

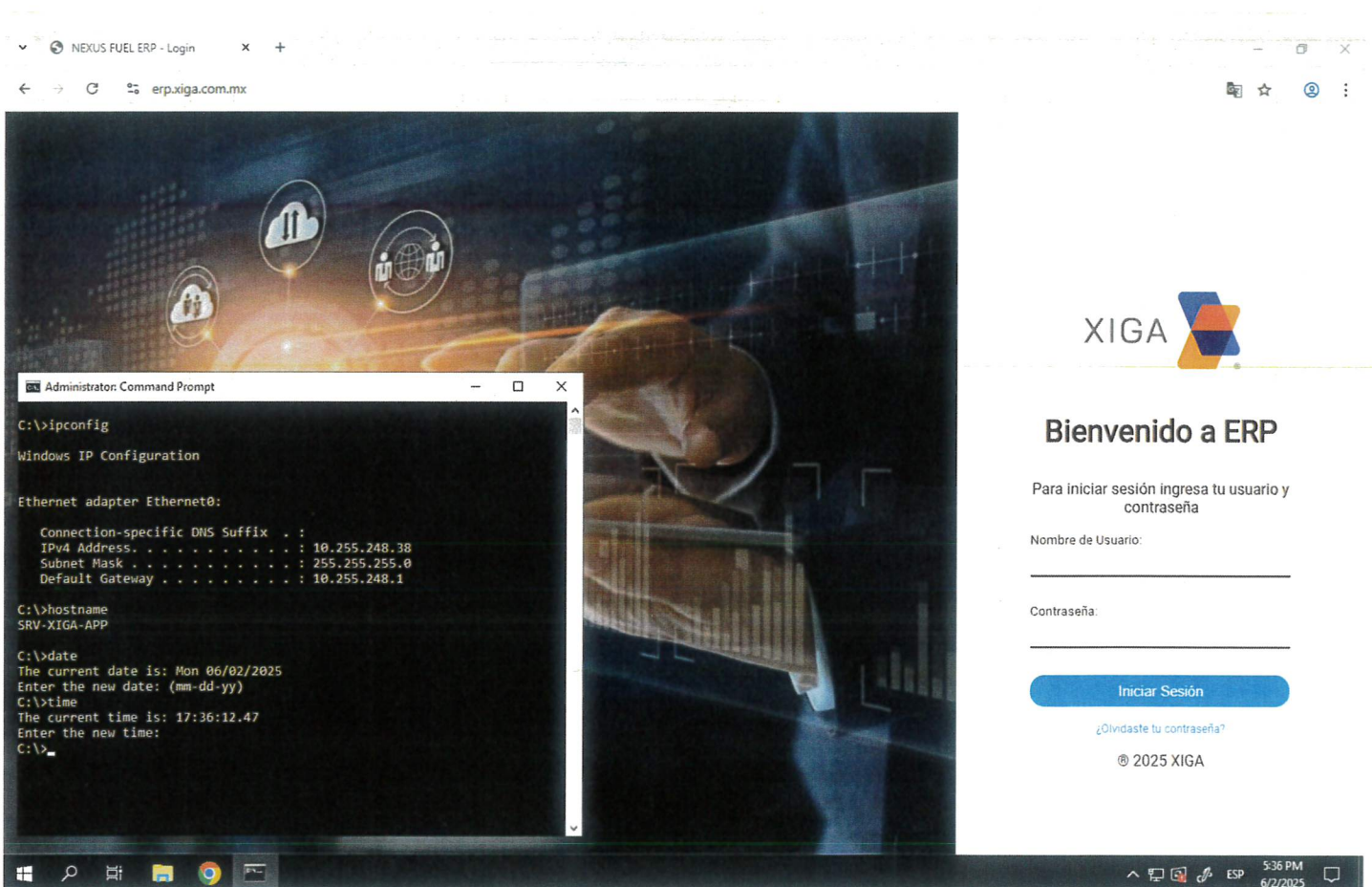
Req 46 Evidencia de Registros de Actividades de los Sistemas de Información y Sistemas Operativos

A nivel Aplicación

Toda actividad de transacciones del monedero electrónico queda registrada en una bitácora de eventos, la misma naturaleza de diseño del sistema impide que los usuarios puedan modificar o eliminar dichos registros por los siguientes motivos:

- Los logs se guardan en la base de datos del monedero
- La aplicación esta soportada por dos servidores, uno de base de datos y otro de aplicación
- Ni los usuarios comunes, ni los usuarios administradores del monedero tienen acceso
- Los usuarios no necesitan conectarse al servidor para usar la aplicación, esta es de tipo web, se conectan través de un navegador de Internet.

