Universidad Internacional del Ecuador

Comunicación y Medios Digitales

Autor:

Hachig Zapata Diego Alexander

Materia:

LOGICA DE PROGRAMACION 1-ECC-1D

Fecha de entrega:

Domingo, 29 de junio de 2025

PROYECTO INTEGRADOR

a. Proyecto Generador de Contraseñas

Un programa generador de contraseñas puede tener un impacto significativo en las nuevas tecnologías y en la sociedad, especialmente si lo visualizamos en un futuro donde la ciberseguridad es aún más crítica. Presento una visión estructurada de cómo podría influir:

Impacto en las Nuevas Tecnologías

Seguridad Digital Avanzada

Los generadores de contraseñas inteligentes, integrados con IA, podrían crear contraseñas únicas, complejas y adaptativas que cambien automáticamente según el nivel de amenaza detectado.

Esto fortalecería la protección de datos en tecnologías emergentes como el Internet de las Cosas (IoT), blockchain y sistemas de identidad digital.

Integración con Biometría y Autenticación Multifactor (MFA)

En el futuro, los generadores podrían trabajar junto con sistemas biométricos para crear contraseñas temporales que solo se activen con la presencia del usuario autorizado.

Automatización y Gestión de Identidades

En entornos corporativos, estos programas podrían integrarse con plataformas de gestión de identidades para asignar contraseñas seguras automáticamente a nuevos empleados o dispositivos.

Impacto en la Sociedad

Conciencia y Educación en Ciberseguridad

El uso generalizado de generadores de contraseñas podría fomentar una cultura de seguridad digital desde edades tempranas, integrándose en la educación básica.

Reducción del Cibercrimen

Al dificultar el acceso no autorizado a cuentas personales y corporativas, se reducirían los ataques de phishing, ransomware y robo de identidad.

Inclusión Digital

Con interfaces accesibles y multilingües, estos programas podrían ayudar a personas mayores o con poca experiencia tecnológica a protegerse en línea.

Visualización del Futuro

Imagina un mundo donde:

Cada dispositivo tiene un generador de contraseñas integrado por defecto.

Las contraseñas ya no se recuerdan, sino que se gestionan de forma segura y automática.

La identidad digital está protegida por capas de seguridad invisibles pero robustas, impulsadas por IA.

b. Descripción general del problema o la situación que busca atender el proyecto, acorde al objetivo de la asignatura.

En la actualidad, el crecimiento acelerado de las tecnologías digitales ha transformado profundamente la forma en que las personas interactúan, trabaja, estudian y acceden a la información. Sin embargo, este avance también ha traído consigo nuevos desafíos, especialmente en el ámbito de la seguridad digital. Uno de los problemas más comunes y persistentes es el uso de contraseñas débiles o repetidas, lo que expone a los usuarios a riesgos como el robo de identidad, el acceso no autorizado a cuentas personales y la pérdida de información sensible.

A pesar de la disponibilidad de herramientas tecnológicas para mejorar la seguridad, muchas personas aún no adoptan buenas prácticas digitales, ya sea por desconocimiento, desconfianza o falta de educación en ciberseguridad. Esta situación evidencia una brecha entre el desarrollo tecnológico y su apropiación consciente por parte de la sociedad.

Propósito del Proyecto

Este proyecto busca que las personas desarrollen una visión crítica y propositiva sobre el uso de las nuevas tecnologías, a través del diseño y análisis de un generador de contraseñas seguras. La intención es que comprendan cómo una herramienta aparentemente simple puede tener un impacto significativo en la protección de la información personal y colectiva, y cómo su implementación puede contribuir a una sociedad más segura y digitalmente responsable.

c. Propósito del proyecto.

El propósito de este proyecto es visualizar el impacto de las nuevas tecnologías en la sociedad y fomentar en las personas una reflexión crítica sobre su potencial futuro. A través del análisis y desarrollo de una herramienta tecnológica —como un generador de contraseñas seguras— se busca que los estudiantes comprendan cómo las innovaciones digitales pueden influir en la vida cotidiana, la seguridad de la información y la transformación social.

Este ejercicio permitirá a los estudiantes no solo adquirir conocimientos técnicos, sino también desarrollar una conciencia ética y responsable sobre el uso de la tecnología, preparándolos para enfrentar los desafíos del mundo digital de manera informada y proactiva.

d. Instrucciones para el desarrollo del proyecto.

CRONOGRAMA GENERADOR DE CONTRASEÑAS

Actividad Principal	Descripción
Investigación y análisis	Investigar tipos de diagramas funcionales y arquitecturas de software. Seleccionar el tipo de software (generador de contraseñas) y definir el problema a resolver.
Diseño funcional y arquitectónico	Diseñar funcionalidades del generador de contraseñas. Crear diagramas de casos de uso y seleccionar la arquitectura adecuada.
Configuración del entorno	Configurar entorno de desarrollo (por ejemplo, Python + GitHub). Crear repositorio y preparar herramientas necesarias.
Inicio de codificación	Iniciar codificación del sistema base. Crear interfaz básica y lógica para generación de contraseñas.
Desarrollo de funcionalidades	Implementar estructuras lógicas: longitud, complejidad, caracteres especiales, etc.
Optimización y documentación	Agregar comentarios, validar entradas, mejorar la experiencia de usuario.
Programación funcional y revisión	Aplicar técnicas de programación funcional si es posible. Participar en revisión de código con compañeros.
Presentación del proyecto	Preparar documentación, video o presentación. Entregar el generador de contraseñas funcional y bien documentado.