**Incidentes de ciberseguridad**

# Análisis de riesgos

# 

# Índice

[**Análisis de riesgos 1**](#_n6arwwmay01c)

[**Índice 2**](#_z77repcs18xk)

[**Introducción 4**](#_mxalo06ha5c8)

[**Activos 4**](#_ox8un2qxixq3)

[Hardware 4](#_wpno7qr0w6v8)

[Software 5](#_qj7o5kr4xc5)

[Humanos 6](#_psj0u5bxaex3)

[**Análisis 6**](#_wsgjyslwni2w)

[Activo 1 6](#_n09566mvlhtf)

[Amenazas 6](#_dau9drpi1wr5)

[Vulnerabilidades 7](#_fftbuvaaanv5)

[Activo 2 8](#_x6kr1qj7ggfy)

[Amenazas 8](#_wpla4xv2rev6)

[Vulnerabilidades 8](#_wpla4xv2rev6)

[Activo 3 9](#_uw77qyqzqlt3)

[Amenazas 9](#_vzp7i5q0tjrw)

[Vulnerabilidades 10](#_ljpc9057z0wf)

[Activo 4 10](#_wk8uiqof0kdk)

[Amenazas 11](#_z8z4p4t0nsnw)

[Vulnerabilidades 11](#_5e8aa198pcmy)

[Activo 5 12](#_binhbpjcdyq0)

[Amenazas 12](#_smkhh8gzznlv)

[Vulnerabilidades 12](#_smkhh8gzznlv)

[**Medidas generales de mitigación 13**](#_4lmsnasxr665)

[Recomendaciones generales para los routers 13](#_smkhh8gzznlv)

[**Análisis de Riesgo 14**](#_qvyswcst1ser)

[Activo 1 17](#_p4xa9ya6j9nf)

[Activo 2 18](#_i6g84yjjgtdf)

[Activo 3 20](#_912p0z47yg42)

[Activo 4 22](#_kopozepmh2z)

[Activo 5 25](#_nx1s8j776jbd)

# Introducción

En este documento se llevará a cabo el análisis de activos empresariales definiendo sus amenazas y vulnerabilidades.

Seguido a esto, se evaluará el nivel de riesgo siguiendo la siguiente fórmula

**Riesgo = Nivel de amenaza \* Nivel de vulnerabilidad \* Nivel de impacto**

**R = A \* V \* I**

# Activos

## Hardware

| **Id** | **Nombre** | **Descripción** | **Responsable** | **Tipo** | **Ubicación** | **Crítico** |
| --- | --- | --- | --- | --- | --- | --- |
| 001 | R0 | Salida a internet | PINO | ROUTER | Sala administración | SI |
| 002 | R1 | Red administrativa | PINO | ROUTER | Sala administración | SI |
| 003 | R2 | Red personal | MANOLO | ROUTER | Zona Restauración | SI |
| 004 | R3 | Red clientes | MANOLO | ROUTER | Zona Restauración | NO |
| 005 | S0 | Base de datos administración | PINO | SERVER | Sala administración | SI |
| 006 | S1 | Server Web | PINO | SERVER | Sala adminstración | SI |
| 007 | PC1 | Pc PINO | PINO | PC | Sala administración | NO |
| 008 | PC2 | Pc caja | MANOLO | PC | Zona Restauración | NO |
| 009 | PC3 | Móvil  Manolo | MANOLO | PC | Zona Restauración | NO |

## Software

| **Id** | **Nombre** | **Descripción** | **Id Hardware** | **Tipo** |
| --- | --- | --- | --- | --- |
| SO1 | Windows 11 pro |  | 007 | SO |
| AT1 | Norton 360 | Antivirus para pc | 007 | antivirus |
| AT2 | Kaspersky for web servers | Antivírus para servidor | 006 | Antivirus - firewall |
| SS1 | Apache 2.4.58 | Servidor página web | 006 | Servidor web |
| SO2 | Ubuntu 20.04 LTS |  | 006 |  |
| SS2 | Mysql 8.0 LTS | Servidor de bases de datos local | 005 | Base de datos |
| SO3 | Ubuntu 20.04 LTS | So de base de datos | 005 | SO |
| SC1 |  | Copia de seguridad de base de datos | 007 | fichero |

