en casos de incidentes.





PROBLEMA

EMPATIZAR

Elaboramos encuestas, observamos la realidad y conversamos con nuestros compañeros para definir el problema.

DEFINIR

A través de una lluvia de ideas definimos la propuesta de solución según el problema identificado.

IDEAR

Diseñamos la propuesta de solución según lo que analizamos e identificamos.

La creciente dependencia de la tecnología y la falta de medidas adecuadas de seguridad aumentan la exposición a riesgos en línea, como el robo de datos y el fraude. Esto subraya la necesidad urgente de fortalecer la seguridad digital para proteger a los usuarios. El problema se define como la vulnerabilidad de los individuos y la información personal en el entorno digital debido a la falta de medidas de seguridad adecuadas. Esto incluye amenazas como el robo de datos, el fraude en línea y la exposición a contenido dañino.





PROPUESTA

APP PARA CYBERSEGURIDAD: "DC/SECURE"
¡Protegiendo lo que más importa!

EL APLICATIVO PROPUESTO ACTÚA COMO UN ESCUDO DIGITAL PARA COMBATIR LA INSEGURIDAD EN LA CIUDADANÍA DIGITAL.

- Ha sido diseñado para reforzar el área de ciberseguridad de la policía nacional.
- Este aplicativo es descargable en dispositivos móviles y permite la vinculación con hasta tres dispositivos para acciones remotas en caso de robo o pérdida.
- Protege tu dispositivo de virus y malware.
- Brinda acceso a información sobre qué aplicaciones están instaladas y te permite escanear archivos en busca de problemas de seguridad.
- Para vincular un dispositivo a otro en nuestra app: Debes ir a la sección "Dispositivos Vinculados". seleccionas "agregar un nuevo dispositivo". Luego, ingresa tu contraseña para confirmar que eres tú. Una vez hecho esto, recibirás un mensaje de confirmación. ¡Y listo! dispositivo vinculado. Revisa tus notificaciones para saber que todo fue exitoso.
- Para hacerlo, Activas la aplicación como "administrador del dispositivo" desde los ajustes de seguridad, otorgando los permisos necesarios. Puedes rastrear el tiempo de actividad de las aplicaciones y compararlo con los límites configurados.
- También te ofrecemos un tutorial de configuración, visualización de uso de los dispositivos e informes para entender mejor los hábitos de uso.

¿CÓMO HAGO PARA DESVINCULAR MI DISPOSITIVO EN SITUACIONES DE UN RIESGO DIGITAL?

1. Debes ir a la sección "Dispositivos Vinculados" para gestionar los dispositivos controlados por el usuario.
2. Para la autenticación de seguridad requerimos contraseña o PIN para iniciar el proceso de desvinculación, y verificación adicional para confirmar la identidad del usuario.
3. En la confirmación y ejecución, solicitamos la aprobación del usuario y luego desvinculamos el dispositivo seleccionado, eliminando todas las configuraciones asociadas con operaciones de desvinculación.
4. Para la recuperación y seguridad adicional ofrecemos la opción de volver a vincular dispositivos previamente

