# Informe de evaluación de riesgos de seguridad

|  |
| --- |
| **Parte 1: Seleccione hasta tres herramientas y métodos de endurecimiento para implementar** |
|  |
|

|  |  |  |
| --- | --- | --- |
| **Tarea de refuerzo de la seguridad** | **Descripción** | **Usos comunes** |
| Mantenimiento del cortafuegos | El mantenimiento del cortafuegos implica comprobar y actualizar las configuraciones de seguridad con regularidad para adelantarse a las posibles amenazas. | Esto puede suceder regularmente. Las reglas de firewall se pueden actualizar en respuesta a un evento que permita un tráfico de red anormal en la red. Esta medida se puede utilizar para protegerse contra varios ataques DDoS. |
| Autenticación multifactor (MFA) | Una medida de seguridad que requiere que un usuario verifique su identidad de dos o más maneras para acceder a un sistema o red. Las opciones de MFA incluyen una contraseña, un número PIN, una credencial, una contraseña de un solo uso (OTP) enviada a un teléfono móvil, una huella dactilar y mucho más. | Puede ayudar a protegerse contra ataques de fuerza bruta y eventos de seguridad similares. MFA se puede implementar en cualquier momento, y es principalmente una técnica que se configura una vez que luego se mantiene. |
| Privilegios de acceso a la red | Los privilegios de acceso a la red implican permitir, limitar y/o bloquear privilegios de acceso a los activos de la red para personas, roles, grupos, direcciones IP, direcciones MAC, etc. | Reduce el riesgo de que usuarios no autorizados y tráfico externo accedan a la red interna. Esto se puede implementar una vez, o volver a revisarlo dependiendo de la probabilidad de ingeniería social o ataques de fuerza bruta. |
| Políticas de contraseñas | Las últimas recomendaciones del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) para las políticas de contraseñas se centran en el uso de métodos para sal y hash de contraseñas, en lugar de requerir contraseñas demasiado complejas o imponer cambios frecuentes en las contraseñas. | Las políticas de contraseñas se utilizan para evitar que los atacantes adivinen fácilmente las contraseñas de los usuarios, ya sea manualmente o mediante el uso de un script para intentar miles de contraseñas robadas (comúnmente llamado ataque de fuerza bruta). |

|  |
| --- |
| **Parte 2: Explica tus recomendaciones** |
| Es importante establecer una Política de contraseñas para que los atacantes no les sea fácil acceder al sistema ya que actualmente la empresa no cuenta con esta política esto en conjunto con la Autenticación multifactor ayudará de disminuir los futuros ataques o amenazas.  Además, se recomienda mantener los cortafuegos actualizados para evitar el tráfico de red anormal y se evitará que el servidor se bloquee. |