## 

## 

## Humanos

| **Nombre** | **Lugar de trabajo** | **Puesto** |
| --- | --- | --- |
| Manolo Pérez Gonzalez | Zona de restauración | Encargado de restauración/ CTO |
| PINO Rojo Pérez | Sala administración | Jefa administrativa y tecnológica |
| Manolín Perez Cruz | Zona de restauración | Ayudante de cocina |

# 

# Análisis

## Activo 1

| 005 | S0 | Base de datos administración | PINO | SERVER | Sala administración | SI |
| --- | --- | --- | --- | --- | --- | --- |

| SS2 | Mysql 8.0 LTS | Servidor de bases de datos local | 005 | Base de datos |
| --- | --- | --- | --- | --- |
| SO3 | Ubuntu 20.04 LTS | So de base de datos | 005 | SO |

### Amenazas

1. **Ataques de Ransomware**
   * Los ataques de ransomware pueden cifrar los datos de la base de datos y exigir un rescate para restaurar el acceso. Aunque se cuente con un antivirus, nuevas variantes de ransomware así como errores humanos, la falta de actualizaciones o medidas de seguridad puede exponer la base de datos a este tipo de amenazas.
2. **Fugas de Información por Acceso No Autorizado**
   * La base de datos puede estar en riesgo de accesos no autorizados, ya sea a través de vulnerabilidades en el sistema operativo o debido a errores de configuración.

### Vulnerabilidades

1. **Falta de Copias de Seguridad Regulares y Seguras**
   * La falta de copias de seguridad regulares y seguras puede ser una gran vulnerabilidad. Si la base de datos se ve comprometida o si hay pérdida de datos por alguna razón, la falta de copias de seguridad actualizadas puede dificultar o imposibilitar la recuperación de la información crítica.
2. **Acceso No Seguro a la Base de Datos**
   * Configuraciones incorrectas de acceso a la base de datos o falta de ellas pueden dejarla expuesta a amenazas. Las bases de datos no son seguras por defecto y necesitan configuración y mantenimiento.
3. **Falta de cifrado de las comunicaciones de la base de datos.**
   * La falta de seguridad en el intercambio de información podrá presentar una brecha de seguridad que burle los procedimientos de securización de los dispositivos. Es necesario el uso de protocolos seguros y mantener actualizadas y protegidas las claves de encriptación.

## 

## 

## Activo 2

| 008 | PC2 | Pc caja | MANOLO | PC | Zona Restauración | NO |
| --- | --- | --- | --- | --- | --- | --- |

### Amenazas

1. **Acceso Físico No Autorizado**
   * La información en formato físico, como notas o documentos impresos, puede estar en riesgo si hay acceso físico no autorizado al PC. Esto podría ocurrir si el lugar donde se almacena el PC no está adecuadamente protegido, como una oficina sin seguridad física.
2. **Vigilancia Física o "Shoulder Surfing"**
   * Los atacantes pueden realizar vigilancia física para obtener información confidencial al observar las actividades en la pantalla del PC o al revisar notas y documentos mientras el usuario trabaja. Este tipo de ataque se conoce como "shoulder surfing".

### Vulnerabilidades

1. Falta de Protección Física
   * Si el PC no está protegido adecuadamente contra el acceso no autorizado, ya sea por la falta de cerraduras físicas en la ubicación de almacenamiento o la ausencia de medidas de seguridad física en la oficina, la información en formato físico puede estar en riesgo.
2. No Uso de Medidas de Privacidad en Pantalla
   * Si el usuario no utiliza medidas de privacidad en la pantalla, como protectores de pantalla o filtros de privacidad, la información en la pantalla del PC puede ser visible para personas cercanas, aumentando el riesgo de vigilancia o "shoulder surfing".

## Activo 3

| 007 | PC1 | Pc PINO | PINO | PC | Sala administración | NO |
| --- | --- | --- | --- | --- | --- | --- |

| SO1 | Windows 11 pro |  | 007 | SO |
| --- | --- | --- | --- | --- |
| AT1 | Norton 360 | Antivirus para pc | 007 | antivirus |
| SC1 |  | Copia de seguridad de base de datos | 007 | fichero |

### 

### Amenazas

1. **Malware y Virus**
   * La descarga involuntaria de malware o la infección por virus puede comprometer la seguridad de la información almacenada en el ordenador. Manolo puede hacer clic en enlaces maliciosos o descargar archivos infectados, exponiendo así la red y los datos sensibles de Ca’Manolo.
2. **Ataques de Ingeniería Social**
   * Los ciberdelincuentes pueden utilizar tácticas de ingeniería social para manipular a Manolo y obtener acceso no autorizado a información confidencial. Esto podría incluir la manipulación psicológica, como pueda ser la **suplantación de identidad,** para que se revelen contraseñas, credenciales u otra información confidencial.

