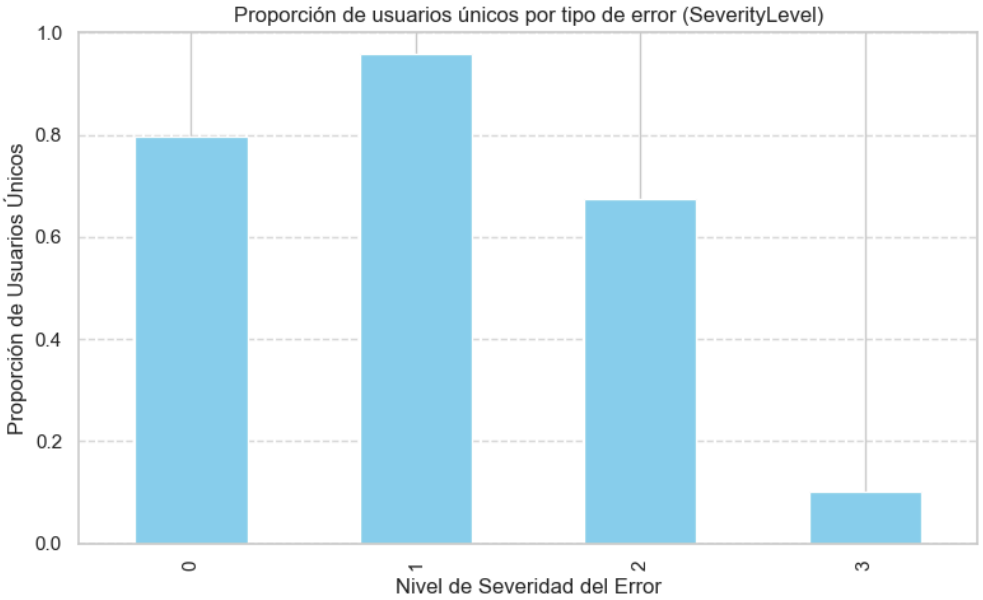
Análisis de Bitácoras

Reporte Ejecutivo

Humberto Mondragón García A01711912
Gabriela Marissa Mosquera A01666191
Felipe de Jesús Damián Rodríguez A01707246

Insight 1: Concentración de errores críticos (Severity 3) en un grupo reducido de usuarios

El análisis de los errores tipo 3 (críticos) muestra una fuerte concentración en pocos usuarios: solo 5 generaron los 22,525 errores detectados, y algunos mensajes críticos fueron provocados exclusivamente por un único usuario, con más de 16,000 errores repetidos. En contraste, los errores leves y moderados están ampliamente distribuidos entre la mayoría. Esto indica que las fallas más graves no reflejan un problema sistémico, sino situaciones puntuales —posiblemente por mala configuración o mal uso del sistema— que deben atenderse de forma personalizada, evitando acciones correctivas generalizadas.



Gráfica 1: Proporción de usuarios únicos por tipo de error

```
ErrorTipo
Control Type Mismatch. Tag 50000 is TKToolBar not a TCAToolBarDesigner    16349
Control Not Found!                                                         2755
Invalid Tag: 0. Command: DisableFields                                     2187
Control Type Mismatch. Tag 1111 is TCAButton not a TKButton                1056
GetProductUsersByDBId                                                        84
GetProductProfilesByDBId                                                     84
Name: count, dtype: int64
```

Tabla 1: Errores más comunes de tipo 3

	ErrorTipo	Total ocurrencias	Usuarios únicos
0	Control Type Mismatch. Tag 50000 is TKToolBar ...	16349	1
1	Control Not Found!	2755	1
2	Invalid Tag: 0. Command: DisableFields	2187	1
3	Control Type Mismatch. Tag 1111 is TCAButton n...	1056	1
4	GetProductUsersByDBId	84	1
5	GetProductProfilesByDBId	84	1

Tabla 2: Errores más comunes tipo 3 provocados por un solo usuario único diferente

Los errores críticos tipo 3 están fuertemente concentrados: varios fueron generados por un solo usuario con miles de ocurrencias, como muestra la Tabla 2. La Tabla 3 confirma que solo 5 usuarios concentran todos estos errores, lo que indica problemas muy localizados y no fallas del sistema en general.