La Imagen muestra captura de pantalla de la aplicación del monedero electrónico, en un navegador web



Handwritten signature

La imagen muestra captura de pantalla del servidor SRV-XIGA-APP con dirección IP 10.255.248.38, donde se observa la bitácora de cambios en la cuenta de los clientes, la cual registra entre otras cosas, **origen de los cambios**, en este caso el portal web, se observa también **usuario que realizó el cambio, fecha, cliente, vehículo y descripción del cambio**. En este caso, (enmarcado en rectángulo de borde rojo) el usuario "ALEJANDRA" de la cuenta 10573 hizo cambio en los horarios de carga para el vehículo 00192 el día 22 de mayo a las 00:59

Lo que cumple con los siguientes requerimientos:

- Identificador del usuario que realiza la actividad.
- Descripción de la actividad realizada.
- Origen de la conexión al sistema.
- Resultado de la actividad efectuada
- Registros de solo lectura (en la aplicación no hay forma de eliminar o modificar los logs, son de solo lectura)

Departamento XIGA EMPRESARIAL

Carlos Alberto Calvillo Uribe

Bitácora Cambios Clientes

General

Cliente: _____ Vehículo: _____

Fuente: Todos Descripción: _____

Rango de Fecha

Inicial: 05/22/2025 Final: 06/02/2025

Buscar

Fuente	Fecha	Usuario	Cliente	Vehículo	Descripción
PORTAL	05/22/2025 00:59	ALEJANDRIA	10573	00192	
PORTAL	05/22/2025 00:59	ALEJANDRIA	10573	00192	Miércoles cambio en 00:00 a 00:59 de Encendido a Apagado Miércoles cambio en 08:59 de Encendido a Apagado Miércoles cambio en 17:00 a 17:59 de Encendido a Apagado a Jueves cambio en 02:00 a 02:59 de Encendido a Apagado Jueves cambio en 11:00 a 11:59 de Encendido a Apagado Jueves cambio en 19:00 a 19:59 de Encendido a Apagado
PORTAL	05/22/2025 00:59	ALEJANDRIA	10573	00192	
PORTAL	05/22/2025 01:53	Administrador de la cuenta	00746	00012	
PORTAL	05/22/2025 01:56	Administrador de la cuenta	00746	00019	POR LITRO: Limite Diario Litros: De 107 a 80. POR LITRO: Limite Diario Litros: De 107 a 80.
PORTAL	05/22/2025 02:05	Administrador de la cuenta	00746	00025	
PORTAL	05/22/2025 02:15	Diego Zepeda	11674	00000	Nuevo conductor Nombre: JAIME SALMERON Teléfono: 11674 00000 Activación de conductor JAIME SALMERON]
			11674	00123	Se agregó el conductor JAIME SALMERON con QR: [QR]
			03314	09190	Placa agregada;
			13999	00003	POR LITRO: Limite Diario Litros: De 80 a 100.
			03314	10170	Placa agregada;
			10516	00000	Se eliminó el conductor IGNACIO MARTINEZ.

5:55:56 PM
Monday, June 2, 2025

June 2025

Su Mo Tu We Th Fr Sa

1 2 3 4 5 6 7

8 9 10 11 12 13 14

15 16 17 18 19 20 21

22 23 24 25 26 27 28

29 30 1 2 3 4 5

6 7 8 9 10 11 12

Date and time settings

5:55 PM
6/2/2025

Administrator: Command Prompt

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
IPv4 Address. : 10.255.248.38
Subnet Mask : 255.255.255.0
Default Gateway : 10.255.248.1

Handwritten signature

A nivel base de datos

La imagen muestra captura de pantalla de SQL Management Studio en el Servidor SRV-XIGA-DB con dirección IP 10.255.248.37 mostrando la bitacora de cambios para clientes, donde se observan 2 registros por cada transacción el "Original" y el "Modificado", estos registros estan fuera del alcance de los usuarios.

