# CONSEJOS CIBERSEGURIDAD APLICACIÓN WEB
## DESAFÍO DE TRIPULACIONES

Pablo primo, Claudio Haraba, Christian de López y Adrian Pascual
CIBERSEGURIDAD

### Implementación cabecera de seguridad

La cabecera de seguridad se implementa para prevenir la ejecución de scripts externos en la aplicación web.

**Ataques de inyección:** Las cabeceras de seguridad pueden proteger contra ataques de inyección de código, como el SQL injection o el Cross-Site Scripting (XSS), al garantizar que los datos recibidos estén correctamente validados y escapados.
**Ataques de repetición:** Las cabeceras de seguridad pueden incluir mecanismos de prevención de ataques de repetición, como el uso de tokens CSRF (Cross-Site Request Forgery) para evitar que se realicen acciones no deseadas en nombre del usuario.
**Ataques de denegación de servicio (DoS) y distribuidos (DDoS):** Pueden ayudar a detectar y mitigar ataques DoS y DDoS, identificando patrones de tráfico anómalos o implementando listas negras y listas blancas para filtrar direcciones IP sospechosas.
**Falsificación de identidad (Spoofing):** Al incluir información sobre la identidad del remitente en las cabeceras de seguridad, es posible evitar la falsificación de identidad y garantizar que solo las comunicaciones auténticas sean aceptadas.
**Ataques de fuerza bruta:** Pueden implementar políticas de bloqueo temporal después de varios intentos fallidos de autenticación para proteger contra ataques de fuerza bruta.
**Ataques de intermediario (MitM:** Mediante el uso de cifrado y autenticación, las cabeceras de seguridad pueden proteger contra ataques en los que un atacante intenta interceptar y manipular la comunicación entre dos partes.
**Exposición de información sensible:** Las cabeceras de seguridad pueden proteger la información sensible mediante técnicas de cifrado y asegurarse de que no se exponga inadvertidamente en la comunicación.

- Opción: “Content-Security-Policy” Cabecera de seguridad utilizada en aplicaciones web para mitigar y prevenir ciertos tipos de ataques. Esta cabecera se implementa en las respuestas HTTP enviadas por el servidor web y le indica al navegador qué fuentes de contenido pueden ser cargadas y ejecutadas en la página.

### Política de contraseñas

La política de contraseñas se establece para evitar ataques de command injection y garantizar una mayor seguridad en las credenciales de acceso. Los requisitos incluyen:

**Nombre de usuario:** Distingue entre mayúsculas y minúsculas, y solo admite letras.

**Contraseña:** 8 caracteres, incluyendo minúsculas, mayúsculas y al menos un carácter especial que no coincida con el nombre de usuario.