	UserId	ErrorTipo	Ocurrencias
4	q3jl0z2ceDGReWSeifyTrj	Control Type Mismatch. Tag 50000 is TKToolBar ...	16349
3	nm4lPB3QyfwUdNMqpBms22	Control Not Found!	2755
0	7HudNhG1J8x5OP0Ri4eRwd	Invalid Tag: 0. Command: DisableFields	2187
5	tnr5w5YKWmBCjUJIXYx1BK	Control Type Mismatch. Tag 1111 is TCAButton n...	1056
1	jNrNGCGQ8Uj6jkq9wRsCfn	GetProductProfilesByDBId	84
2	jNrNGCGQ8Uj6jkq9wRsCfn	GetProductUsersByDBId	84

Tabla 3: Usuarios que provocan los errores más comunes tipo 3

Los errores críticos del sistema no son producto de fallas generalizadas, sino de casos muy específicos concentrados en un pequeño grupo de usuarios. Esto permite enfocar las acciones correctivas en la revisión del entorno y comportamiento de estos usuarios, optimizando recursos y reduciendo el impacto operativo sin necesidad de aplicar cambios amplios al sistema en su conjunto.

Insight 2: Análisis de errores por país y su distribución proporcional

Se realizó un análisis por país para identificar los errores más frecuentes y su gravedad relativa. A partir del tipo de error extraído desde los mensajes de bitácora, se identificaron los cinco errores más comunes por país y se calculó la proporción de errores severos (Severity ≥ 2) en función del total de bitácoras reportadas. Esto permitió detectar **diferencias técnicas relevantes por región** y evaluar el nivel de criticidad operacional en cada una.

	ClientCountryOrRegion	ErrorTipo
309	Mexico	WebMethod=ProcessBRRequest
304	Mexico	WebMethod=GetKendoCustomDataSourceInstance
223	Mexico	ProcessBRRequest.CheckForReturn
132	Mexico	FastRequest.CheckForReturn
174	Mexico	Params ? Id: ? Values:
320	United Kingdom	WebMethod=ProcessBRRequest
316	United Kingdom	ParseTagValuePairToClientTransferPackage
317	United Kingdom	ProcessBRRequest.CheckForReturn
318	United Kingdom	Requesting
319	United Kingdom	Unpack
338	United States	FastRequest.CheckForReturn
322	United States	Control Not Found!
321	United States	- UpdateSession
352	United States	UpdateSession
353	United States	WebMethod=GetKendoGridInstance

Tabla 4: Top 5 errores más comunes por país

Hallazgos clave:

- **México** concentra el mayor número absoluto de errores, mayormente relacionados con fallas en la lógica de negocio.
- **Reino Unido** presenta errores típicos de interoperabilidad y manejo de estructuras de datos entre sistemas.
- **Estados Unidos** destaca por errores en la interfaz, reflejando posibles fallas en la experiencia de usuario.
- Aunque México tiene más errores en total, **EE. UU. presenta la mayor proporción de errores críticos**, lo cual indica un mayor impacto relativo en su operación.

	Ocurrencias
309	671811
304	568233
223	329637
132	263716
174	235631
320	288
316	144
...	
322	16452
321	9468
352	9439
353	8535

Tabla 5: Ocurrencias de los errores más comunes de países

```
ClientCountryOrRegion
Mexico            5642489
United States      136408
United Kingdom       1502
Name: count, dtype: int64
```

Tabla 6: Total de Bitácoras por país

No obstante, para obtener una interpretación más precisa y **evitar sesgos por el volumen total de bitácoras**, se calculó la **proporción de errores graves** (SeverityLevel ≥ 2) respecto al total de bitácoras por país. El resultado se presenta a continuación:

```
ClientCountryOrRegion
United States     0.384318
Mexico            0.226775
United Kingdom    0.041278
Name: count, dtype: float64
```

Tabla 7: Proporción de errores graves

Los errores críticos varían por región: mientras México presenta más errores en total, Estados Unidos tiene mayor proporción de fallos graves. Esto sugiere la necesidad de aplicar soluciones focalizadas según el tipo de error predominante en cada país.