Lo que cumple con los siguientes requerimientos:

a) Identificador del usuario que realiza la actividad.

b) Descripción de la actividad realizada.

c) Origen de la conexión al sistema.

d) Resultado de la actividad efectuada

e) Registros de solo lectura

errororAllowed	is_portal_consumptionGeneratorAllowed	pre_collection	Tipo	FechaCambio	Host_Name	APP_Name	System_User	Upd
1	1	1	Original	2025-06-02 13:29:07.870	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
2	1	1	Modificado	2025-06-02 13:29:07.870	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
3	1	0	Original	2025-06-02 13:29:03.107	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
4	1	0	Modificado	2025-06-02 13:29:03.107	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
5	0	1	Original	2025-06-02 13:29:00.917	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
6	0	1	Modificado	2025-06-02 13:29:00.917	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
7	0	1	Original	2025-06-02 13:29:00.450	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
8	0	1	Modificado	2025-06-02 13:29:00.450	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
9	1	1	Original	2025-06-02 13:28:59.493	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
		1	Modificado	2025-06-02 13:28:59.493	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
		1	Original	2025-06-02 13:28:59.380	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
		1	Modificado	2025-06-02 13:28:59.380	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
		1	Original	2025-06-02 13:28:57.990	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
		1	Modificado	2025-06-02 13:28:57.990	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
		1	Original	2025-06-02 13:28:57.880	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net
		1	Modificado	2025-06-02 13:28:57.880	SRV-MOVLAPP	Net SqlClient Data Provider	nexus_user	net

La imagen muestra captura de pantalla de SQL Management Studio en el Servidor SRV-XIGA-DB con dirección IP 10.255.248.37 mostrando la bitacora de cambios para l atabla de clientes donde se observa la ip de origen del cambio

SQLQuery1.sql - SRV-XIGA-DB\XIGA.GasmartCard (dbas (123)) - Microsoft SQL Server Management Studio

File Edit View Query Project Tools Window Help

Object Explorer

SRV-XIGA-DB

Database

System

Data

GasmartCard

Results

Messages

100 %

SELECT TOP 1000 [client_id]
.[number]
.[opening_balance]
.[enable]
.[balance]
.[contact_agent_id]
.[name]

Query executed successfully.

SRV-XIGA-DB\XIGA (15.0 RTM) | dbas (123) | GasmartCard | 00:00:53 | 1,000 rows

Ready Ln 241 Col 177 INS

Command Prompt

C:\>hostname
SRV-XIGA-DB
C:\>

07:28:34 p.m.
lunes, 2 de junio de 2025

junio de 2025

do. lu. ma. mi. ju. vi. sb.

1 2 3 4 5 6 7

8 9 10 11 12 13 14

15 16 17 18 19 20 21

22 23 24 25 26 27 28

29 30 1 2 3 4 5

6 7 8 9 10 11 12

Date and time settings

07:28 p.m.
02/06/2025

Free

Lo que cumple con los siguientes requerimientos:

f) Controles contra pérdida, destrucción, falsificación, acceso no autorizado y distribución no autorizada de dichos registros.

