

# Riesgos y Amenazas en la Seguridad Web

Alexys Gomez Elizalde

## Pregunta a ChatGPT4

Si fueras una persona, ¿qué vulnerabilidad crees que sea la que mas comúnmente cometerías y qué harías para evitarlo? Da una explicación larga y creativa

## Respuesta de ChatGPT4

A continuación se pondrá la respuesta que chatGPT4 nos dio y además le pedi que la escribiera en latex para hacer un copiar y pegar:

Si fuera una persona navegando por la web y gestionando mi propia seguridad, la vulnerabilidad más común que probablemente cometería sería **el uso de contraseñas débiles o repetidas**. Este tipo de vulnerabilidad es muy común porque, como persona, es fácil caer en la comodidad de usar una contraseña simple y conocida en múltiples cuentas para no tener que recordar una lista interminable de combinaciones complejas.

## Escenario: ¿Cómo sucedería?

Imagina que estoy constantemente registrándome en nuevas aplicaciones, redes sociales y servicios de compras en línea. Mi vida es un constante ir y venir entre diferentes plataformas, y cada una de ellas me pide una contraseña. Como soy una persona ocupada, comienzo a caer en la trampa de utilizar contraseñas sencillas como 123456 o mi nombre y fecha de nacimiento. Más tarde, con algo de "inspiración creativa", podría añadir un signo de exclamación al final, pensando que eso es suficiente. Y claro, utilizo esa misma contraseña para mis cuentas de correo, redes sociales y hasta mi banco, porque, ¿quién tiene tiempo para recordar varias contraseñas, verdad?

Lo que no me doy cuenta es que un **ataque de fuerza bruta** o un simple ataque de **phishing** podría exponer mis credenciales. Un ciberdelincuente podría acceder a una de mis cuentas más débiles y, si yo he utilizado la misma contraseña en diferentes plataformas, automáticamente tendría acceso a todas mis otras cuentas. Así, una vulnerabilidad aparentemente pequeña podría desencadenar un colapso total de mi privacidad y seguridad en línea.

## Cómo evitarlo

Para corregir esta debilidad, lo primero que haría sería implementar un **gestor de contraseñas**. Este tipo de software me permitiría crear contraseñas largas y únicas para cada cuenta, que no necesitaría recordar porque el gestor las almacenaría por mí. De esa manera, todas mis contraseñas serían diferentes y extremadamente difíciles de adivinar, protegiéndome del riesgo de reutilización.

Además, comenzaría a practicar algo llamado **autenticación multifactor (MFA)**. Esto implica que, incluso si un atacante consigue mi contraseña, necesitaría un segundo nivel de verificación para acceder a mi cuenta. Podría usar mi teléfono móvil para recibir un código temporal, o incluso una aplicación como *Google Authenticator*.

## Ejemplo de cómo cambiaría mi enfoque

**Antes:** Mi contraseña para casi todo era algo simple como P@ssword123! y la usaba en mi correo, redes sociales y hasta en mi cuenta bancaria.

**Después:** Con un gestor de contraseñas, mi nueva contraseña para una red social sería algo como `m73#eS2!kT84zCp9nL`, mientras que mi cuenta bancaria tendría otra completamente diferente generada aleatoriamente. Ninguna contraseña se repetiría, y solo necesitaría recordar una **contraseña maestra** para el gestor de contraseñas.

También me comprometería a **actualizar mis contraseñas** regularmente, algo que muchas personas olvidan hacer. Y si alguna de mis cuentas se viera comprometida, gracias a las contraseñas únicas, los daños estarían contenidos, ya que el atacante no podría usar esa misma contraseña en otro lugar.

## Reflexión

En el fondo, la clave es reconocer que *la comodidad es el enemigo de la seguridad*. Como persona, es natural buscar atajos, pero en el mundo digital esos atajos pueden abrir la puerta a amenazas devastadoras. Así que, mientras antes prefería contraseñas fáciles por conveniencia, mi enfoque ahora sería de **proactividad y responsabilidad** en la protección de mi información.

Optaría por estar siempre **vigilante y educado en cuanto a las mejores prácticas de seguridad**. Esto incluiría mantener mi software y dispositivos actualizados con los últimos parches de seguridad, porque no solo las contraseñas importan; una vulnerabilidad en el software que uso también podría comprometerme.

Así, con esta nueva mentalidad, me aseguraría de no caer en la trampa de la facilidad y protegería mis datos de la forma en que lo haría un verdadero profesional de la seguridad.

## Evaluación

La respuesta de ChatGPT es bastante buena y completa, supero mis expectativas. Yo creo que al poner en el prompt que "si fueras una persona" y pedirle la explicación larga y creativa hizo que la respuesta se potenciara y tuviera esos toques de lenguaje informal en el texto y de imaginación, ya que menciona lo escribió como si se estuviera imaginando que es una persona. Sobre el aprendizaje creo que si se puede aprender sobre ciertos temas, en este caso, el tema es amplio y se habla bastante por lo que creo que tiene una amplia información a su alcance para poder realizar respuestas reales, útiles y educativas. Sin embargo sé que hay temas en los que aun no se puede confiar, como en las matematicas, que cuentas bastante sencillas, como una suma o una resta, se pueden poner bastante feas para este tipo de chatbots. Volviendo a este tema su respuesta me gusto ya que explica bien el cómo evitarlo y el como piensa en hacer el cambio para mejorar esa vulnerabilidad.