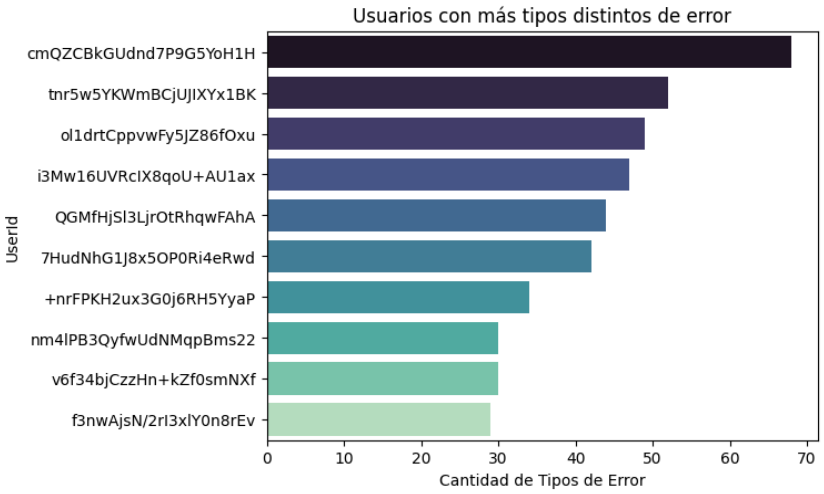
Query 3: Usuarios con Errores Diversos en un Mismo Rol

Se identificaron usuarios que, aun compartiendo el mismo rol (innv103-wapp), presentan una alta **diversidad de errores**(hasta 68 tipos distintos). Esta variabilidad no se explica por diferencias de permisos, sino por factores individuales y técnicos como el entorno de uso o la configuración del sistema.

El usuario **cmQZCBkGUdnd7P9G5YoH1H** presentó la mayor diversidad de errores con **68 tipos distintos**. Otros usuarios, como **tnr5w5YKWmBCjUJIXYx1BK** y **ol1drtCppvwFy5JZ86fOxu**, generaron entre **49 y 52 tipos**, y varios de ellos también están relacionados con errores críticos tipo 3.

	UserId	TiposDeErrorDistintos
0	cmQZCBkGUdnd7P9G5YoH1H	68
1	tnr5w5YKWmBCjUJIXYx1BK	52
2	ol1drtCppvwFy5JZ86fOxu	49
3	i3Mw16UVRcIX8qoU+AU1ax	47
4	QGMfHjSl3LjrOtRhqwFAhA	44
5	7HudNhG1J8x5OP0Ri4eRwd	42
6	+nrFPKH2ux3G0j6RH5YyaP	34
7	nm4lPB3QyfwUdNMqpBms22	30
8	v6f34bjCzzHn+kZf0smNXf	30
9	f3nwAjsN/2rl3xlY0n8rEv	29

Tabla 8: Usuarios con más tipos de errores distintos



Gráfica 2: Usuarios con más tipos de error distintos

Este hallazgo indica que algunos usuarios no solo cometen errores críticos, sino también una gran variedad de fallos, lo que podría deberse a mal uso, configuraciones incorrectas o fallas en flujos no validados. Todos pertenecen al mismo rol (innv103-wapp), por lo que las diferencias no se explican por permisos, sino por el uso individual del sistema.

AppRoleName	count	mean	max	std
innv103-wapp	49	14.755102	68	16.692726

Tabla 9: Existencia de un solo rol (innv103-wapp)

El análisis revela que algunos usuarios, como **cmQZCBkGUdnd7P9G5YoH1H**, generan tanto errores críticos como una alta diversidad de fallos, lo que sugiere problemas de uso, entrenamiento o entorno. Varios de ellos también están vinculados a errores tipo 3, confirmando que las fallas se concentran en pocos usuarios.