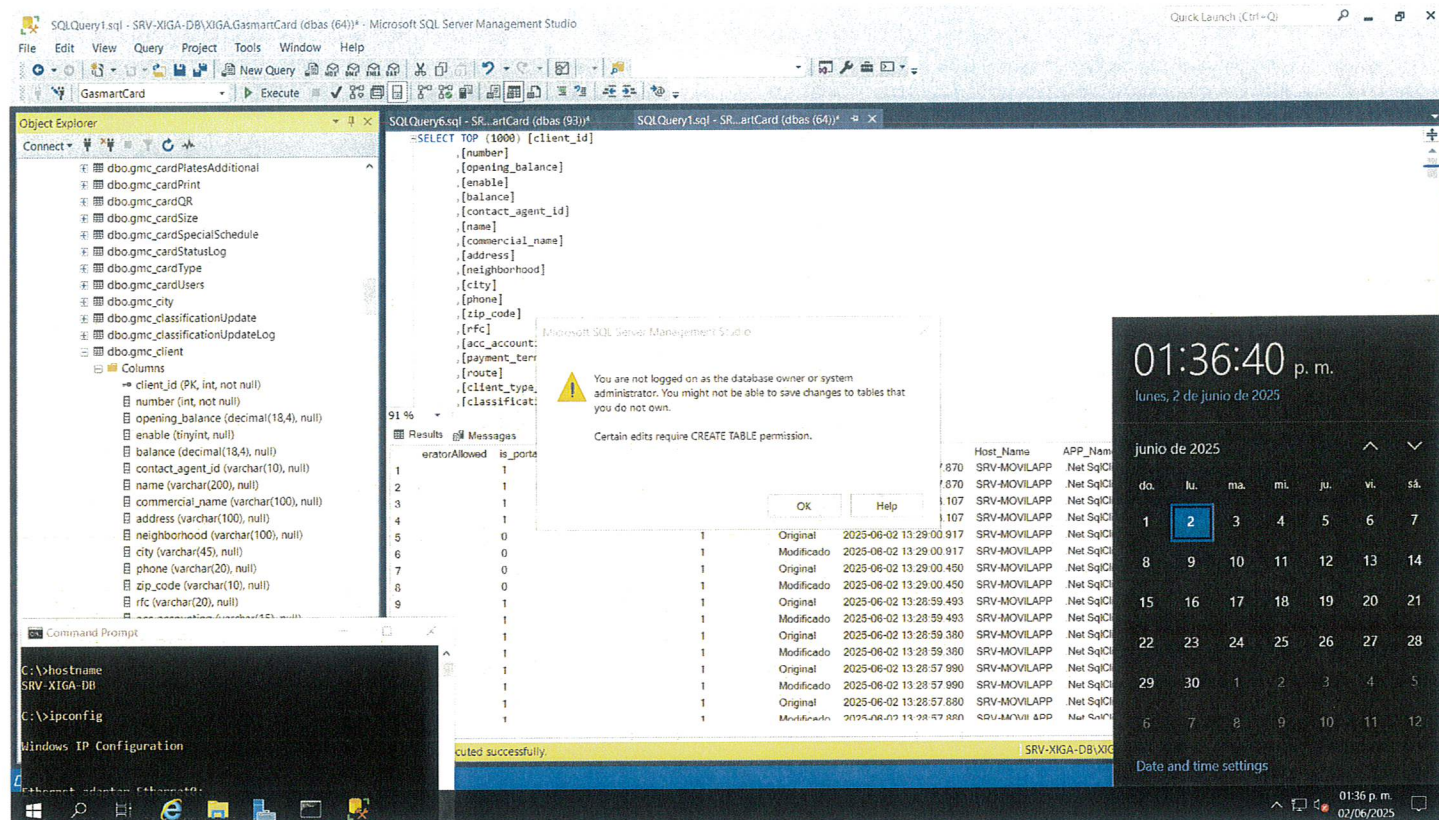


La imagen muestra captura de pantalla de SQL Management Studio en el Servidor SRV-XIGA-DB con dirección IP 10.255.248.37, la cual muestra mensaje de error al intentar eliminar un registro, incluso para el Administrador de la base de datos.

Lo que cumple con los siguientes requerimientos:

e) Registros de solo

f) Controles contra pérdida, destrucción, falsificación, acceso no autorizado y distribución no autorizada de dichos registros.

