# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| * **Firewall**: Un firewall es un dispositivo o programa que filtra el tráfico de red y permite o bloquea el acceso a los recursos según unas reglas predefinidas. Un firewall puede ayudar a proteger el sistema de ataques externos, como escaneos de puertos, denegación de servicio o intrusiones. * **Antivirus**: Un antivirus es un software que detecta y elimina virus, malware, spyware y otras amenazas informáticas. Un antivirus puede ayudar a prevenir la infección del sistema, el robo de datos, el daño a los archivos o el secuestro de recursos. * **Actualización de software**: La actualización de software consiste en instalar las últimas versiones de los programas y sistemas operativos que se utilizan en el sistema. La actualización de software puede ayudar a corregir vulnerabilidades, errores, fallos o incompatibilidades que podrían ser explotados por los atacantes. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Una de las técnicas de reforzamiento de la seguridad que recomendaría para evitar que el incidente de fuerza bruta vuelva a ocurrir en el futuro es la instalación de un firewall. Un firewall es un dispositivo o programa que filtra el tráfico de red y permite o bloquea el acceso a los recursos según unas reglas predefinidas. Un firewall puede ayudar a proteger el sistema de ataques externos, como escaneos de puertos, denegación de servicio o intrusiones.  La técnica de reforzamiento de la seguridad recomendada es eficaz porque:   * Impide que el atacante pueda enviar múltiples solicitudes HTTP al servidor web desde una misma dirección IP, lo que dificulta el adivinar la contraseña por fuerza bruta. * Detecta y alerta de cualquier actividad sospechosa o anormal en la red, lo que permite tomar medidas correctivas de forma rápida y oportuna. * Permite configurar las reglas de acceso según las necesidades y los riesgos de cada sistema, lo que mejora la seguridad y el rendimiento de la red.   La técnica de reforzamiento de la seguridad debe aplicarse de forma continua y periódica, ya que:   * Los ataques informáticos son cada vez más sofisticados y variados, lo que requiere una actualización constante de las reglas y los parámetros del firewall. * Los sistemas y las redes pueden cambiar o evolucionar con el tiempo, lo que implica una revisión y una adaptación frecuente de las medidas de seguridad. * Los firewalls pueden tener fallos o vulnerabilidades, lo que exige una supervisión y un mantenimiento regulares para garantizar su correcto funcionamiento. |