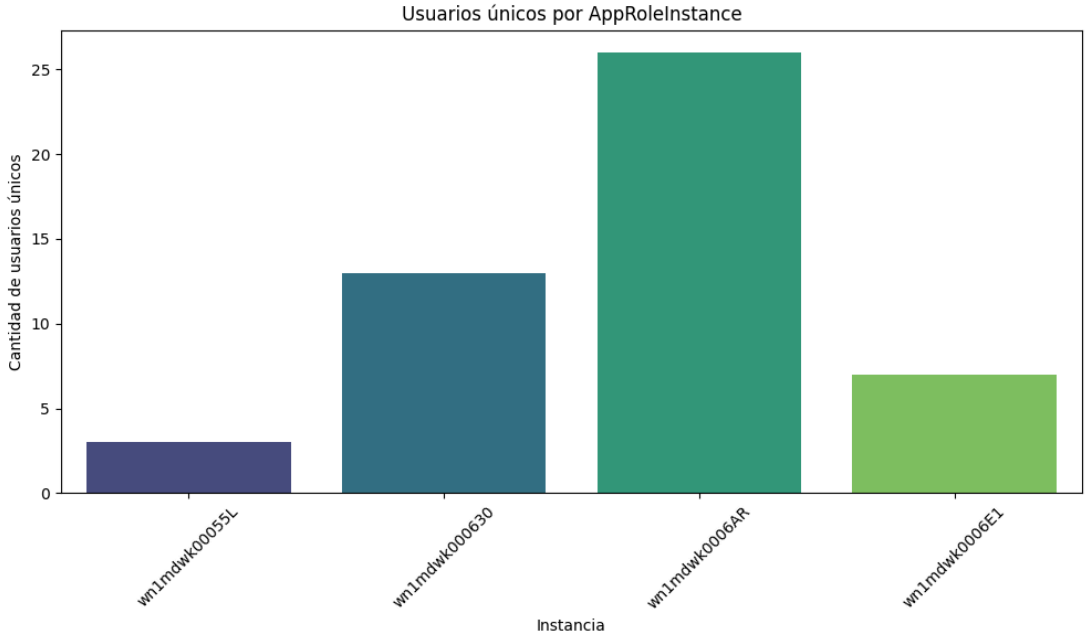
	AppRoleInstance	Usuarios Únicos
0	wn1mdwk00055L	3
1	wn1mdwk000630	13
2	wn1mdwk0006AR	26
3	wn1mdwk0006E1	7

Tabla 10: Diferentes instancias del único rol

Durante el análisis se identificó que todos los usuarios con errores pertenecen al mismo rol (**innv103-wapp**), pero operan en **cuatro instancias distintas del sistema**. Estas instancias representan entornos separados donde se ejecuta el mismo rol, lo que permite detectar diferencias de comportamiento no atribuibles al rol, sino al entorno técnico específico.

	AppRoleInstance	Errores Críticos	% del total
0	wn1mdwk0006AR	22347	99.253831
1	wn1mdwk00055L	168	0.746169

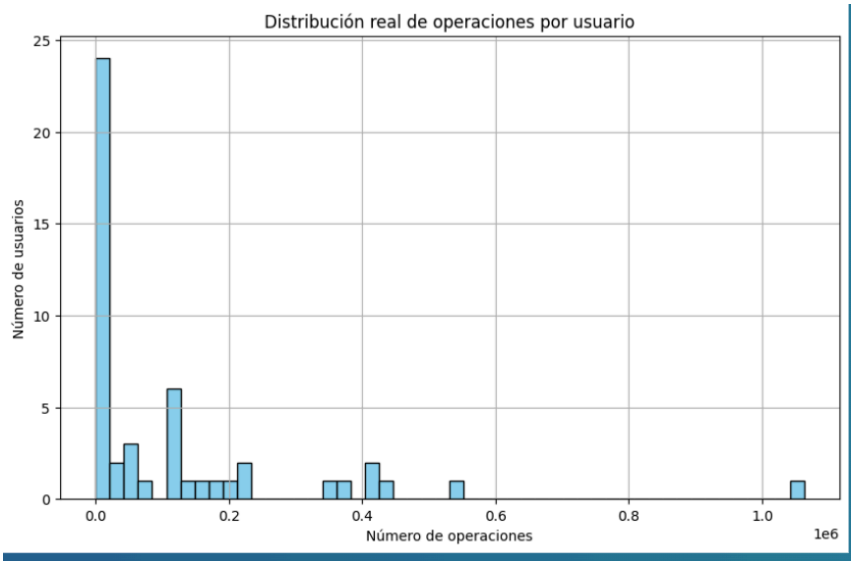
Tabla 11: Errores críticos por instancia



