CORE BOT

Documento Oficial: Sistema de Blacklist Global



Autoridad Emisora: Joel, Fundador de Core Bot
Sitio Web Oficial: corebot.cat | **Servidor de Soporte:** discord.gg/rtuEvqEVVD
Panel Web: panelcorebot.com

1. ¿Qué es la Blacklist Global?

El sistema de blacklist global de **Core Bot** protege automáticamente a todos los servidores asociados a la red. La **Global Blacklist** impide el acceso de usuarios peligrosos a **todos** los servidores que utilizan los sistemas de Core Bot.

Cuando un usuario es añadido a la blacklist

- No podrá entrar a los servidores protegidos.
- Será expulsado automáticamente.
- Se bloqueará el uso de comandos.
- Su actividad quedará registrada en la red.
- Sus cuentas alternativas podrán ser detectadas.

2. Niveles de Sanción

Las sanciones se dividen en cinco niveles según la gravedad de la conducta. Cada nivel define los motivos que lo originan, su duración y las consecuencias que se aplican en toda la red.

Resumen de niveles

Nivel	Duración	Consecuencias principales
Leves	2 semanas · 1 mes	Restricción parcial, monitorización automática, limitación de comandos y advertencia global.
Medias	1 · 2 · 4 meses	Expulsión automática, bloqueo completo de Core Bot, denegación temporal de acceso y registro en la red.
Intermedias	4 · 6 · 8 meses	Blacklist severa, expulsión instantánea, bloqueo global, detección de cuentas alternativas y reporte al staff.
Graves	12 · 24 meses · Permanente	Blacklist permanente, ban automático en toda la red, bloqueo irreversible y sin posibilidad de apelación.
Permanente	Indefinida	Prohibición permanente, bloqueo total del ecosistema Core Bot y registro permanente en la red.

Sanciones Leves

Motivos

- Spam leve
- Flood leve
- Mini ping spam
- Molestias menores
- Mensajes repetitivos
- Emojis/GIF spam leve
- Intento leve de publicidad
- Toxicidad moderada
- Alteración menor del chat

Duración: 2 semanas · 1 mes

Consecuencias

- Restricción parcial
- Monitorización automática
- Limitación de comandos
- Advertencia global

Sanciones Medias

Motivos

- Spam masivo
- Flood agresivo
- Publicidad no autorizada
- Intento de spam
- Ping raid
- Uso de multicuentas
- Troll masivo
- Intento de evasión
- Uso sospechoso de automatizaciones
- Alteración moderada del servidor
- Toxicidad extrema
- Intento de scam

Duración: 1 mes · 2 meses · 4 meses

Consecuencias

- Expulsión automática
- Bloqueo completo de Core Bot
- Denegación temporal de acceso
- Registro en la red global

Sanciones Intermedias

Motivos

- Uso de selfbot
- Intento de raid
- Colaboración en raid
- Spam automatizado
- Scam moderado
- Enlaces maliciosos
- Uso de scripts externos
- Nuking parcial
- Intento de phishing
- Distribución de malware sospechoso
- Evasión de blacklist
- Suplantación de identidad
- Robo de cuentas
- Uso de herramientas maliciosas
- Webhook spam
- Mass DM

Duración: 4 meses · 6 meses · 8 meses

Consecuencias

- Global Blacklist severa
- Expulsión instantánea
- Bloqueo global del sistema
- Detección de cuentas alternativas
- Reporte automático al staff

Sanciones Graves

Motivos

- Raid masivo
- Organización de raids
- Nuking total
- Malware real
- Estafas confirmadas
- Robo de cuentas
- Phishing confirmado
- Uso avanzado de selfbots
- Ataques coordinados
- Doxxing
- Amenazas graves
- Venta de cuentas robadas
- Uso de exploits
- Creación de bots maliciosos
- Manipulación de seguridad
- Evasión masiva de bans
- Destrucción de servidores
- Participación en redes maliciosas

Duración: 12 meses · 24 meses · Permanente

Consecuencias

- Global Blacklist permanente
- Ban automático en toda la red
- Bloqueo irreversible
- Inclusión en la base de datos global
- Imposibilidad de apelación

Global Blacklist Permanente

Aplicable por

- Malware confirmado
- Redes de raids
- Scams organizados
- Daños graves a servidores
- Ataques repetidos
- Uso reiterado de selfbots
- Amenazas reales
- Actividad criminal digital
- Reincidencia extrema

Consecuencias

- Prohibición permanente
- Expulsión automática de cualquier servidor protegido
- Bloqueo total del ecosistema Core Bot
- Registro permanente en la red

3. Sistemas Automáticos de Core Bot

Core Bot protege automáticamente los servidores asociados contra las siguientes amenazas:

Protección activa 24/7

- Spam
- Flood
- Raids
- Selfbots
- Nukers
- Malware
- Phishing
- Estafas
- Mass DM
- Webhook abuse
- Multicuentas
- Bots maliciosos
- Evasión de sanciones
- Scripts automatizados
- Token grabbers

4. Cómo Funciona el Proceso

Del aviso a la sanción

1. Detección
Los sistemas automáticos o el staff detectan la conducta.

2. Registro
La acción queda registrada en la red de Core Bot.

3. Aplicación
Se aplican expulsión, bloqueo y limitaciones en la red.

4. Revisión
El staff puede ajustar la sanción según cada caso.

5. Información Importante

Condiciones generales

- Intentar evadir una sanción aumentará automáticamente su duración.
- Las cuentas alternativas serán bloqueadas automáticamente.
- Todas las acciones quedan registradas.
- El staff de Core Bot puede modificar las sanciones dependiendo de cada caso.

6. Reportes y Consultas

¿Quieres reportar a un usuario o consultar una sanción?

Abre un ticket de soporte en nuestro servidor oficial o a través de nuestros canales de contacto. Para agilizar la revisión, indica el **ID del usuario** y aporta pruebas (capturas, enlaces o registros). El equipo de Core Bot revisará cada caso de forma individual. Recuerda que las sanciones graves y permanentes no admiten apelación.

Sitio Web Oficial: corebot.cat | **Servidor de Soporte:** discord.gg/rtuEvqEVVD
Panel Web: panelcorebot.com