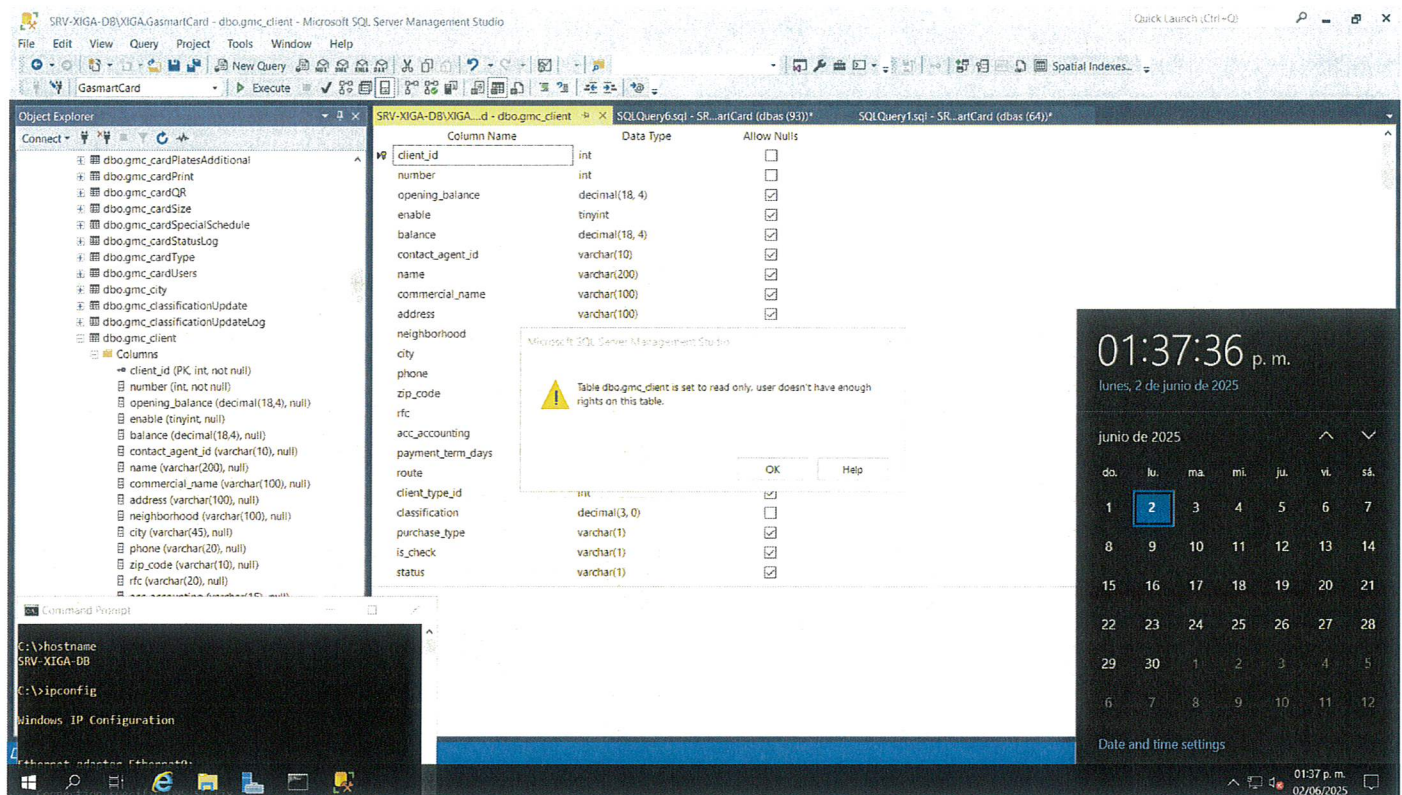


La imagen muestra captura de pantalla de SQL Management Studio en el Servidor SRV-XIGA-DB con dirección IP 10.255.248.37, la cual muestra falta de permisos de solo lectura al intentar modificar la base de datos.

Lo que cumple con los siguientes requerimientos:

e) Registros de solo lectura

f) Controles contra pérdida, destrucción, falsificación, acceso no autorizado y distribución no autorizada de dichos registros.