Gráfica 3: Usuarios únicos por instancia

La mayoría de los errores críticos (más del 99 %) se concentran en la instancia **wn1mdwk0006AR**, que además es la que más usuarios agrupa. Esto sugiere posibles fallos de configuración, uso intensivo o pruebas en ese entorno. Aunque todos los usuarios comparten el mismo rol, las diferencias de errores se explican por el uso y configuración de la instancia, no por los permisos del rol.

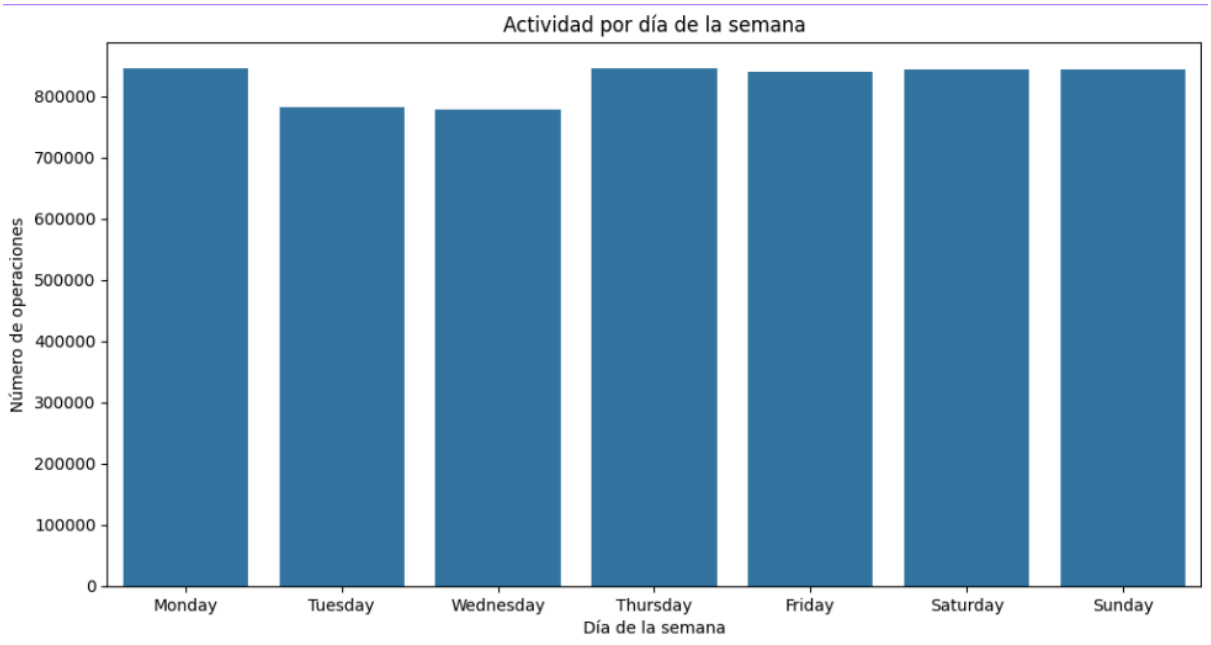
Insight 4



Gráfica 4: Distribución de operaciones por usuario (en millones)