### Vulnerabilidades

1. **Falta de Actualizaciones de Seguridad**
   * Si el ordenador no se mantiene actualizado con los últimos parches y actualizaciones de seguridad, podría estar vulnerable a exploits conocidos.
2. **Contraseñas Débiles o Mal Gestionadas**
   * Las contraseñas débiles o mal gestionadas son una vulnerabilidad común. Si en Ca’Manolo eligen contraseñas fáciles de adivinar o las comparten, se aumenta el riesgo de acceso no autorizado a el ordenador. La falta de una política de contraseñas sólida y la ausencia de medidas de autenticación multifactor es la raíz del problema.

## Activo 4

| 006 | S1 | Server Web | PINO | SERVER | Sala adminstración | SI |
| --- | --- | --- | --- | --- | --- | --- |

| AT2 | Kaspersky for web servers | Antivírus para servidor | 006 | Antivirus - firewall |
| --- | --- | --- | --- | --- |
| SS1 | Apache 2.4.58 | Servidor página web | 006 | Servidor web |
| SO2 | Ubuntu 20.04 LTS |  | 006 | SO |

### 

### Amenazas

1. **Ataques de Denegación de Servicio (DoS) o Distribuidos (DDoS)**
   * Los servicios web de la página de Ca’Manolo pueden ser blanco de ataques de denegación de servicio, donde un atacante intenta sobrecargar el servidor con tráfico falso para hacer que el servicio sea inaccesible.
2. **Inyección de Código SQL u Otros Ataques a la Seguridad de la Aplicación**
   * Los atacantes podrían intentar inyectar código malicioso, como SQL, para comprometer la seguridad de la aplicación web. Esto podría conducir a la manipulación de datos, acceso no autorizado o incluso la eliminación de información crítica.

### Vulnerabilidades

1. **Falta de Actualizaciones de Software y Parches de Seguridad**
   * No mantener actualizado el software del servidor web Apache puede dejar la puerta abierta a vulnerabilidades conocidas. Los atacantes podrían aprovechar estas vulnerabilidades a través de ataques automatizados para comprometer el sistema y acceder a información confidencial.
2. **Configuración Insegura del Servidor Web**
   * Configuraciones incorrectas del servidor web, como permisos inapropiados, enlaces simbólicos o la exposición innecesaria de servicios, pueden ser explotadas.

## Activo 5

| 004 | R3 | Red clientes | MANOLO | ROUTER | Zona Restauración | NO |
| --- | --- | --- | --- | --- | --- | --- |

### Amenazas

1. **Ataques de Intercepción de Tráfico (Man-in-the-Middle)**
   * En una red pública, los atacantes podrían realizar ataques de tipo "man-in-the-middle" para interceptar y modificar el tráfico entre el router y los dispositivos conectados. Esto podría resultar en la captura de información confidencial, como credenciales de inicio de sesión.
2. **Ataques de Fuerza Bruta al Router**
   * Los atacantes podrían intentar realizar ataques de fuerza bruta para descifrar las contraseñas del router. Si las contraseñas son débiles o no se han cambiado desde las configuraciones predeterminadas, el riesgo de acceso no autorizado al router aumenta considerablemente.

### Vulnerabilidades

1. **Configuración Predeterminada del Router**
   * Muchos routers se envían con configuraciones predeterminadas que son conocidas y pueden ser explotadas fácilmente. Si no se cambian las credenciales de administrador y otros parámetros de configuración, el router podría ser vulnerable a ataques.
2. **Falta de Actualizaciones de Firmware**
   * Los routers a menudo reciben actualizaciones de firmware para abordar vulnerabilidades de seguridad. La falta de actualizaciones periódicas puede dejar el router expuesto a exploits conocidos que podrían comprometer la integridad y la seguridad de la red.