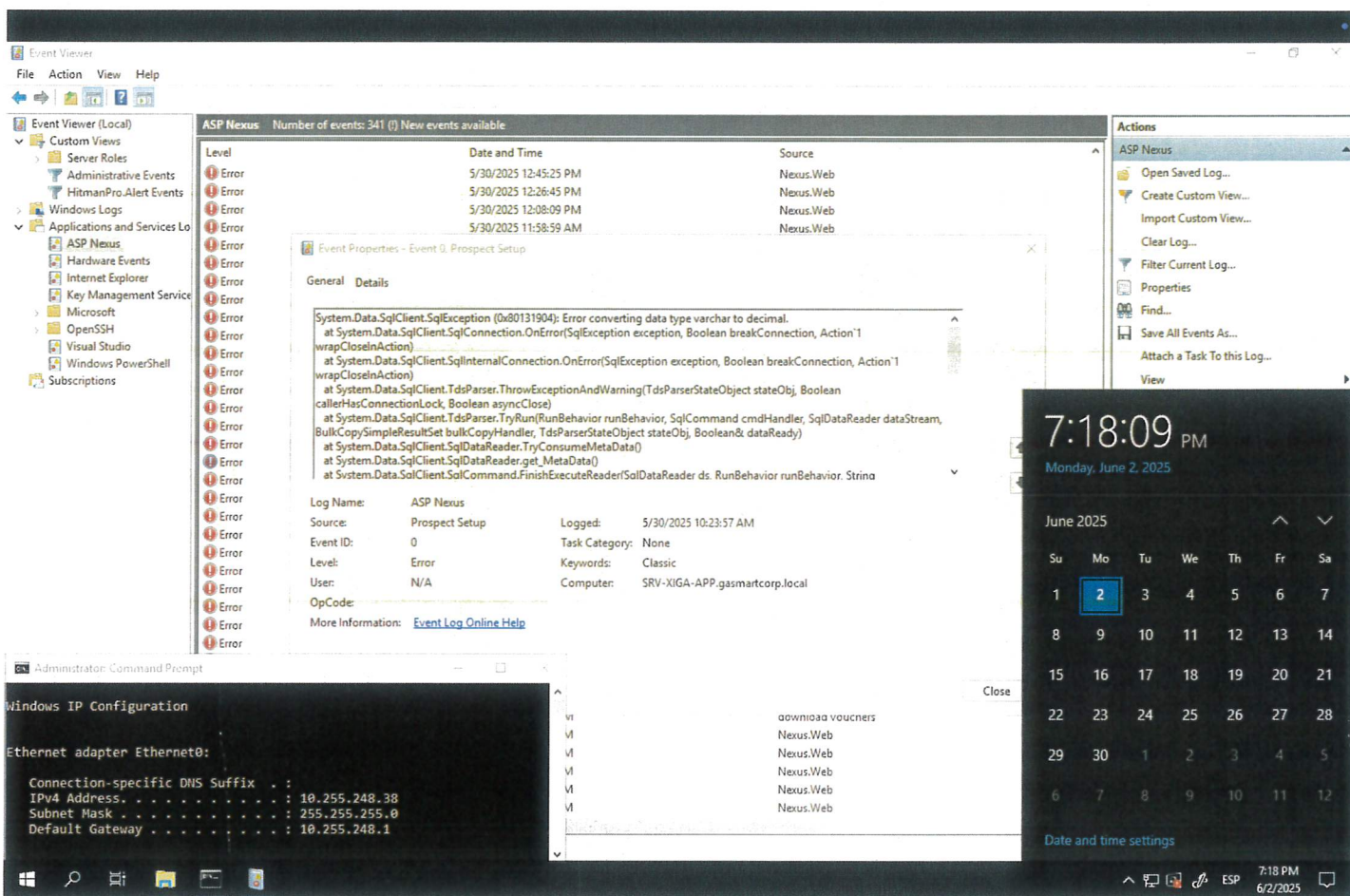
A nivel Sistema Operativo

La imagen muestra captura de pantalla del visor de eventos del sistema operativo, del servidor SRV-XIGA-APP con dirección IP 10.255.248.38, donde se observa el registro de errores de la aplicación a nivel sistema operativo, en este caso un error de conversión de tipos, ocasionado por captura de datos incorrecta, capturaron datos alfanuméricos en lugar de digitar sólo números.

Los registros del visor de eventos están fuera del alcance de los usuarios, por lo que nos permite cumplir con los requerimientos

e) Registros de solo lectura

f) Controles contra pérdida, destrucción, falsificación, acceso no autorizado y distribución no autorizada de dichos registros.

