

Riesgos

El apartado de Riesgos es un módulo de validación y verificación que ejecuta múltiples controles de seguridad en tiempo real durante una sesión. Su función principal es validar la autenticidad de tres componentes críticos:

- 1. **Device Risks:** Validar que el dispositivo es legítimo y seguro
- 2. **Location Risks:** Verificar que la ubicación es coherente y permitida
- 3. **Behavioural Risks:** Confirmar que el comportamiento corresponde al usuario real

Estados de Validación

Estado	Color	Significado	Interpretación
VERDE	Verde	Validación Exitosa	El parámetro fue verificado correctamente. Los controles de seguridad pasaron satisfactoriamente. El elemento cumple con los criterios de seguridad establecidos
ROJO	Rojo	Validación Fallida	El parámetro no pudo ser validado positivamente. Los controles de seguridad detectaron problemas. El elemento presenta características que generan alertas de seguridad
MORADO	Morado	Validación Indeterminada	El parámetro no se pudo validar completamente. Los controles no pudieron obtener información suficiente. El estado del elemento es incierto o ambiguo

DEVICE RISKS - RIESGOS DEL DISPOSITIVO

Device Risks

Unknown device

Active malware (42)

Suspicious device characteristics

Device properties consistency for identity

Emulator

Bot

Identities accessed by this device

Device is in blacklist

vpn

vpn installed?

Compromised Device

Remote Access

Rooted Device

Location Risks

Unknown location for identity

Suspicious location attributes

Location change velocity

Location is in blacklist

GPS enabled?

new IP country?

GPS location mismatch

Behavioural Risks

Risky keyboard event

Risky mouse event

Use of autocomplete

Form navigation: N/A

Parámetros de Alto Riesgo (ROJO)

Parámetro	Descripción	Interpretación	Nivel de Riesgo
Unknown device	El dispositivo no existe en la base de datos de dispositivos conocidos	Es la primera vez que este dispositivo accede a la plataforma	Dispositivos nuevos pueden ser utilizados específicamente para fraude
Suspicious device characteristics	Las características técnicas del dispositivo presentan anomalías	Hardware, software o configuraciones que no son típicas o han sido modificadas	Dispositivo alterado para evadir controles de seguridad
Emulator	Se detectó que se está usando un emulador de dispositivo móvil	Software que simula un teléfono/tablet en una computadora	Herramienta común para automatizar fraudes masivos
VPN	Se detectó una conexión VPN activa	El usuario está ocultando su ubicación real mediante una red privada virtual	Evasión de controles geográficos y ocultamiento de identidad

Parámetros de Riesgo Indeterminado (MORADO)

Parámetro	Descripción	Razón del Estado Morado	Interpretación
VPN installed?	Hay indicios de software VPN instalado pero no confirmación total	El sistema detecta patrones de VPN pero no puede acceder completamente a la lista de aplicaciones	Posible capacidad de ocultar ubicación
Compromised Device	El dispositivo muestra algunos signos de haber sido comprometido	Algunos indicadores sugieren compromiso pero el análisis no es concluyente	Posible infección de malware o acceso no autorizado

Parámetros Validados - Bajo Riesgo (VERDE)

Parámetro	Descripción	Estado Actual	Interpretación
Active malware (42)	Sistema de detección de malware funcionando, 42 indica nivel de análisis completado	No se detectó software malicioso activo	Dispositivo limpio
Device properties consistency for identity	Las propiedades del dispositivo coinciden con el perfil del usuario	El dispositivo es consistente con el historial del usuario legítimo	Validación positiva de autenticidad
Bot	Análisis para detectar comportamiento automatizado o scripts	No se detectó actividad de bots	Interacción humana confirmada
Identities accessed by this device	Registro de cuántas identidades diferentes han usado este dispositivo	Patrón normal de uso del dispositivo	Sin uso sospechoso por múltiples identidades
Device is in blacklist	Verificación contra listas negras de dispositivos conocidos como maliciosos	El dispositivo no está reportado como peligroso	No está en listas de bloqueo
Remote Access	Detección de software de acceso remoto activo	No se detectaron herramientas de control remoto	Usuario en control directo del dispositivo
Rooted Device	Verificación si el dispositivo tiene permisos de root/jailbreak	Sistema operativo sin modificaciones peligrosas	Dispositivo con seguridad íntegra

LOCATION RISKS - RIESGOS DE UBICACIÓN

Device Risks	Location Risks	Behavioural Risks
<div>Unknown device</div> <div>Active malware (42)</div> <div>Suspicious device characteristics</div> <div>Device properties consistency for identity</div> <div>Emulator</div> <div>Bot</div> <div>Identities accessed by this device</div> <div>Device is in blacklist</div> <div>vpn</div> <div>vpn installed?</div> <div>Compromised Device</div> <div>Remote Access</div> <div>Routed Device</div>	<div>Unknown location for identity</div> <div>Suspicious location attributes</div> <div>Location change velocity</div> <div>Location is in blacklist</div> <div>GPS enabled?</div> <div>new IP country?</div> <div>GPS location mismatch</div>	<div>Risky keyboard event</div> <div>Risky mouse event</div> <div>Use of autocomplete</div> <div>Form navigation: N/A</div>