# Medidas generales de mitigación

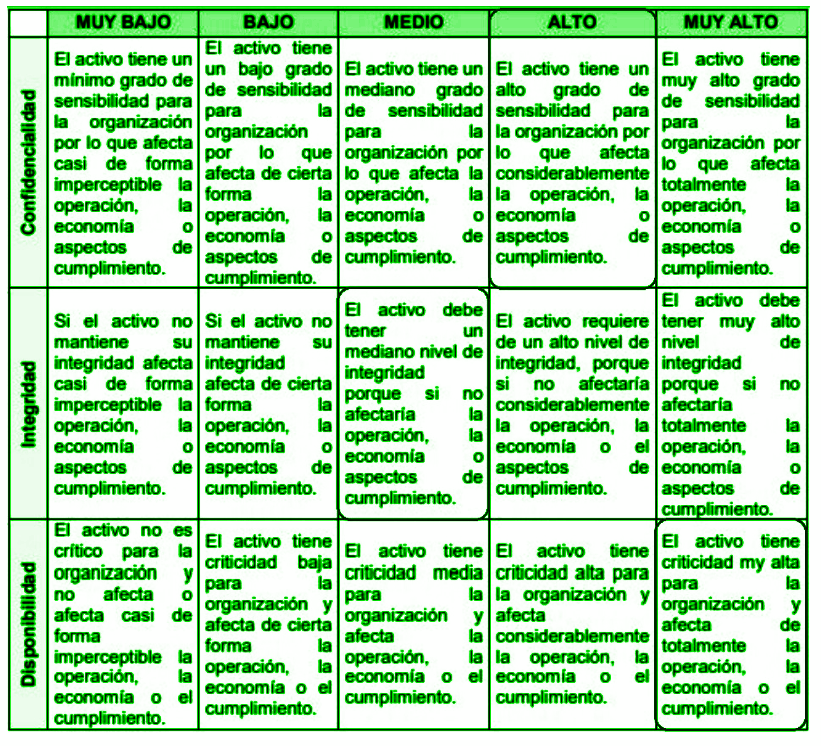
## Recomendaciones generales para los routers

* Cambiar las credenciales predeterminadas del router.
* Utilizar cifrado fuerte para la conexión Wi-Fi (por ejemplo, WPA3).
* Implementar un cortafuegos para controlar y filtrar el tráfico.
* Desactivar servicios y funciones innecesarios.
* Habilitar funciones de detección de intrusiones, si están disponibles.
* Mantener actualizado el firmware del router.

Servicios web

* **Firewall Configurado Correctamente**
  + Configurar el firewall para permitir el tráfico necesario y bloquear el tráfico no autorizado. Limitar el acceso solo a los puertos y servicios esenciales.
* **Uso de Protocolos Seguros (HTTPS)**
  + Implementar SSL/TLS para cifrar la comunicación entre el cliente y el servidor. Esto ayuda a proteger la confidencialidad de la información transmitida.
* **Monitoreo de Eventos y Registro**
  + Establecer sistemas de monitoreo y registro para detectar patrones de tráfico inusual o intentos de intrusión.
* **Actualizaciones y Parches Regulares**
  + Mantener actualizado el software del servidor, el sistema operativo y las aplicaciones para protegerse contra vulnerabilidades conocidas.
* **Configuración Segura del Servidor**
  + Asegurarse de que la configuración del servidor web sea segura y siga las mejores prácticas de seguridad. Limitar los privilegios y desactivar servicios innecesarios.
* **Implementación de Medidas contra Ataques DoS/DDoS**
  + Utilizar servicios o herramientas de mitigación de ataques DoS/DDoS para proteger el servicio web contra sobrecargas maliciosas.

# Análisis de Riesgo

Se hará uso de esta tabla para contextualizar las puntuaciones:

* **Probabilidad (P)**
  + 1 Muy baja
  + 2 Baja
  + 3 Moderada
  + 4 Alta
  + 5 Muy alta
* **Impacto (I)**
  + 1 Muy bajo
  + 2 Bajo
  + 3 Moderado
  + 4 Alto
  + 5 Muy alto
* **Riesgo (R)** Se calcula multiplicando la probabilidad por el impacto.
  + 1-5 Bajo
  + 6-10 Medio
  + 11-15 Alto
  + 16-20 Muy alto
  + 21-25 Extremadamente alto

| Muy alta | 5 | 7 | 16 | 20 | 25 |
| --- | --- | --- | --- | --- | --- |
| Alta | 4 | 5 | 9 | 16 | 21 |
| Moderada | 3 | 4 | 7 | 12 | 18 |
| Baja | 2 | 3 | 5 | 11 | 16 |
| Muy Baja | 1 | 2 | 4 | 9 | 15 |
| Probabilidad | X | 1 | 2 | 3 | 4 |
|  | Impacto | Irrelevante | Menor | Serio | Grave |