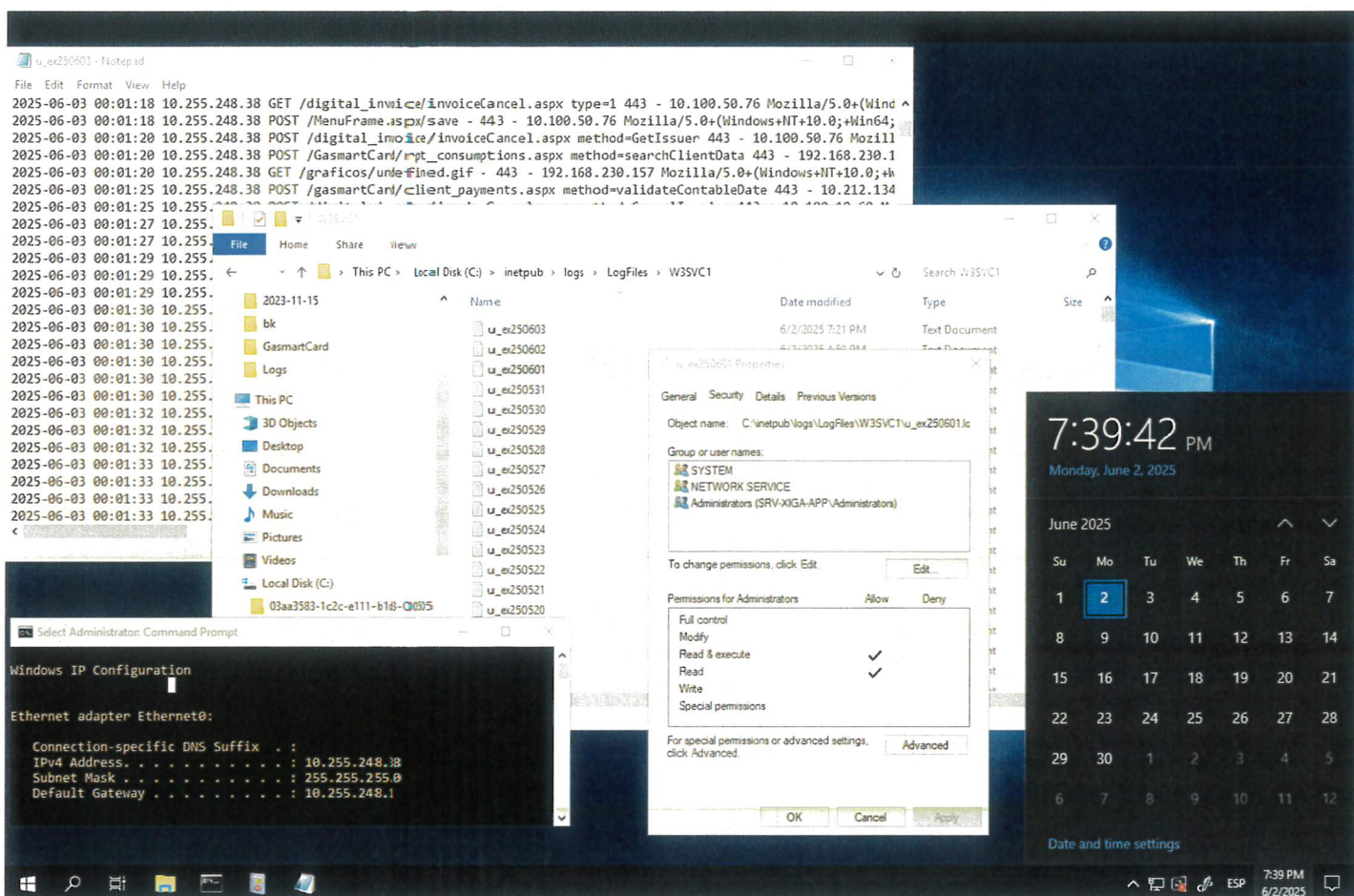


La imagen muestra captura de pantalla de la carpeta de logs del IIS (Internet Information Server), en el servidor SRV-XIGA-APP con dirección IP 10.255.248.38, donde se observa el registro de todas las

peticiones que recibió el servidor a nivel sistema operativo para la aplicación del monedero. Se observa que los permisos para el archivo u_ex250501 son de solo lectura para el administrador, no existen permisos de ningún tipo para el resto de los usuarios, lo que nos permite cumplir con los requerimientos

e) Registros de solo lectura

f) Controles contra pérdida, destrucción, falsificación, acceso no autorizado y distribución no autorizada de dichos registros.



Handwritten signature

A nivel Sistema Backup

Para recuperarse de la destrucción o pérdida de los sistemas de forma deliberada o accidental, como última línea de defensa se implementan una serie de sistemas de respaldo, con estrategias 3-2-1 basado en VeeamBackup con repositorios en dos centros de datos diferentes y uno en la nube. La imagen a continuación muestra captura de pantalla de la consola de VeeamBackup, Software utilizado para la gestión de respaldos. Lo que nos permite cumplir con el requerimiento

f) Controles contra **pérdida, destrucción**, falsificación, acceso no autorizado y distribución no autorizada de dichos registros.