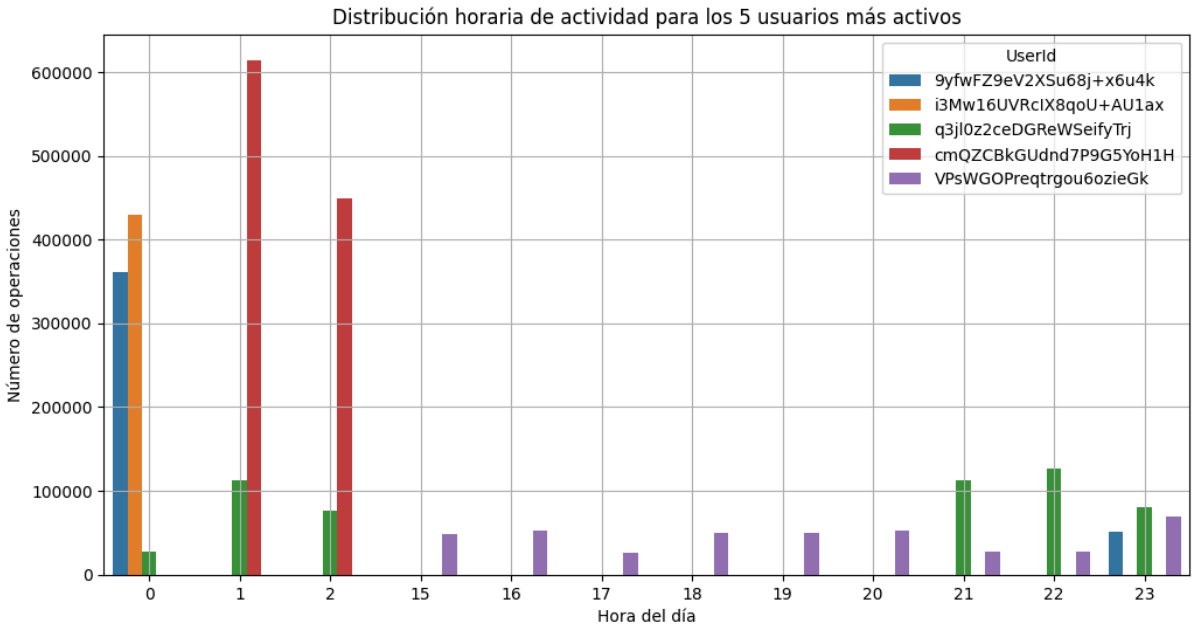
Se observó que el usuario con más actividad acumula más de un millón de registros, lo cual representa una frecuencia de uso inusualmente alta. Esta cifra supera ampliamente el comportamiento esperado para un usuario estándar.

Posiblemente sea algún proceso automático o un tipo de atacante.



Gráfica 5: Distribución de operaciones por día de la semana

No se detectan picos anómalos ni ausencias abruptas de actividad, por lo que se concluye que el sistema presenta un comportamiento estable y predecible a lo largo del calendario semanal. Incluso los fines de semana (que no son días hábiles)



Gráfica 6: Distribución horaria para los 5 usuarios más activos

En este gráfico podemos observar que los usuarios con mayor frecuencia en las bitácoras realizan operaciones en horarios específicos y repetitivos, particularmente alrededor de la 1 y 2 de la mañana. (Para el usuario que más movimientos tiene). Este comportamiento sugiere que dichas actividades podrían estar automatizadas, ya que no es común que usuarios reales interactúen con el sistema de forma consistente en horarios nocturnos.

Este patrón puede ser indicativo de procesos programados, scripts o tareas de mantenimiento que se ejecutan sin intervención humana directa. Si bien esto no implica necesariamente una anomalía, sí es recomendable validar con el equipo si estas operaciones están documentadas y autorizadas, para descartar actividades no supervisadas o potencialmente riesgosas.

UserId	
i3Mw16UVRcIX8qoU+AU1ax	46
9yfwFZ9eV2XSu68j+x6u4k	21
cmQZCBkGUdnd7P9G5YoH1H	17
q3jl0z2ceDGReWSeifyTrj	14
VPsWGOPreqtrgou6ozieGk	12

Tabla 12: Cantidad de días que tienen actividad los usuarios sospechosos.