## Activo 1

| **Activo** | **Enfoque** | **Amenaza** | **Vulnerabilidad** | **Probabilidad (P)** | **Impacto (I)** | **Riesgo (R = P x I)** | **Estrategias de Mitigación** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 005 | Legal | Ataques de Ransomware | Acceso No Seguro a la Base de Datos | Alta (4) | Muy Alto (5) | Muy Alto (20) | Implementación de políticas de seguridad |
| 005 | Económico | Ataques de Ransomware | Acceso No Seguro a la Base de Datos | Moderada (3) | Alto (4) | Alto (12) | Respaldo y recuperación de datos |
| 005 | Operativo | Ataques de Ransomware | Acceso No Seguro a la Base de Datos | Baja (2) | Moderado (3) | Bajo (6) | Actualización regular de sistemas |

## Activo 2

| **Activo** | **Enfoque** | **Amenaza** | **Vulnerabilidad** | **Probabilidad (P)** | **Impacto (I)** | **Riesgo (R = P x I)** | **Estrategias de Mitigación** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 008 | Legal | Acceso Físico No Autorizado | Falta de Protección Física | Moderada (3) | Alto (4) | Alto (12) | Implementación de controles de acceso |
| 008 | Económico | Acceso Físico No Autorizado | Falta de Protección Física | Alta (4) | Muy Alto (5) | Muy Alto (20) | Instalación de sistemas de seguridad física |
| 008 | Operativo | Acceso Físico No Autorizado | Falta de Protección Física | Baja (2) | Moderado (3) | Bajo (6) | Monitoreo y respuesta rápida |

| **Activo** | **Enfoque** | **Amenaza** | **Vulnerabilidad** | **Probabilidad (P)** | **Impacto (I)** | **Riesgo (R = P x I)** | **Estrategias de Mitigación** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 008 | Legal | Vigilancia Física o 'Shoulder Surfing' | No Uso de Medidas de Privacidad en Pantalla | Moderada (3) | Alto (4) | Alto (12) | Implementación de políticas de privacidad |
| 008 | Económico | Vigilancia Física o 'Shoulder Surfing' | No Uso de Medidas de Privacidad en Pantalla | Alta (4) | Muy Alto (5) | Muy Alto (20) | Entrenamiento y concientización del personal |
| 008 | Operativo | Vigilancia Física o 'Shoulder Surfing' | No Uso de Medidas de Privacidad en Pantalla | Baja (2) | Moderado (3) | Bajo (6) | Implementación de protectores de pantalla |

## 

## Activo 3

| **Activo** | **Enfoque** | **Amenaza** | **Vulnerabilidad** | **Probabilidad (P)** | **Impacto (I)** | **Riesgo (R = P x I)** | **Estrategias de Mitigación** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 007 | Legal | Malware y virus | Falta de actualizaciones de seguridad | Moderada (3) | Moderado (3) | Alto (9) | Implementación de políticas de actualización |
| 007 | Económico | Malware y virus | Falta de actualizaciones de seguridad | Alta (4) | Alto (4) | Muy Alto (16) | Implementación de sistemas de detección y respuesta |
| 007 | Operativo | Malware y virus | Falta de actualizaciones de seguridad | Baja (2) | Moderado (3) | Bajo (6) | Mantenimiento regular y actualizaciones |

| **Activo** | **Enfoque** | **Amenaza** | **Vulnerabilidad** | **Probabilidad (P)** | **Impacto (I)** | **Riesgo (R = P x I)** | **Estrategias de Mitigación** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 007 | Legal | Ataques de ingeniería social | Contraseñas débiles o mal gestionadas | Moderada (3) | Alto (4) | Alto (12) | Implementación de políticas de gestión de contraseñas |
| 007 | Económico | Ataques de ingeniería social | Contraseñas débiles o mal gestionadas | Alta (4) | Muy Alto (5) | Muy Alto (20) | Capacitación del personal en seguridad de contraseñas |
| 007 | Operativo | Ataques de ingeniería social | Contraseñas débiles o mal gestionadas | Baja (2) | Moderado (3) | Bajo (6) | Implementación de autenticación de dos factores |