Parámetros de Alto Riesgo (ROJO)

Parámetro	Descripción	Interpretación	Nivel de Riesgo
Unknown location for identity	La ubicación actual no coincide con ninguna ubicación conocida del usuario	Usuario accediendo desde un lugar completamente nuevo	Posible acceso no autorizado desde ubicación comprometida
Suspicious location attributes	La ubicación geográfica tiene características asociadas con fraude	Área conocida por actividades fraudulentas o bloqueada	Zona de alto riesgo para transacciones
GPS enabled?	El GPS del dispositivo está deshabilitado	No se puede verificar la ubicación real del dispositivo	Imposibilidad de validar ubicación precisa
New IP country?	La dirección IP pertenece a un país diferente al habitual del usuario	Acceso desde país no característico del usuario	Posible uso de VPN o acceso comprometido

Parámetros de Riesgo Indeterminado (MORADO)

Parámetro	Descripción	Razón del Estado Morado	Interpretación
GPS location mismatch	La ubicación GPS no coincide con la ubicación determinada por IP	Ambas fuentes proporcionan ubicaciones diferentes pero válidas	Discrepancia que requiere análisis adicional

Parámetros Validados - Bajo Riesgo (VERDE)

Parámetro	Descripción	Estado Actual	Interpretación
Location change velocity	La velocidad de cambio entre ubicaciones es físicamente posible	El desplazamiento es coherente con medios de transporte reales	Patrón normal de movilidad
Location is in blacklist	Verificación contra listas de ubicaciones prohibidas	La ubicación no está en zonas bloqueadas	Ubicación permitida para transacciones

BEHAVIOURAL RISKS - RIESGOS COMPORTAMENTALES

Device Risks

Unknown device

Active malware (42)

Suspicious device characteristics

Device properties consistency for identity

Emulator

Bot

Identities accessed by this device

Device is in blacklist

vpn

vpn installed?

Compromised Device

Remote Access

Rooted Device

Location Risks

Unknown location for identity

Suspicious location attributes

Location change velocity

Location is in blacklist

GPS enabled?

new IP country?

GPS location mismatch

Behavioural Risks

Risky keyboard event

Risky mouse event

Use of autocomplete

Form navigation: N/A

Parámetros Validados - Bajo Riesgo (VERDE)

Parámetro	Descripción	Estado Actual	Interpretación
-----------	-------------	---------------	----------------

Risky keyboard event	Análisis de patrones de escritura, velocidad y ritmo de tecleo	Los patrones de teclado coinciden con la biometría del usuario legítimo	Comportamiento de escritura normal y auténtico
Risky mouse event	Evaluación de movimientos, clicks y patrones del mouse	Los movimientos del mouse son característicos del usuario real	Interacción natural sin automatización
Use of autocomplete	Detección del uso normal de funciones de autocompletado	Uso típico de herramientas del navegador	Comportamiento humano normal

Parámetros Informativos

Parámetro	Estado	Descripción	Razón
Form navigation	N/A	Datos sobre navegación en formularios no disponibles	Este análisis no aplica para el tipo de sesión actual

Interpretación de Resultados

Matriz de Decisión por Combinación de Estados

Combinación de Colores	Nivel de Riesgo	Descripción	Acción Sugerida
Todo Verde	BAJO	Todos los parámetros pasaron las validaciones	Proceder con confianza total
Verde + Morado	MEDIO-BAJO	Mayoría de validaciones exitosas con algunas indeterminadas	Proceder con monitoreo adicional
Verde + 1-2 Rojos	MEDIO	Validaciones mixtas con algunos problemas detectados	Requiere intervención manual o bloqueo automático
Múltiples Morados	MEDIO-ALTO	Múltiples validaciones incompletas	Análisis manual recomendado
Múltiples Rojos	ALTO	Múltiples problemas de seguridad detectados	Bloqueo inmediato, investigación
Todo Rojo	CRÍTICO	Fallas generalizadas en validaciones	Bloqueo total, escalación inmediata

Algoritmo de Puntuación

Color del Parámetro	Valor Numérico	Peso en Cálculo
Verde	+10 puntos	Positivo
Morado	0 puntos	Neutro

Color del Parámetro	Valor Numérico	Peso en Cálculo
Rojo	-15 puntos	Negativo

Distribución de Peso por Categoría

Categoría	Peso en Score Total	Justificación
Device Risks	40%	Fundamental para validar legitimidad del acceso
Location Risks	35%	Crítico para detectar accesos geográficamente anómalos
Behavioural Risks	25%	Importante para distinguir humanos de automatización

Revision #4
Created 30 June 2025 14:53:20 by roger de avila
Updated 1 July 2025 12:53:28 by roger de avila