Podemos ver en la Tabla 12 que los usuarios sospechosos no tienen actividades aisladas o esporádicas, sino que se distribuyen a lo largo de varios días. Esto podría indicar que su comportamiento está bien establecido y no responde a eventos puntuales.

Esto puede ser por automatización de procesos.

Insight 5. Métodos usados por pocas personas

Prop_MethodName	
CloseBRSession	0
Session_End	0
CloseTabForm	1
<RecreateFavorites>b__47_0	1
FreeBRLibrary	1
GetKendoGridCatalogs	1
GetProductProfilesByDBId	1
Environment	1
KendoComboBoxData	1
GetProductUsersByDBId	1

Tabla 13: Métodos usados por muy pocos usuarios

En la Tabla 13 se presentan los métodos que han sido ejecutados por pocos usuarios.

Esto puede indicar que son funciones poco comunes, o de uso especializado. Recordemos que un tipo de ataque es hacer la mayor cantidad de logs posibles, a veces usando funciones que casi nadie haría, por eso los métodos raramente utilizados deben ser revisados para asegurarse de que su activación no corresponde a accesos indebidos, pruebas no autorizadas o intentos de explotación de funciones ocultas.

También podrían ser métodos que podrían estar en desuso o ser parte de funcionalidades que ya no se emplean activamente, por lo que podrían considerarse para revisión y posible eliminación si no tienen una función actual válida.

Prop_MethodName	Invocaciones	UsuariosUnicos
Session_End	58	0
CloseBRSession	41	0
ConfigureControls	819697	10
ChangePropierties	223750	3
LogTime	1181845	26
GetKendoCustomDataSourceInstance	568233	14
ProcessBRRequest	1210627	33
ExecuteClientProtocol	191291	9
CheckForReturn	631494	37
ToolBarDesigner	16349	1

Tabla 14: Métodos con mayor número de invocaciones pero utilizados por pocos usuarios

En esta tabla se presentan los métodos que, a pesar de haber sido invocados miles de veces, han sido utilizados por un número muy reducido de usuarios. Este comportamiento es relevante desde una perspectiva de seguridad y auditoría.

Se recomienda analizar quiénes son los usuarios asociados a estos métodos, validar si las ejecuciones están documentadas y justificadas, y establecer umbrales de uso para detectar comportamientos anómalos en el futuro.

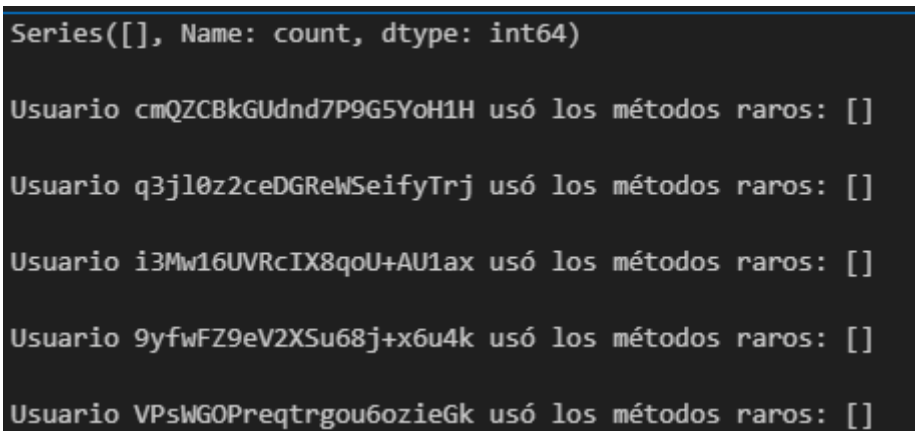


Tabla 15. Comparación de los métodos raros con los usuarios sospechosos

Para esta tabla, comparamos los usuarios que habíamos identificado como sospechosos con estos métodos que también consideramos como raros porque pocos los habían usado, no tuvimos ninguna coincidencia lo que quiere decir que no fueron parte de estos métodos raros.