## 

## Activo 4

| **Activo** | **Enfoque** | **Amenaza** | **Vulnerabilidad** | **Probabilidad (P)** | **Impacto (I)** | **Riesgo (R = P x I)** | **Estrategias de Mitigación** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 006 | Legal | Ataques de Denegación de Servicio (DoS) o DDoS | Falta de Actualizaciones de Software y Parches de Seguridad | Moderada (3) | Moderado (3) | Alto (9) | Implementación de políticas de actualización y parches de seguridad |
| 006 | Económico | Ataques de Denegación de Servicio (DoS) o DDoS | Falta de Actualizaciones de Software y Parches de Seguridad | Alta (4) | Alto (4) | Muy Alto (16) | Implementación de sistemas de detección y mitigación de ataques DDoS |
| 006 | Operativo | Ataques de Denegación de Servicio (DoS) o DDoS | Falta de Actualizaciones de Software y Parches de Seguridad | Baja (2) | Moderado (3) | Bajo (6) | Configuración de medidas de prevención y respuesta ante ataques DDoS |

| **Activo** | **Enfoque** | **Amenaza** | **Vulnerabilidad** | **Probabilidad (P)** | **Impacto (I)** | **Riesgo (R = P x I)** | **Estrategias de Mitigación** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 006 | Legal | Inyección de Código SQL u Otros Ataques a la Seguridad de la Aplicación | Configuración Insegura del Servidor Web | Moderada (3) | Alto (4) | Alto (12) | Implementación de políticas de configuración segura del servidor web |
| 006 | Económico | Inyección de Código SQL u Otros Ataques a la Seguridad de la Aplicación | Configuración Insegura del Servidor Web | Alta (4) | Muy Alto (5) | Muy Alto (20) | Auditorías de seguridad de aplicaciones y corrección de vulnerabilidades |
| 006 | Operativo | Inyección de Código SQL u Otros Ataques a la Seguridad de la Aplicación | Configuración Insegura del Servidor Web | Baja (2) | Moderado (3) | Bajo (6) | Implementación de controles de seguridad en la capa de aplicación |

## Activo 5

| **Activo** | **Enfoque** | **Amenaza** | **Vulnerabilidad** | **Probabilidad (P)** | **Impacto (I)** | **Riesgo (R = P x I)** | **Estrategias de Mitigación** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 004 | Legal | Ataques de Intercepción de Tráfico (Man-in-the-Middle) | Configuración Predeterminada del Router | Moderada (3) | Alto (4) | Alto (12) | Cambio de configuración por defecto en el router |
| 004 | Económico | Ataques de Intercepción de Tráfico (Man-in-the-Middle) | Configuración Predeterminada del Router | Alta (4) | Muy Alto (5) | Muy Alto (20) | Implementación de tecnologías de detección de MITM |
| 004 | Operativo | Ataques de Intercepción de Tráfico (Man-in-the-Middle) | Configuración Predeterminada del Router | Baja (2) | Moderado (3) | Bajo (6) | Actualizaciones periódicas de configuración y monitoreo |

| **Activo** | **Enfoque** | **Amenaza** | **Vulnerabilidad** | **Probabilidad (P)** | **Impacto (I)** | **Riesgo (R = P x I)** | **Estrategias de Mitigación** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 004 | Legal | Ataques de fuerza bruta al router | Falta de actualizaciones de Firmware | Moderada (3) | Alto (4) | Alto (12) | Programación regular de actualizaciones de firmware del router |
| 004 | Económico | Ataques de fuerza bruta al router | Falta de actualizaciones de Firmware | Alta (4) | Muy Alto (5) | Muy Alto (20) | Implementación de medidas de seguridad adicionales en el router |
| 004 | Operativo | Ataques de fuerza bruta al router | Falta de actualizaciones de Firmware | Baja (2) | Moderado (3) | Bajo (6) | Monitoreo constante y respuesta rápida ante intentos de fuerza bruta |