La imagen muestra consola de veeam backup donde se aprecia la definición de la tarea de respaldo para el servidor de aplicación del Monedero xiga (SRV-XIGA- APP) observándose calendarización de respaldo cada 24 horas.

The screenshot displays the Veeam Backup and Replication console. The main window shows the configuration for a backup job named 'Backup_SRV-XIGA-APP'. The job is a VMware Backup with 1 object, currently in a 'Stopped' status. The schedule is set to 'Daily at this time: 01:00 AM' on 'On these days'. The console also shows a list of jobs, including 'Backup_SRV-XIGA-DB', which is also a VMware Backup with 1 object, also in a 'Stopped' status. The console includes a sidebar with navigation options like 'Home', 'Jobs', 'Replication', 'Backup Copy', 'Backups', 'Disk', 'Disk (Copy)', 'Disk (Orphaned)', 'Object Storage (Copy)', 'Replicas', 'Ready', 'Active (1)', 'Last 24 Hours', 'Running (1)', and 'Success'. The bottom of the console shows the system clock as 8:01:38 PM on Monday, June 2, 2025, and a calendar for June 2025. The calendar shows the date June 2, 2025, highlighted. The system clock also shows the date and time settings as 8:01 PM on 6/2/2025.

Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Backup_SRV-XIGA-APP	VMware Backup	1	Stopped	19 hours ago	Success	6/4/2025 1:00 AM	StoreOnce_NGX	Created by SRV-MONITORIA
Backup_SRV-XIGA-DB	VMware Backup	1	Stopped	19 hours ago	Success	6/3/2025 12:30 AM	StoreOnce_NGX	Created by SRV-MONITORIA

Schedule Configuration:

- Run the job automatically: ☒ Daily at this time: 01:00 AM On these days
- Monthly at this time: 10:00 PM
- Periodically every: 1
- After this job: 1
- Automatic retry: ☒ Retry failed items processing: 3 times Wait before each retry attempt for: 10 minutes
- Backup window: ☐ Terminate the job outside of the allowed backup window

Handwritten signature

La imagen muestra consola de veeam backup donde se aprecia la definicion de la tarea de respaldo para el servidor de aplicacion del Monedero xiga (SRV-XIGA- DB) observandose calendarizacion de un respaldo cada 6 horas.

Job Tools

Veeam Backup and Replication

Home

View

Job

Start

Stop

Retry

Active Full

Statistics

Report

Edit

Clone

Disable

Delete

Job Control

Details

Manage Job

Veeam Intelligence

Home

Jobs

Backups

Replicas

Backup

Replication

Backup Copy

Disk

Disk (Copy)

Disk (Orphaned)

Object Storage (Copy)

Ready

Active (1)

Last 24 Hours

Running (1)

Success

Home

Inventory

Backup Infrastructure

Storage Infrastructure

Tape Infrastructure

Files

Jobs

Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Backup_SRV-XIGA-APP	VMware Backup	1	Stopped	19 hours ago	Success	6/4/2025 1:00 AM	StoreOnce_NGX	Created by SRV-MONITORIA
Backup_SRV-XIGA-DB	VMware Backup	1	Stopped	19 hours ago	Success	6/3/2025 12:30 AM	StoreOnce_NGX	Created by SRV-MONITORIA

Edit Backup Job Backup_SRV-XIGA-DB

Schedule

Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

Name

Virtual Machines

Storage

Secondary Target

Guest Processing

Schedule

Summary

☒ Run the job automatically

Daily at this time:

12:30 AM

Everyday

Days

Monthly at this time:

17:00 PM

Fourth

Saturday

Months

Periodically every:

6

Hours

Schedule...

After this job:

Backup_SRV-C2U1 (Created by SRV-MONITOR Administrator at 7/21)

Automatic retry

☒ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

Backup window

☐ Terminate the job outside of the allowed backup window

Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

Window

< Previous

Apply

Finish

Cancel

8:04:08 PM

Monday, June 2, 2025

June 2025

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Date and time settings

1 job selected

Connected to: localhost

Build: 12.3.0.310

8:04 PM

6/2/2025

Handwritten signature